Manažérstvo životného prostredia 2015 ♦ Management of Environment´2015
Zborník z XV. medzinárodnej vedeckej konferencie, 17. - 18. apríl 2015, Bratislava
Proceedings of the 15th International Conference, Bratislava, April 17-18, 2015
Žilina: Strix. Edícia ESE-23, ISBN 978-80-89753-02-4 ■ Rusko, M.-Harangozó, J. [Eds.] ■

# BEZPEČNOST SLOŽITÝCH KRITICKÝCH TECHNOLOGICKÝCH ZAŘÍZENÍ

**Dana PROCHÁZKOVÁ - Jan PROCHÁZKA**

# SAFETY OF COMPLEX CRITICAL TECHNOLOGICAL FACILITIES

***ABSTRAKT***
*Předložená práce pojednává o bezpečnosti složitých technologických objektů a infrastruktur, které chápe jako socio-technologické systémy systémů. Předmětné systémy musí podporovat životy lidí a nesmí je ohrožovat, ani při svých kritických podmínkách. Koncept jejich bezpečnosti je vytvořen na základě propojení přístupu All-Hazard-Approach, konceptu Defence-In-Depth (ochrana do hloubky) a kultury bezpečnosti. Systém řízení bezpečnosti sledovaných technologických systémů pokrývá řadu oblastí, a to technickou, vojenskou, legislativní, kybernetickou, finanční, ekonomickou, sociální, ekologickou, vzdělávací, výzkumnou, atd. Úkoly v oblasti bezpečnosti, na základě současných znalosti a současného pojetí důmyslných bezpečnostních systémů, mají všichni účastníci. Úkoly jednotlivých zúčastněných a jejich propojení v různých situacích musí být stanoveny zákony, standardech a normách.*
***Klíčová slova:*** *riziko; bezpečnost; složité systémy; All-Hazard-Approach; Defence-In-Depth.*

***ABSTRACT***
*The paper deals with the safety of complex technological buildings and infrastructures that understand as the socio-technological systems of systems. These systems need to support the human lives and cannot threaten them at their critical conditions. The concept of their safety is created by the interface pf All-Hazard-Approach, Defence-In-Depth concept and safety culture. The safety management system of followed technological systems covers a lot of domains, namely technological, military, legislative, cyber, financial, economic, social, ecological, educational, research etc. Tasks in domain of safety on the basis of present knowledge and present idea of sophisticated security systems have all participants. Tasks of individual stakeholders and their interconnections at different situations need to be stipulated in legal acts, standards and norms.*
***Key words:*** *risk; safety; complex systems; All-Hazard-Approach; Defence-In-Depth.*

## 1. Úvod

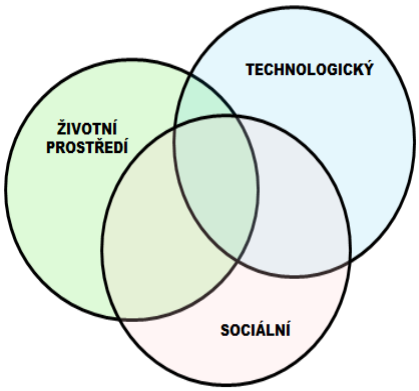
V současné době se v souvislosti se zajištěním bezpečí a dalšího rozvoje pro lidskou společnost stále častěji diskutuje problematika kritických aktiv, kterými jsou kromě lidí, životního prostředí a přírodních zdrojů, majetku, veřejného blaha, i kritické objekty a kritické infrastruktury, které představují složité socio-technologické systémy, a proto se předmětná práce zabývá jejich bezpečností. Předmětné složité socio-technologické systémy jsou důležité pro život lidí v současném světě, a to za normálních, abnormálních i kritických podmínek, a budou důležité i v budoucnu. Cílem odborníků, pracujících na podpoře veřejného zájmu, je zavádět do praxe jen bezpečné složité technologické objekty a infrastruktury, tj. systémy, které jsou zabezpečené jak vůči všem vnějším i vnitřním pohromám, a to včetně lidského faktoru, tak i pohromám, které jsou spojené s vnitřními vazbami a toky, a s propojeními s jejich okolím, a zároveň neohrožují ani sebe, ani své okolí. Jejich modelem je otevřený systém vzájemně propojených systémů, nazývaný systém systémů (zkráceně SoS).
Z hlediska současného poznání [1] jsou základními problémy praxe dále uvedené úkoly:

- Popis a charakteristika systému, který má více chráněných aktiv chápaných systémově, