NĚKOLIK POZNÁMEK K OCHRANĚ KRITICKÉ INFRASTRUKTURY

SOME REMARKS ON THE CRITICAL INFRASTRUCTURE PROTECTION

Jaroslav MOZGA, František KOVÁŘÍK
kovarik@ioolb.izscr.cz

Došlo 12. 2. 2010, přepracováno 22. 4. 2010, přijato 30. 4. 2010.
Dostupné na http://www.population-protection.eu/attachments/027_vol2n1_mozga_kovarik.pdf.

Abstract

Ever increasing complexity of modern society also leads to its bigger vulnerability. Therefore the critical infrastructure and its protection should be approached from a systematic point of view. This article describes two systematic methods – LCCI and SoS, as abstract basis for planning and strategy of protection. Relationship between the state administration and critical infrastructure companies is paramount when formulating strategy of protection and analysis of needs according to the Maslow's pyramid, because critical infrastructure services are crucial for provision of certain standard of living. The article emphasizes necessity of co-operation between private-public sectors when analysing risks of critical infrastructure, and briefly without a detailed analysis describes some methods of risk analysis, which are suitable for identification of risks.

Keywords
Critical infrastructure protection, system, risk, vulnerability.

Lidé měli vždy snahu uspořádat svůj život a společnost tak, aby žití bylo přijatelné a hlavně bezpečné. V každé historické společnosti se vytvářela infrastruktura[1], která na základě dělby práce a technologického rozvoje poskytovala produkty a služby a vždy existovala infrastruktura umožňující existenci a rozvoj společnosti:

- **Fyzické struktury** tvořící základ rozvoje společnosti (např. dodávky vody – akvadukty v Římské říši a dopravní komunikace),
- **Základní služby** (např. dodávka potravin – organizace potravinové soběstačnosti v Incké říši),
- **Infrastruktura správy** (např. správní orgány Číny a říše Římské).

Počínaje průmyslovou revolucí, rozvíjel technologický rozvoj tyto základní typy infrastruktury až do dnešního rozsahu včetně infrastruktury řízení a správy společnosti. Pojem infrastruktura se dlouhodobě užíval především v souvislosti s hospodářským rozvojem (infrastrukturou se rozumí soubor zařízení usnadňujících produkci zboží a služeb) a kladlo se rovnítko mezi rozvoj

společnosti a kvalitu infrastruktury. Marshova zpráva[2] z roku 1997 definovala infrastrukturu současné společnosti „*jako síť nezávislých, převážně privátně vlastněných, člověkem vytvořených systémů, které fungují synergicky tak, aby plynule produkovaly a distribuovaly dodávky důležitých produktů a služeb*“[3]. Některé infrastruktury jsou však důležitější z hlediska celostátního významu nebo z hlediska závažnosti důsledků své nefunkčnosti a hovoří se o **kritické infrastruktuře,** jejíž „*nefunkčnost nebo zničení má závažné dopady na obranu a národní bezpečnost*“ (Marsh, 1997). Marshova definice kritické infrastruktury se časem vyvíjela a byla doplněna například o dopady na kvalitu života obyvatel. Není však cílem článku zabývat se definicemi, které se od sebe často odlišují, jak ostatně ukazuje přehled národních definic kritické infrastruktury (Gordon a Dion, 2008). Nicméně z definic kritické infrastruktury pak vyplývá počet odvětví, které jsou do kritické infrastruktury zahrnuty. Obdobně jak rozdílné jsou definice kritické infrastruktury, bývá rozdílný i počet odvětví kritické infrastruktury a klíčových aktiv (objektů)[4].

Cílem ochrany kritické infrastruktury je snížení její potenciální zranitelnosti (zvýšení její resilience[5]). Také strategie ochrany kritické infrastruktury je poměrně komplikovaná záležitost, poněvadž se musí řešit problémy různé úrovně (strategie celostátní, regionální, municipální) a pro různá odvětví, která jsou vzájemně propojena. Strategie ochrany nemůže být souborem právních předpisů a vyhlášek nebo tabulek, strategie se musí chápat jako „jízdní řád“ pro řešení složitých problémů zahrnujících alokaci zdrojů, organizování, technologie a vliv lidského faktoru.

Luiijf et al. (2005) upozorňují na to, že v mnoha případech krizové plánování i kompetentní autority veřejné správy **nechápou správně** povahu kritické infrastruktury, zejména její složitost a závislosti, přestože fungování složek IZS a ochrany obyvatel závisí také na funkcionalitě kritické infrastruktury. Proto je nezbytné:

A. Zvolit systémový (systémově inženýrský) přístup k ochraně

Na workshopu Úřadu ochrany kritické infrastruktury amerického Ministerstva vnitřní bezpečnosti a Národního centra analýzy a simulace infrastruktury (duben 2009) se konstatovalo, že kritická infrastruktura by se měla chápat jako komplexní systém[6], protože:

- se skládá z mnoha částí, které jsou v interakci pomocí lokálních pravidel, což má za následek **emergentní struktury** (sítě) a **chování** (kaskády) v rozsáhlém měřítku;
- obsahuje **lidi s jejich chováním a myšlením** (viz Socio Cognitive Engineering);
- reaguje na místní a globální politiku;
- kritickou infrastrukturu tvoří **vzájemně závislé systémy systémů.**

Systémový přístup ke kritické infrastruktuře je důležitý, poněvadž se jím vytváří nástroj na simulaci a modelování chování kritické infrastruktury v různých provozních situacích s cílem pochopit v předstihu dynamické změny.

B. Zabývat se vztahem veřejné správy s podniky kritické infrastruktury

V Norsku se komise vedená ministerským předsedou K. Willochem (The Willoch Commission, JD NOU, 2000) zabývala problémem zranitelnosti současné společnosti a iniciovala vznik projektu CISS (Critical Infrastructures, public sector reorganisation and Societal Safety). Klíčovou otázkou projektu je otázka: „**Jaké jsou důsledky reorganizace veřejné správy pro kritickou infrastrukturu a bezpečnost společnosti**?" v kontextu organizačních parametrů, jako jsou **kontrola, koordinace, redundance a kultura bezpečnosti.**

Deregulace, „rozpojení" (unbundling) a privatizace způsobují, že privátní aktéři v rámci sítě služeb pro veřejnost se zajímají o veřejné hodnoty jen potud, pokud vytvářejí zisk. Současně má veřejná správa omezené možnosti kontroly nad provozem infrastruktury, přičemž občané činí veřejnou správu odpovědnou za průběh obnovy funkcí kritické infrastruktury po případné poruše. Ochrana kritické infrastruktury však vyžaduje partnerství soukromého sektoru a veřejné správy, což znamená porozumět podnikovému řízení a řízení podnikových rizik, zejména rizik nefunkčnosti kritické infrastruktury nebo jejích prvků a plánování kontinuity (pokračování v dodávkách produktů a služeb pro veřejnost), jelikož primárním zájmem ochrany kritické infrastruktury není udržení maximální účinnosti a efektivity každého prvku infrastruktury (odvětví), nýbrž zajištění přiměřené úrovně služeb i v případě pohromy nebo krizové situace.

C. Analyzovat kritickou infrastrukturu z hlediska lidských potřeb

Příkladem takové analýzy může být inspirativní dokument „*Dall´analisi alla proteziome delle infrastrutture critiche*" vypracovaný pracovníky italského Úřadu civilní ochrany (Franchina et al., 2009).

Z výše uvedeného vyplývá, že plánování a strategie ochrany kritické infrastruktury vyžaduje pochopení a poznání:

- role a odpovědnosti veřejné správy a soukromého sektoru při hledání strategie ochrany a dostatečné resilience,
- vztahů mezi fyzickými a kybernetickými hrozbami,
- účinků poruch kritické infrastruktury na municipality a regiony,
- nutnosti investic na zlepšení ochrany a resilience kritické infrastruktury,
- nezbytné úrovně znalosti o technických systémech a socio-technických systémech včetně znalosti organizačních aspektů, ekonomických a tržních podmínek apod.,
- tendencí v prioritách občanů v souvislosti s aktuálními standardy životní úrovně a vnímáním stavu životního prostředí.

1. Kritická infrastruktura jako síť, systém, systém systémů

Každý systém se obecně skládá ze souboru (množiny) vzájemně propojených prvků a funkcionalita[7] celého systému závisí na správné funkčnosti jednotlivých prvků. Zásadní rozdíl mezi sítí a systémem spočívá v tom, že zatímco

systém je zcela definován **vztahy mezi prvky** a je proto vnitřně soudržný, tak síť se rozpíná a komunikuje v každém směru, aniž by ztratila svou soudržnost. Síť je tedy svou podstatou otevřeným systémem. Tato poznámka je důležitá, protože se někdy dávají do protikladu systém systémů a pojetí infrastruktury jako rozsáhlého složitého systému (LCCI), přičemž oba koncepty pracují s naprosto stejnými vlastnostmi (resilience, zranitelnost, přežití, vzájemné závislosti apod.) a stejnými typy poruch[8].

1.1 Kritická infrastruktura jako rozsáhlý a složitý systém[9] (koncept LCCI)

Koncept LCCI (Large Complex Critical Infrastructure) se zavedl v projektu SAFEGUARD a definuje se jako **distribuovaná síť počítačových systémů**, která se zkoumá v různých vrstvách: **fyzické, kybernetické** (regulace), **organizační** (management, supervize) a **strategické** (podniková politika provozovatele kritické infrastruktury). Z těchto vrstev vyplývá, že je nutné se zabývat i podnikovými hledisky funkcionality kritické infrastruktury.

Bologna a Beer (2003) upozorňují na určité obtíže spojené se síťovou reprezentací LCCI, týkající se **složitosti strukturální** (počet uzlů sítě a spojení mezi uzly) a **dynamické** (uzly mohou být nelineárními systémy), **rozmanitosti uzlů** (uzly mohou být různého typu) a **spojení** (spoje mezi uzly mohou mít různou důležitost a směr), a tyto obtíže se projevují zejména ve formulaci modelů chování LCCI v různých provozních stavech.

Nicméně síťový přístup může být přínosem ve strategii ochrany kritické infrastruktury, protože síť nelze ochránit jako celek, lze ochránit jen tzv. „hubs" sítě (propojení v rámci sítě) na základě analýzy kritických uzlů.

1.2 Systém systémů

Tradiční systémový přístup staví na hierarchii – podsystém, systém, suprasystém. Tento přístup však v případě kritické infrastruktury není vždy na místě, protože kritická infrastruktura je v podstatě **socio-technickým systémem**[10] (technický systém – technologie a technická zařízení, sociální systém – lidé, instituce, podniky), v němž je nezbytné zabývat se, kromě hierarchie, také kooperací, koordinací a sdílením. A navíc se v kritické infrastruktuře musí pracovat s tzv. **emergentním** (vynořujícím se) chováním, jež je výsledkem **interakcí prvků každého systému** a které **nelze předvídat na základě znalostí o chování jednotlivých prvků systému.** Vhodným myšlenkovým východiskem je tudíž chápání kritické infrastruktury jako **systému systémů**, protože se analyzují a hodnotí různé typy systému vyžadující různé metodiky.

Systém systémů existuje jako skupina nezávislých systémů, které jsou propojeny tak, aby účinně a účelně podporovaly jak každodenní operace a plánované činnosti, tak činnosti v nouzových a krizových situacích. Systém systémů vychází z těchto konceptů:

- Systémy mají tyto složky: *lidé, organizace, procesy, produkty* (výsledky činnosti systémů) a *technologie*. Výsledky systému systémů se dají vyjádřit ve tvaru

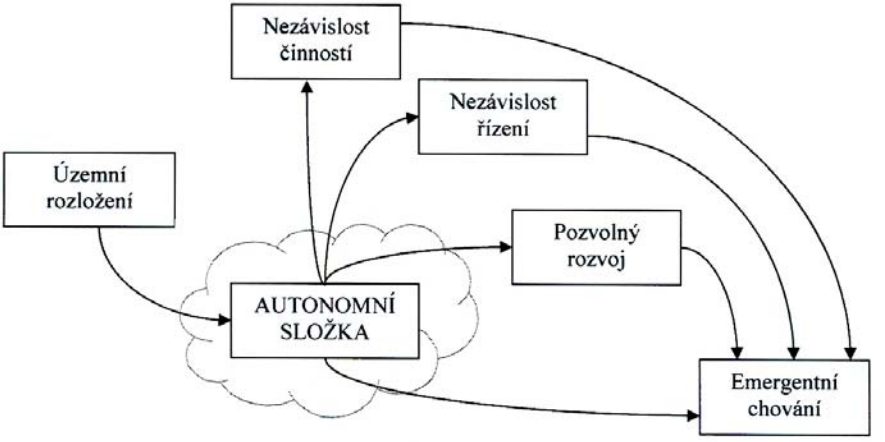
$$\mathbf{V = R\ (EX, EN, P)},$$

kde V jsou výsledky (realizace cílů), R jsou vztahy (funkční, kauzální, mezi vnějšími a vnitřními vlivy), EX jsou vnější vlivy, EN jsou vnitřní vlivy, P je strategie a koncepce.
- Systémy mají vztahy na úrovni řízení a správy (governance), mezi technologiemi a standardizovanými provozními postupy.
- Systém systémů je územně rozprostřen mezi různými správními obvody.
- Systémy jsou vzájemně závislé prostřednictvím tzv. kontinua interoperability[11] (governance, informační technologie, rozhodovací procesy apod.). Kompatibilní technologie nezaručují interoperabilitu, ta se dosahuje propojením technologií, lidí a organizace.

Konceptuální charakteristiky systému systémů zformuloval Maier (1998):

- **Nezávislost činností** (za určitých podmínek)
  Je třeba rozlišovat mezi *schopností* fungovat nezávisle a *podmínkou (požadavkem)* fungovat nezávisle. Systém systémů pracuje s pojmem **funkční závislosti** (jedno nebo obousměrné) vztahující se zejména k technologii (výroba, zpracování informací, rozhodování).
- **Nezávislost řízení**
  Prvek systému systémů udržuje kontinuitu činností nezávisle na systému systémů.
- **Územní rozložení** (diktuje výměnu informací)
  V rámci územního rozložení se analyzuje **prostorová korelace** (těsnost územních vztahů) ve vztahu k funkční závislosti (přímá či nepřímá).
- **Pozvolný rozvoj**
  Funkce a zaměření (včetně klíčové role) jednotlivých systémů se přidávají, odstraňují a upravují podle zkušenosti nebo situace.

Konceptuální vlastnosti systému systémů zformulované Maierem se vztahují k emergentnímu chování (obr. 1) a nejsou v rozporu s analytickými charakteristikami kritické infrastruktury, jak je uvádí příloha 1. Nicméně nutno konstatovat, že je žádoucí ověřit tento přístup v praxi a zjistit, jaký je jeho příspěvek pro rozhodování o ochraně kritické infrastruktury.



Obr. 1
Charakteristiky systému systémů

Kritická infrastruktura se ze zorného úhlu systému systémů může klasifikovat a zkoumat několika způsoby:

- **Podle úrovně analýzy** (analýza celku, analýza částí**)**
  - *systém systémů* (veřejná správa, společnost, hospodářství),
  - *vzájemně závislé systémy* (soubor kritických infrastruktur),
  - *individuální systémy* (telekomunikace, doprava, energetika apod.),
  - *technické prvky* (počítače, rozvodné sítě apod.).
- **Podle způsobu řízení - centralizace/decentralizace**
  Decentralizovaná infrastruktura se liší od centralizované mírou závislostí, a jelikož má méně závislostí než centralizovaná infrastruktura, je spolehlivější[12] v krizové situaci.
  Centralizovaná infrastruktura v kontextu SSTR (Security Stability Transition Reconstruction) má problémy s údržbou a ochranou „lineárních aktiv“ (rozvody elektřiny a plynu) a kaskádní selhání vzájemně provázaných infrastruktur má za následek, že centralizovaná infrastruktura je velmi problematická v nestabilních podmínkách.
- **Podle poruch**
  Porucha nebo přerušení poskytování služeb a produktů má za následek závažné škody a ztráty a analýza dopadů hledá hranice přijatelnosti a tolerovatelnosti v závislosti na čase – 6 h, 24 h, 72 h, týden atd.

2. Veřejná správa, municipální infrastruktura a analýza potřeb

Služby poskytované kritickou infrastrukturou mají vysokou důležitost pro veřejnost, přičemž hodnoty veřejnosti (bezpečí, spolehlivost, cenová dostupnost) jsou většinou v rozporu s orientací na ziskovost ze strany soukromého vlastníka kritické infrastruktury. Veřejná správa zabezpečující službu ochrany obyvatelstva by měla věnovat zvýšenou pozornost zejména těm službám, jejichž selhání nebo porucha se okamžitě rozpozná – jmenovitě se to týká dodávky vody, potravin a energií (tzv. život podporující funkce).

Lewis a Darken (2005) publikovali zajímavý přehled problémů a falešných mýtů na základě poznatků z praxe včetně komentářů autorů, s nimiž se lze potkat při budování ochrany kritické infrastruktury. Některé problémy a mýty uvádíme jako příklad pro srovnání s naší praxí:

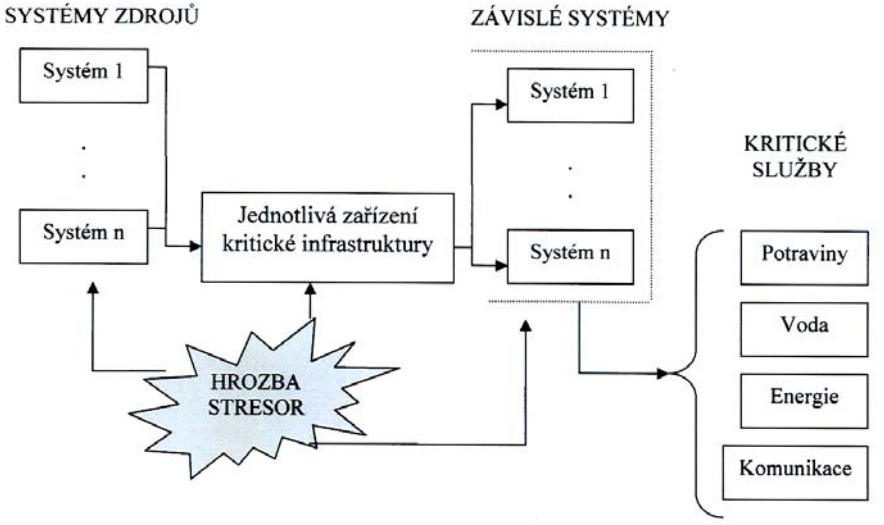
- Mylný předpoklad: **Místní veřejná správa rozhoduje o alokaci zdrojů na ochranu kritické infrastruktury.**
  Jednoduše řečeno, to co je kritické na místní úrovni, nemusí být kritické na celostátní úrovni. Financování musí vycházet z objektivních znalostí skutečných potřeb a jak Lewis a Darken uvádějí, tak většina amerických měst nemá kvalifikované vědecké expertizy rizik.
- Mylný předpoklad: **Alokace finančních zdrojů by měla záviset na velikosti regionu a jiných politických faktorec**h.
  Autoři konstatují na základě datové analýzy, že alokace zdrojů, založená na libovolných nebo politických faktorech a požadavcích, neřeší v žádném případě problém zlepšení bezpečnosti.
- Problém: **Kritickou infrastrukturu vlastní převážně soukromí vlastníci a veřejná správa nemůže intervenovat v zájmu veřejnosti, a proto kritickou infrastrukturu by měli ochraňovat vlastníci, nikoli veřejná správa. Protože ochranná opatření jsou nákladná, je nepravděpodobné, že by vlastníci investovali do ochrany v zájmu veřejnosti.**
  Výše zmíněná argumentace, která často ospravedlňuje politiku nicnedělání veřejné správy, zcela opomíjí regulační mechanizmy některých odvětví (energetika, telekomunikace, vodárenství apod.) včetně „diktátu“ bezpečnostních standardů ze strany Ministerstva vnitřní bezpečnosti USA.
- Mylný předpoklad: **Ochrana kritické infrastruktury je příliš nákladná, aby ji realizovali vlastníci, takže se musí zvýšit daně a musí se navrhnout finanční pobídky pro vlastníky, aby zodolnili svá aktiva v zájmu státu**.
  Tento mylný předpoklad zcela opomíjí fakt kontinuity operací (kontinuita operací = provozní kontinuita), která je bytostným zájmem každého podniku, a tak největší škody může způsobit ztráta provozní kontinuity, a proto by se **veřejná správa měla zaměřit na řešení problémů provozní kontinuity.** To však **předpokládá orientaci v systému podnikového řízení, znalost managementu aktiv, znalost vztahů v rámci dodavatelského řetězce** (vztahy mezi podniky) apod.[13]

Strategie ochrany kritické infrastruktury ze strany veřejné správy musí vycházet z pochopení, že ochrana *per se* (sama o sobě) by neměla být cílem. Neochraňuje se infrastruktura jako taková, ale **ochraňují se poskytované služby**, na nichž závisí kvalita života občanů, a strategie ochrany není životaschopná, není-li ekonomicky a politicky udržitelná.

Jak uvádí Auerswald et al. (2005), kromě hodnocení zranitelnosti, plánování provozní kontinuity, investování do technologií podnikových strategií (organizační, finanční) by se měly zlepšit schopnosti vlastníka kritické infrastruktury a veřejné správy tak, aby se:

- rozpoznala a podporovala tzv. vysoce spolehlivá organizace a systém řízení spolehlivosti,
- hledala rovnováha mezi strategiemi zdůrazňujícími anticipaci a strategiemi, které zdůrazňují resilienci,
- sdílely informace o technologických a organizačních změnách a podporovala se kultura bezpečnosti v organizaci,
- podporoval dialog mezi občany a zájmovými skupinami s cílem stanovit priority,
- rozvíjely programy finanční pobídky pro privátní investice do bezpečnosti.

2.1 Regionální a municipální infrastruktura



Obr. 2
Systémy municipální infrastruktury

Poskytovatelé produktů a služeb kritické infrastruktury jsou stranou **nabídky**, ale pro potřeby ochrany obyvatel je nutné znát situaci na straně

poptávky, jelikož služby infrastruktury jsou vždy **lokální** – vztahují se ke konkrétnímu místu a ke konkrétním sociálním skupinám.

Analýza služeb infrastruktury v nouzových a krizových situacích by měla zkoumat **úroveň zabezpečení** služeb majících vliv na zdraví sociálních skupin. Obecně existuje několik možností ohrožení zdraví vedoucích až ke smrti:

a) **nežádoucí teplota prostředí** (ochrana proti chladu a teplu vyžaduje energii a ukrytí),
b) **nedostatek potravin a vody**,
c) **zranění a infekce** (zdravotní, hygienické a sanitární služby).

Některé služby lze **generovat na místě** (například fotovoltaické panely umožní generovat elektřinu) a některé mohou využít **místní zdroje** (začíná se podporovat vznik lokálních potravinových systémů v rámci potravinové bezpečnosti).

Municipální infrastruktura je sice součástí centralizované infrastruktury, nicméně municipalita má možnost zabývat se tzv. **improvizovanou lokální infrastrukturou** (viz například *Small is profitable* od Rocky Mountain Institute). Improvizovanou lokální infrastrukturu tvoří například systémy, které se instalují na budovy, takže infrastruktura je **vlastněna a chráněna** majiteli budov (viz TIDES – Transportable Infrastructures for Development and Emergency Support).

Na úrovni lokality, municipality je možné se zabývat tzv. **resilientní komunitou**, což je komunita, která předvídá, připravuje se, zvládá a zotavuje se z významných lokálních hrozeb s minimem škod na zdraví, místním bezpečném prostředí a místní ekonomice. Mezi její charakteristické znaky patří **soběstačnost, sebespoléhání** a **schopnost sebeobnovy** ve vztahu ke kritickým službám (příloha 3).

A v posledku orientace na municipality a resilientní komunitu vede k tomu, že plány ochrany se dávají do souvislostí s plány územního rozvoje lokality, a zvyšuje se tak podíl odpovědnosti samosprávy i občanů samotných.

2.2 Analýza potřeb

Přístup pracovníků Dipartimento di Protezione Civile (Franchina et al., 2009) se dá popsat jednoduchým heslem „*Od potřeb občanů ke zdrojům"*. Služby kritické infrastruktury zajišťují to, co nazýváme „*kvalitou žití*", a existuje tudíž rovnítko mezi funkcionalitou kritické infrastruktury a naplňováním lidských potřeb. Závislost na službách kritické infrastruktury je natolik značná, že se dá s vysokou pravděpodobností předpokládat, že by jedinec v moderní společnosti velmi obtížně zvládal situace vyplývající z dlouhodobějšího nedostatku produktů nebo nedostatečných služeb. Franchina et al. (2009) uvádějí příklad třídenní celostátní stávky italských autodopravců a popisují její dopady na různé společenské funkce.

Franchina et al. (2009) doporučují jako **východisko** plánování ochrany kritických infrastruktur **identifikaci potřeb občanů na základě Maslovowy pyramidy**, rozpoznání a určení **zdrojů na uspokojení lidských potřeb** a nakonec by se mělo postupovat již známým způsobem – v rámci charakteristik každého zdroje analyzovat kritéria závislosti a vzájemné závislosti.

I když detailní metodická dokumentace je na obecné úrovni neveřejná, je možné z přístupu těchto autorů odvodit několik závěrů:

a) Orientace na zdroje (identifikace a hledání) využívá přístupy dodavatelského řetězce (produkce – distribuce – užití) a životní cyklus zdroje (Life Cycle Analysis).
b) Důležitou roli hrají místní zdroje (souvislost s řízením aktiv municipality je zřejmá).
c) Plánování ochrany kritické infrastruktury vyžaduje interdisciplinární přístup syntetizující různá hlediska:
   - **Logistické hledisko:** popis logistických funkcí kritické infrastruktury, toky zboží a služeb v municipalitě.
   - **Právní hledisko:** jaká jsou právní omezení ekonomické činnosti a sociálního chování, jaká jsou pravidla provozu kritické infrastruktury.
   - **Sociologické hledisko:** analýza sociální zranitelnosti, sociální strategie v rámci ochrany kritické infrastruktury.
   - **Územní hledisko:** určení analytických úrovní, prostorová blízkost mezi kritickými infrastrukturami, prostorová charakteristika (dispozice, layout) a dynamika produkce kritické infrastruktury, vztahy municipality s okolím.
   - **Plánovací hledisko:** prostorové určení ekonomických činností, faktory municipality ovlivňující sociální chování, regulační rámec ekonomických činností.

3. Řízení rizik

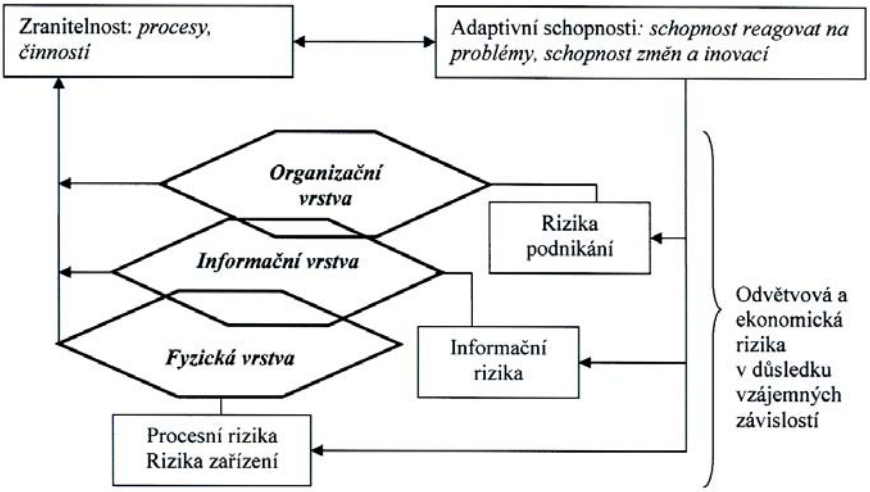
Soukromý sektor jako vlastník převážné části infrastruktury společnosti je také ohrožován různými hrozbami, avšak vydává zdroje pouze na hrozby, jež může zvládat. Jsou to buď hrozby v rámci organizační působnosti podniku, anebo jsou to hrozby zvladatelné na základě právní nebo smluvní dohody. Podnik se sice v rámci dodavatelského řetězce zajímá o vzájemné závislosti, ale nenachází se v postavení, v němž může realizovat kontrolu a ochranná opatření odvětví jako celku. A navíc podniky cítí odpovědnost především vůči akcionářům, nikoliv vůči bezpečnému prostředí se zřetelem na ochranu obyvatelstva.

Z rozdílnosti zájmů veřejné správy a soukromého sektoru vyplývá, že je nezbytné konzistentní a kooperativní partnerství mezi veřejnou správou a vlastníky kritické infrastruktury. Soukromý sektor by měl plánovat životní cyklus aktiv, formulovat směrnice pro přijatelné a tolerovatelné riziko a měl by se zabývat adaptivním řízením pro zkvalitnění služeb kritické infrastruktury vzhledem k bezpečnému prostředí, zdraví a prosperitě. Naopak veřejná správa by měla usnadňovat dialog mezi různými zájmovými skupinami a rozvíjet nástroje a iniciativy podporující systémový přístup, jenž napomáhá vytvoření rámce přijatelného a tolerovatelného rizika. Spojovacím můstkem mezi soukromým sektorem a veřejnou správou by mělo být **periodické stanovení rizik oběma partnery** a **šíření informací o riziku.**

3.1 Řízení rizik podniku[14] – operátor kritické infrastruktury

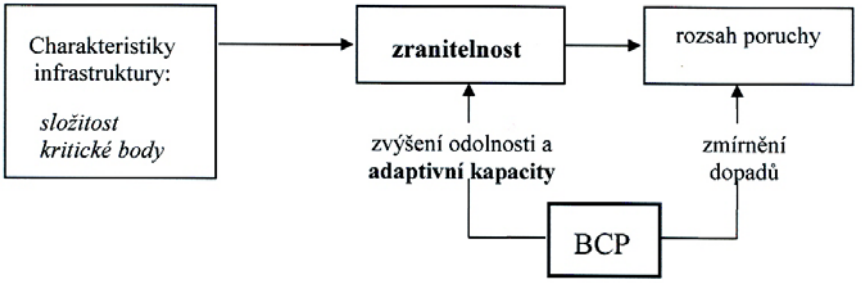
V podnikové praxi je řízení rizik poměrně dobře ukotveno, což dokumentují normy ISO 31000 a tzv. Risk Maturity Model, který hodnotí etapy přechodu od tradičního řízení rizik (zejména finanční rizika), přes integrované řízení rizik (veškerá rozhodování v podniku počítají s riziky) až po celopodnikové řízení rizik (obr. 3).

Podnikové řízení rizik se zabývá riziky jak ve vztahu k podnikání (kritická/strategická rizika pro kontinuitu podnikání), tak riziky v souvislosti s technickou a technologickou úrovní – provozní spolehlivost[15].



Obr. 3
Vztahy mezi podnikovými riziky

Bohužel se opomíjí skutečnost, že podnikové cíle (produktivita a růst) se mohou rozcházet s cíli bezpečnostními, a management podniku by měl přijmout závazek vůči stavu bezpečí (commitment to safety) a kontinuitě podnikání (Business Continuity Planning) (obr. 4).



Obr. 4
Plánování kontinuity podnikání

3.2 Řízení rizik infrastruktury a veřejná správa

Objektivně řečeno, co se týče řízení rizik kritické infrastruktury, tak se veřejná správa nachází v nelehké situaci. Na jedné straně musí, z pozice regulátora, vyžadovat sdílení dat z plánů kontinuity a musí věnovat značnou pozornost podnikovému systému řízení bezpečnosti a rizikům plynoucím z nedostatečné údržby podnikových zařízení, neboť může být ohrožena funkcionalita infrastruktury[16]. Na druhé straně musí průběžně analyzovat kvalitu života obyvatel (komunity) v místních nouzových a krizových situacích a anticipovat jejich potřeby a zabývat se tzv. bezpečnostními externalitami (příloha 2) a institucionálními riziky, které vytváří veřejná správa svým rozhodováním.

Kritická infrastruktura je bezesporu rozsáhlým a složitým systémem a při hodnocení kritické infrastruktury se musí objasnit a dokumentovat nejen prvky a vazby, závislosti a vzájemné závislosti, cíle a omezení, ale je rovněž nezbytné brát zřetel na širší společenská hlediska. To však nelze postihnout jednoduchým modelem nebo skórovací tabulkou, a proto je nezbytné:

A. Rozložit kritickou infrastrukturu do různých funkčních oblastí (okruhů působnosti)

procesy (informační vazby a propojení, poruchy procesů),
produkce – rizika zařízení (procesní propojení a poruchy funkcí),
infrastruktura – rizika infrastruktury (fyzické a regionální propojení, poruchy dodávky produktů a služeb),
odvětví – ekonomická a sociální rizika (regionální propojení).

B. Analyzovat různé koncepty zranitelnosti, které jsou vzájemně vnořené

vnitřní zranitelnost vyplývá z povahy věcí, a kterou nelze odstranit,
zranitelnost jako vztah mezi vnímavostí a schopností zvládat nežádoucí situace,
zranitelnost jako vztah mezi vnímavostí, schopností zvládat nežádoucí situace, expozicí a adaptivní schopností,

vícerozměrná zranitelnost (zranitelnost environmentální, ekonomická, sociální, fyzická a institucionální).

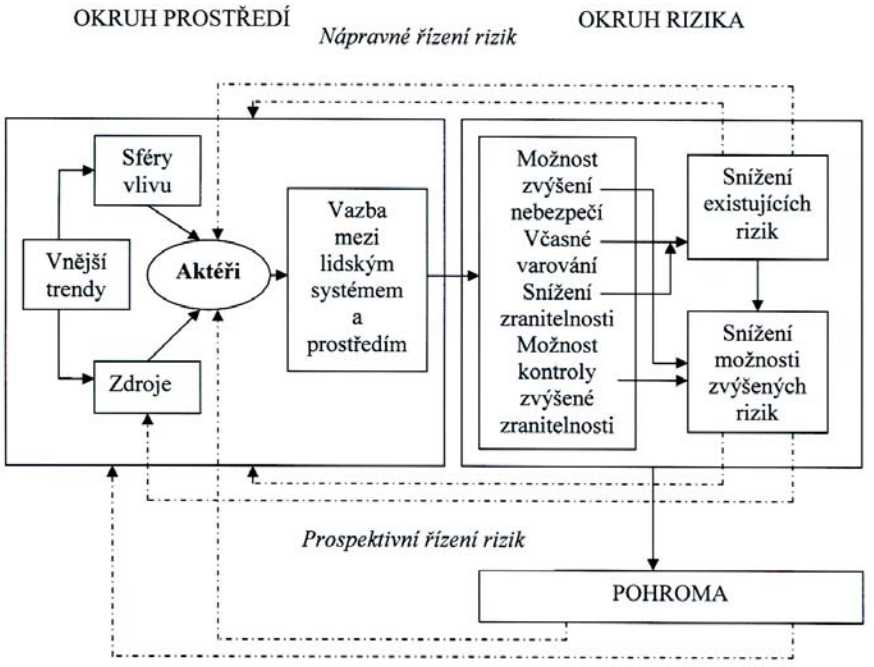
C. Použít komplexnější přístup k řízení rizik (integrované řízení rizik)

Proces stanovení rizika sice využívá standardní otázky „*Co může selhat/co nežádoucího se může stát?, Jak možné/pravděpodobné to je? Jaké jsou následky (škody, ztráty)?"* a vzhledem k tomu, že existuje velká škála metod stanovení a analýzy rizika, mohlo by se zdát, že neexistuje žádný metodický problém. Přesto se dá říci, že určitý metodický problém, vzhledem k povaze kritické infrastruktury, existuje v identifikaci nežádoucích situací a situací selhání – nejde totiž jen o technické poruchy, ale musí se počítat i s institucionálním selháním a selháním sociálního chování lidské komunity. Příloha 2 uvádí stručný informativní popis (detailní hodnocení metod je nad rámec příspěvku) vybraných metod identifikace – modifikovaná What – If analýza, metoda HHM a scénáře.

Na stanovení rizik by měl navazovat proces řízení rizik zabývající se hledáním vhodných opatření (využívají se metody, jako je strom hrozeb, strom problémů, strom hodnot apod.). I proces řízení rizik je v případě ochrany kritické infrastruktury metodicky a organizačně poměrně náročný a je patrné, že oba procesy vyžadují komplexnější přístup.

Příkladem takového přístupu může být GIRO rámec (V***illagran*** de Leon, 2008), který se sice explicitně nevztahuje ke kritické infrastruktuře – vztahuje se spíše k pohromám, může však posloužit jako inspirace pro zformulování podobného rámce výhradně pro kritickou infrastrukturu. GIRO rámec se užívá k analýze vazeb mezi lidskou činností/akcemi, generovanými riziky a pozdějšími pohromami. Skládá se z **okruhu prostředí** (vnější trendy, zdroje, sféry vlivu, aktéři a vazby mezi lidským systémem – společností a prostředím), **okruhu rizika** (zvýšené možnosti nebezpečí, včasné varování, snížení zranitelnosti, kontrola zvýšené zranitelnosti, snížení existujících rizik, snížení nových rizik) a **okruhu pohromy.**

V***illagran*** de Leon (2008) předpokládá, že úspěšné řízení rizik se musí zakládat na systematizaci kořenových příčin, které vedly ke generování rizik nebo k jejich zvýšení, a rovněž předpokládá, že řízení rizik musí brát v úvahu odpovědnost aktérů (instituce, podniky, jedinci apod.) za vytváření či zvýšení rizik. Z GIRO rámce vyplývají dva typy řízení rizik: **nápravné/korektivní** řízení rizik existujících (prevence, zmírnění, připravenost) a **prospektivní řízení rizik** nových nebo vynořujících se rizik, které klade značné nároky na veřejnou správu, takže se nabízí možná souvislost s **risk governance**[17]. Je nad rámec článku detailní analýza a hodnocení GIRO rámce, jehož základní schéma popisuje obr. 5.



Obr. 5
GIRO rámec

4. Závěr

Zpráva Willochovy komise, publikace Luiijfa et al., Franchiny et al. a publikace George Mason University[18] mají jedno společné – nezabývají se notoricky známými věcmi o kritické infrastruktuře a nehledají přesné definice ani „novosti“ za každou cenu. Naopak se snaží **kriticky nahlížet kritickou infrastrukturu z různých hledisek a jejich texty inspirují a vyvolávají otázky vůči naší praxi.**

- ***Willochova zpráva*** se zabývá důsledky zranitelnosti moderní společnosti a klade důraz na organizaci veřejné správy ve vztahu ke kritické infrastruktuře.

Důsledek: Lze předpokládat, že charakteristiky zranitelnosti společnosti neplatí jen pro Norsko, ale platí pro globalizovanou společnost obecně. Možné dopady klimatických změn, problém potravinové soběstačnosti, možný Peak oil atd. jsou příklady, které by se neměly chápat jako alarmistické, ale měly by se věcně analyzovat z hlediska možného vývoje dopadů na společnost. A pokud se

neprokáží negativní dopady, tím lépe, ale musí se prokázat odbornou expertizou, nikoliv jako nepodložená politicky zbožná přání. Naskýtá se proto otázka, zda **ochrana kritické infrastruktury by neměla mít strategickou úroveň**, která by se zabývala globalizačními trendy a analyzovala je z hlediska jejich dopadů na různé úrovně společnosti a která by rovněž byla odpovědná za odbornou úroveň metodické a odborné podpory pro všechny úrovně veřejné správy.

Návrh Willochovy komise na reorganizaci veřejné správy by měl vést k otázce, zda by nebylo vhodné se zamyslet nad organizací veřejné správy ve vztahu ke kritické infrastruktuře z pohledu již rozpracovaných konceptů, jako jsou koncepty tzv. organizačních havárií – Organisational Accident (většinu havárií způsobuje lidský faktor v rámci organizační struktury a styl rozhodování) a tzv. vysoce spolehlivé organizace – High Reliability Organisation (zjednodušeně řečeno, jsou to organizace, které jsou odolné vůči nepříznivým jevům a problémy řeší účelnými mechanizmy).

- Publikace ***Luiijfa et al***. se zabývá sice stručně, leč výstižně stavem znalostí veřejné správy, protože bez znalostí nelze rozhodovat a řídit.

Důsledek: Publikace vyvolává otázku na **odbornou a znalostní úroveň naší praxe ochrany kritické infrastruktury – zda znalosti jsou na odpovídající úrovni, jak to vyžaduje složitost ochrany kritické infrastruktury.** Pakliže znalosti nejsou na odpovídající úrovni, mělo by se zjišťovat, proč tomu tak je, jelikož v teoretické rovině existuje mnoho metod, které se však v praxi běžně nepoužívají. Problém znalosti také implikuje otázku na obsahovou náplň nástrojů, dokumentace a mechanizmů organizace a řízení ochrany.

- Z textu ***Franchiny et al***. vyplývá, že na prvním místě jsou lidské potřeby.

Důsledek: Je třeba počítat i s monitorováním, kvantifikací a hodnocením **sociální zranitelnosti,** která úzce souvisí s lidskými potřebami podle Maslovowy pyramidy, ale pro potřeby praxe není metodicky rozpracována. Navíc koncept sociální zranitelnosti se prolíná s jinými koncepty, o nichž se sice píše, ale nejsou „algoritmizovány" pro potřeby praxe. Jedná se o koncepty **bezpečné komunity**, **resilientní komunity** a **lidského bezpečí**. Jinak řečeno, v souvislosti s lidskými potřebami a jejich naplňováním v krizových a nouzových situacích je žádoucí zabývat se vztahy odolnosti, sebespoléhání a soběstačnosti. Publikace George Mason University je dokladem, že se odborná veřejnost **kriticky** zamýšlí nad problémy ochrany a resilience, jak lze vidět z tabulky ze zmíněné publikace.

Tabulka 1
Vztahy mezi ochranou a resiliencí

	OCHRANA	RESILIENCE
Plánované činnosti	Posilování struktury	Rekonstrukce procesů
Zaměření na	Aktiva	Služby
Požadované metriky	Absolutní	Podmíněné
Hodnotová orientace na	Náklady	Přínosy
Přístup k bezpečnosti	Reaktivní	Proaktivní
Typy poruch	Náhlé poruchy	Pozvolná degradace
Rozpočet	Krátkodobé investice	Dlouhodobé investice
Systémové interakce	Lineární	Nelineární
Systémové vazby	Uvolněné	Těsné

Sociální zranitelnost rovněž vyvolává potřebu diskuse problémů **přežití** (existuje hnutí nazývající se survivalismus) **a kolapsů**, poněvadž z některých závěrů historických analýz vyplývá, že existuje životní cyklus společnosti – společnosti vznikají, rozvíjejí se a pak kolabují.

V souvislosti s **přežitím** je nutné upozornit na to, že v rámci ochrany kritické infrastruktury se věnuje malá pozornost problému **udržitelnosti** infrastruktury (souvislost s udržitelným rozvojem) a **zelené infrastruktuře**, což je koncept zdůrazňující důležitost přírodního prostředí pro život podporující funkce.

Orlov[19] popisuje 5 fází možného **kolapsu** moderní společnosti: 1 fáze finanční kolaps, 2. fáze hospodářský kolaps, 3. fáze politický kolaps (kolaps veřejné správy), 4. fáze sociální kolaps, 5. fáze kulturní kolaps. I když se tyto fáze kolapsu vztahují ke společnosti jako celku, lze si dost dobře představit, že by se vyskytovaly i v menším měřítku v případě dlouhodobé nefunkčnosti kritické infrastruktury.

V praxi se někdy stává, že převládá byrokratické myšlení nad myšlením kritickým a tak se sice volá po novosti výsledků pro ochranu kritické infrastruktury, avšak opomíjí se skutečnost, že nové výsledky vznikají jen systematickým výzkumem, který by se měl zaměřit například na:

- teoretické a výpočetní modelování zranitelnosti složitých systémů včetně predikce extrémních jevů,
- nástroje hodnocení lidské zranitelnosti a na modelování dopadů na přírodní a vytvořené prostředí,
- účelné a účinné řídící struktury, strategie a operace pro normální stavy a pro stavy extrémní události,
- podporu proaktivního rozhodování pro složité a neurčité situace,
- technickou podporu kritické infrastruktury (senzory jako nervový systém kritické infrastruktury).

Résumé

Public administration should protect people from any serious and lasting consequences of the failure to infrastructure services, supplying such necessities as water, food, energy etc. It is crucial to understand how the system works and how to analyze it; possible failures and disruptions should be repeatedly analyzed and forecasted. Public sector and private sector have often different interests and thus there must be consistent and mutual partnership between those two sectors. A common platform for those two sectors might be the time sharing fixing risks and more public information concerning the possible risks. The public sector will never be able to work without infrastructures and therefore it has to become more familiar with the business culture. However the public sector needs to be prepared to keep people safe.

The article briefly describes LCCI and SoS concepts, which in its consequences lead to the necessity of systematic approach and as an example of the systematic approach a GIRO framework is stated. The article also highlights requirement to identify human needs, which are fulfilled by the services of critical infrastructures. Therefore it is important to formulate strategy of protection from various aspects (logistical, territorial, social, planning aspect, etc.). Needfulness to deal with the municipal (decentralized) infrastructures is also emphasized.

The risks analysis of the nationwide and regional infrastructures is very complicated. We must look at that from the broad point of view, utilizing technical, social and environmental approach, and then implement those approaches into the Risk Filtering, Ranking and Management method, modified What-If analysis and scenarios.

At the end of the article, questions are asked concerning level of professional knowledge, organization and management; direction of research is also suggested.

POZNÁMKY:

[1] Mezi lidmi a infrastrukturou společnosti jakéhokoliv typu je **vzájemný vztah**. Lidé potřebují infrastrukturu, protože bez služeb, které poskytuje, by každodenní život byl trpkým údělem. Naopak infrastruktura potřebuje lidi, protože bez jejich přičinění by byla infrastruktura neudržitelná a nerozvíjela by se.

[2] *Critical Foundation, Protection America´s Infrastructure,* The Report of the President´s Commission on Critical Infrastructure Protection, October 1997.

[3] Tato definice ještě postrádá zmínku o tom, že moderní společnost čím dál tím více závisí na informační infrastruktuře - kritická informační infrastruktura.

[4] Odvětví: *zemědělství a výroba potravin, voda, energetika, doprava, telekomunikace, bankovnictví, chemické a nebezpečné látky, zdravotnická zařízení, záchranářský systém* apod. Do klíčových aktiv (objektů) obvykle náleží: *jaderná zařízení, přehrady, vládní zařízení, národní památníky a symboly apod.*

[5] **Resilience (pružná odolnost) infrastruktury** je schopnost snížit závažnost a/nebo trvání účinků poruchy a znamená anticipaci, absorbování, přizpůsobení a zotavení se z poruchy.

Rozdíl mezi odolností a pružnou odolností spočívá především v pružnosti a mechanizmech přizpůsobivosti, které jsou vlastní pružné odolnosti. Z praktických důvodů se v dalším textu používá pojem resilience.

[6] **Komplexní systém** je systém složený ze vzájemně propojených částí, které jako celek projevují jednu nebo více vlastností, které nejsou zřejmé z vlastností jednotlivých částí.
Komplexní adaptivní systém je speciálním případem komplexního systému. Komplexnost spočívá v rozmanitosti, protože systém je složený z mnoha navzájem propojených prvků a adaptivita (přizpůsobivost) je výrazem schopnosti změny a učení se ze zkušenosti a souvisí s decentralizací a přežitím. Problémem přizpůsobivosti sociálních systémů je odpor člověka ke změnám.

[7] **Funkcionalita** je „účelová zaměřenost", funkčnost je zhruba „schopnost vykonávat funkci".

[8] **Kaskádní porucha** znamená, že porucha v jednom prvku/systému/infrastruktuře je příčinou poruchy nějaké entity (prvek, jednotka, subsystém, systém) v jiném systému/infrastruktuře, což má za následek její nefunkčnost.
Eskalující porucha vyjadřuje situaci, v níž existující porucha v jednom prvku/systému /infrastruktuře zhoršuje parametry poruchy v jiném prvku/systému/infrastruktuře.
Společná porucha se vyskytuje, když dva nebo více prvků/systémů/infrastruktury jsou současně v poruše a poruchy mají obdobnou příčinu.

[9] **Rozsáhlý** systém je územně rozprostřený a složitý systém se vyznačuje mnoha vzájemně propojenými prvky s četnými interakcemi a jeho chování je emergentní.

[10] Neexistuje čistě technický systém z podstaty. Každý technický/technologický systém je v nějaké interakci s lidmi na nějaké činnosti: *Technický systém (materiály, zařízení, transformační podmínky) →ÚKOL← Sociální systém (pracovníci, pracovní vztahy, rozhodovací procedury).*

[11] **Interoperabilita** je schopnost různých systémů vzájemně spolupracovat, poskytovat si služby, dosáhnout vzájemné součinnosti.

[12] Míra závislosti má vliv na spolehlivost. Pět systémů s osmdesátiprocentní spolehlivostí vytvoří kombinovaný systém se spolehlivostí třicet tři procent.

[13] Příkladem dobrého vztahu mezi veřejnou správou a vlastníky kritické infrastruktury je Nový Zéland.

[14] Riziko se nechápe jen ve vztahu k hrozbám, riziko je také příležitost, jejíž výsledky jsou sice nejasné, ale příležitost by se měla využít (tzv. apetit k riziku).

[15] Provozní spolehlivost se charakterizuje spolehlivostí *(reliability)*, připraveností poskytovat služby *(availability)*, udržovatelností/údržbou *(maintainability)*, bezpečností vůči okolí *(safety)* a ochranou před nežádoucími vlivy okolí *(security)*.

[16] Neměla by se věnovat pozornost jen haváriím, nýbrž pozornost si zaslouží tzv. „near-miss" (těsně vedle, o vlásek) incidenty, u nichž je možnost zlepšit bezpečnostní opatření před možnou havárií. Podle Wikipedie pojem „near-miss" vyjadřuje **neplánovanou událost, která sice nevedla ke škodám na životech, zdraví, prostředí a majetku, avšak událost má škodlivý potenciál a jen souhra šťastných okolností zabránila jeho projevu.**

[17] O. Renn, (2008): *Risk: Governance Coping with Uncertainty in a Complex World,* Earthscan Publications Ltd.

[18] *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience,* CIP Program, Discussion papers, George Mason University, 2007.

[19] http://cluborlov.blogspot.com (nebo wikipedia).

[20] *Kritičnost je relativní míra důsledků četnosti výskytu typů poruch a selhání (www.bizmanualzcom).*
Kritičnost vyjadřuje podmínky popisující přechod mezi kvalitativně odlišnými stavy (www.esse.ou.edu). Kritičnost je stav značné naléhavosti (http://wordnet.princeton.edu).
Z definic kritičnosti se dá vyvodit, že se jedná o **prahovou hodnotu**, která může být

projektově stanovena a může se vztahovat k události, parametru procesu/funkce, typu poruch a odolnosti.

[21] Pojem **hierarchické** vyjadřuje nutnost pochopit rizika a jejich projevy na různých úrovních – co na různých úrovních může selhat. Výsledkem je makroskopické riziko (riziko na vyšších úrovních) a mikroskopické riziko (riziko nižších úrovní).
Pojem **holografické** je metaforou pro potřebu přistupovat k riziku z různých pohledů – pohled technický, ekonomický, sociální, environmentální, politický, bezpečnostní, územní atd.

[22] **Redundance** je schopnost prvků systémů přejímat funkce prvků v poruše, **robustnost** se týká necitlivosti výkonnosti systému vůči vnější zátěži, **resilience** je schopnost zotavit se z nouzového stavu.

Literatura

[1] AUERSWALD, P., BRANSCOMB, M.L., LAPORTE, M.T. a MICHEL-KERJAN, E. *The Challenge protecting Critical Infrastructure.* Pensylvannia: Wharton School of University of Pensylvannia, Center for Risk Management and Decision Processes, Working Paper 05-11, 2005.

[2] BOLOGNA, S. a BEER, T. *An Integrated Approach to Survivability Analysis of Large Komplex Critical Infrastructures,* INFORMATIK 2003 „Sicherheit-Schuzt und Zuverlassigkeit“, Frankfurt am Main, 2003.

[3] FRANCHINA, L., CARBONELLI, M., GRATTA, K.L., PETRICCAO, C. a PERUCCHINI, D. *Dall´analisi alla protezione delle infrastrutture critiche*, Rivista La comunicazione - note, recensioni e notizie, Istituto superiore delle communicazioni e delle technologie dell´informazioni, 2009.

[4] GORDON, K. a DION, M. *Protection of Critical Infrastructure' and the Role of Investment Policies relating to National Security.* Paris: OECD, 2008.

[5] HAIMES, Y.Y., KAPLAN, S. a LAMBERT, J.H. Risk Filtering, Ranking and Management using Hierarchic Holographic Modeling. *Risk Analysis*, 2002, vol. 22, no. 2.

[6] LEWIS, G.T. a DARKEN, R. Potholes and Detours in the Road to Critical Infrastructure Protection. *Homeland Security Affairs*, 2005, vol. 1, no. 2.

[7] LUIIJF, H.A.M. a KLAVER, M.H.A. Critical Infrastructure Awareness required by Civil Emergency Planning. In *Proceedings 1st IEEE Workshop on Critical Infrastructure Protection*, Darmstadt: Germany, 2005. ISBN 0-7695-2426.

[8] MAIER, M. Architecting Principles for System of Systems. *INCOSE System Engineering Journal*, 1998, vol. 1, no. 4.

[9] TOLONE, J. W., SEOK-WON LEE, NING XING, MCNALLY, K.R. a SCHUMPERT, T. Effective Scenario Composition for the Revelation of Blind Spots in Critical Infrastructure. *First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, New Hamsphire, 2007.

[10] VILLAGRAN DE LEON, J.C. *GIRO – The Integral Risk Management Framework: An overview.* Working Paper No. 6., UNU-EHS, 2008.

Příloha 1 – Analytické charakteristiky infrastruktury

Tabulka 2
Charakteristiky infrastruktury – příklad

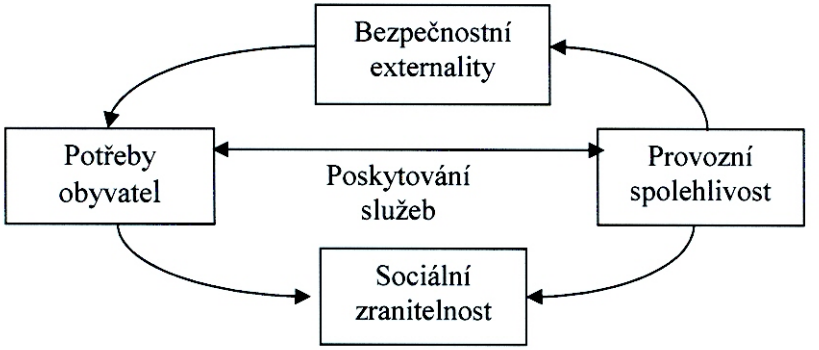
Charakteristiky infrastruktury		Energetika	Doprava	…..
SLOŽITOST	Fyzická			
	Organizační			
	Rychlost změn			
ZÁVISLOSTI	Na jiné infrastruktuře			
	Pro jinou infrastrukturu			
	Vnitřní závislost			
	Informační závislost			
ZRANITELNOST	Vnější vlivy			
	Technické/lidské selhání			
	Systém řízení			
	Napadení ICT			
	Teroristický cíl			
TRH (ekonomické prostředí)	Míra liberalizace			
	Přiměřenost regulace			
	Rychlost změn			
PROSTŘEDÍ (přírodní, sociální)	Dostupnost zdrojů			
	Bezpečnost prostředí			
	Urbanizace			
	Postoje veřejnosti k rizikům			
KRITIČNOST[20] *(faktory)*	Působnost			
	Závažnost dopadů			
	Časové účinky			
	Bezpečnostní externality			

Příloha 2 – Bezpečnostní externality, modifikovaná What - If analýza, Risk Filtering, Ranking and Management, scénáře

- **Bezpečnostní externality**

Externalitou se v ekonomické teorii označují situace, kdy činnost jednoho subjektu nepřímo ovlivňuje jiné subjekty, respektive přenáší na jiné subjekty náklady, aniž tyto jiné subjekty dostanou řádnou kompenzaci. Ochrana obyvatel například řeší **negativní externality** (zdravotní újmy v důsledku různých havárií). Kromě toho existují **pervasivní (trvalé) externality** mající charakter globálních rizik – například klimatické změny.

Specifické postavení má **bezpečnostní externalita**, která se objevuje v publikaci Auerswald et al. (2005). Bezpečnostní externalita je odvozena ze spoléhání se na systém řízení bezpečnosti v rámci dodavatelského řetězce veřejných služeb.



Obr. 6
Vztahy v poskytování služeb a bezpečnostní externalita

- **Modifikovaná What-If analýza**

Metoda je sice „zaškatulkována“ v souboru metod Preliminary Hazard Analysis, to by však nemělo bránit tomu, aby se využil její potenciál k identifikování **kritických podmíněných** situací (Co by se stalo – kdyby) na základě zkušeností a představivosti experta. Modifikovaná What-If analýza existuje ve dvojí podobě – reaktivní a preventivní.

Reaktivní What-If analýza se realizuje v případě zjištění kritických podmínek v systému. Cílem je, aby se systém co možná nejrychleji „vzdálil“ z těchto kritických podmínek.

Preventivní What-If analýza se zabývá kritickými podmínkami, které odhalila periodická predikce a navrhuje akce v různých časech. Je však nutno

připomenout, že každá predikce je zatížena nejistotou a neurčitostí, a proto existuje riziko chyby I. a II. typu.

Předpokládejme, že předpověď se chápe jako testování hypotéz. Testuje se, zda existuje dost důkazů proto, aby nulová hypotéza H_0 (kritické podmínky se budou v čase t_i v systému vyskytovat) byla přijata či odmítnuta:

	H_o je pravdivá	H_o je nepravdivá
Predikce zjistila kritické podmínky		Přijetí H_0 – chyba II. typu
Predikce nezjistila kritické podmínky	Odmítnutí H_0 – chyba I. typu	

- **Risk Filtering, Ranking and Management (**Haimes et al., 2002)

Metoda slučuje praktiky stanovení rizika a řízení rizik do jednoho postupu. Výchozím bodem metody je **Hierarchické Holografické**[21] **Modelování** (HHM) identifikující všechny zdroje rizika a rizikových faktorů z mnoha hledisek, což je případ kritické infrastruktury. Výstupem z HHM však může být značné množství scénářů rizika, které je třeba kriteriálně filtrovat a uspořádat tak, aby bylo možné se soustředit na nejkritičtější a nejdůležitější variantu. K tomu se využívá metoda Risk Filtering, Ranking and Management, která se používá dvoustupňovým způsobem. Nejprve se aplikují kroky 1 až 4 na systémové úrovni a posléze se z kroku 4 přechází do kroku 1 na úrovni specifikace aktiv infrastruktury.

Kroky postupu RFRM s využitím HHM:

Krok 1: Identifikace scénářů s využitím Hierarchical Holographic Modeling (HHM)

Zdroje rizik se identifikují jednak ve scénáři, jenž popisuje zkoumaný systém tak, jak byl **naplánován/naprojektován** (jaký současně je) pomocí otázky „*Co může selhat/co nežádoucího se může stát",* jednak ve scénáři **úspěšného fungování** systému. HHM vytváří diagram zobrazující kritéria úspěšného fungování systémů z mnoha pohledů. Detailní sestavení HHM je časově náročné, takže je třeba nalézt vhodný kompromis mezi detailem, správností a přesností.

Krok 2: Filtrování scénářů na základě rozsahu analýzy a úrovně rozhodování

Filtrování vyžaduje určité odborné znalosti a zkušenosti se zkoumaným systémem.

Krok 3: Kriteriální filtrování a uspořádání

Většinou se využívá klasická matice rizika (pravděpodobnost a závažnost důsledků).

Krok 4: Multikriteriální hodnocení

V tomto kroku se analyzují scénáře z hlediska *resilience, robustnosti* a *redundance*[22] nebo z hlediska systémové analýzy provozní spolehlivosti.

Při hodnocení se využívají tato kritéria (podle potřeby se seznam může změnit a přizpůsobit) na definované škále intenzity:

- **Nezjistitelnost** (neexistují způsoby jak zjistit počáteční událost scénáře předtím, než se realizují škody),
- **Neovladatelnost/neřiditelnost** (není možné preventivně zabránit škodám),
- **Existence více způsobů vedoucích k selhání/poruše** (naznačuje se, že existuje více způsobů vzniku poruch/selhání, z nichž některé mohou být neznámé),
- **Nevratnost** (nežádoucí podmínky neumožní návrat do stavu před událostí),
- **Trvání nežádoucích účinků**,
- **Kaskádní účinky**,
- **Provozní prostředí** (navrhují se scénáře pro důsledky vnější zátěže/stresorů),
- **Opotřebování** (uvádí se scénáře popisující zhoršenou výkonnost),
- **Hardware, software, organizační rozhraní** (nežádoucí účinky se zvyšují na rozhraní různých subsystémů),
- **Složitost/emergentní chování**,
- **Nevyzrálost návrhu/konstrukce**.

Krok 5: Kvantitativní uspořádání

Ke kvantifikaci možnosti výskytu scénáře se využívá Bayesovský vzorec nebo Bayesovská síť.

Krok 6: Volby pro řízení rizik

V tomto kroku se řeší účinnost, účelnost (jak se sníží riziko) a nákladovost různých variant v kontextu otázky *„Co by se mělo udělat?“*.

Krok 7: Ochrana a zabezpečení kritických prvků

Krok 8: Provozní/operační zpětná vazba na realizaci kroků 6 a 7

- **Scénáře** (Tolone et al. 2007)

Scénář se chápe jako most spojující analytický proces plánování s kognitivním aparátem, jenž rozprostírá myšlení do širší perspektivy. Scénář ochrany kritické infrastruktury se uskutečňuje v těchto krocích:

Krok 1: Plánování

Hledají se odpovědi na otázky:

- Jaký je záměr scénáře? (stanovení zranitelnosti, podpora rozhodování apod.)
- Jaké jsou doprovodné jevy a události?
- Jaký je rozsah scénáře (funkční, časový, prostorový, infrastrukturní)?
- Jaké jsou cíle scénáře v rámci deklarovaného záměru?

Krok 2: Sběr dat a analýza dat

V rámci tohoto kroku se formuluje řada možných událostí a ke každé události se přiřazují známé bezprostřední a kumulativní účinky, popisuje se kauzální vazba mezi událostí a důsledky a časový rámec iniciace události, analyzují se územní vlastnosti participujících infrastruktur a nakonec se předvídají další bezprostřední a kumulativní účinky každé události.

Krok 3: Sestavení scénáře

Všechny informace o infrastrukturách se sestavují do formátu, který vyjadřuje budoucí stavy a situace a je syntézou prostorové a funkční reprezentace vazeb tak, aby se vytvořila narativní forma scénáře. Ve scénáři by se měl zvažovat kompletní rejstřík iniciačních událostí, kterými obvykle bývají poruchy, které se klasifikují následovně:

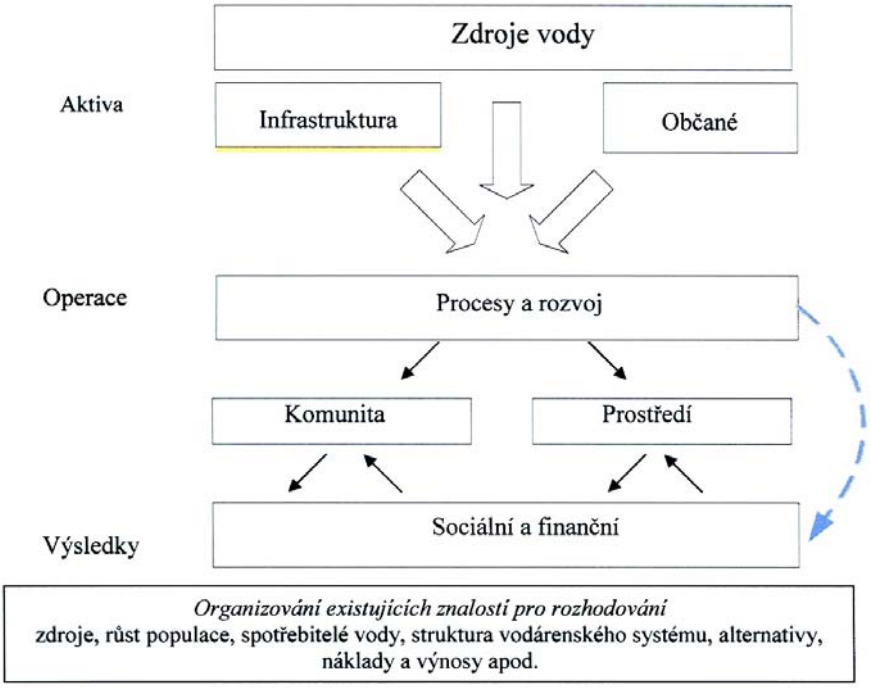
- Typ 1: Jedna událost (porucha) v jedné lokaci vypíná/narušuje funkci jedné důležité charakteristiky infrastruktury.
- Typ 2: Jedna událost (porucha) v jedné lokaci vypíná/narušuje funkce většího počtu důležitých charakteristik infrastruktury.
- Typ 3: Vícečetné, simultánní události (poruchy) typu 1 nebo 2.
- Typ 4: Vícečetné, časově rozložené události (poruchy) typu 1, 2, 3.

Krok 4: Vyhodnocení a úpravy scénáře

Každý scénář by se měl analyzovat a zhodnotit z hlediska vnitřní soudržnosti na základě otázek, jako jsou například otázky „Vyplývá budoucí situace logicky z toho, co je známo?, Jsou kauzality správně identifikovány a správně zahrnuty do scénáře?, Je budoucí situace na základě iniciační situace a klíčových nejistot hodnověrná?“.

Krok 5: Verifikace a validace scénáře

Příloha 3 – Příklad řízení municipální infrastruktury – zdroje vody



Obr. 7
Schéma řízení zdrojů vody lokality

Zabezpečení vody (water security) se týká ***udržitelného užívání*** *zdrojů vody a jejich* ***ochrany*** *proti hrozbám, jako jsou povodně a sucha,* ***zajištění*** *přístupu k vodě pro lidi a prostředí a* ***udržitelného rozvoje*** *systému vodních zdrojů.*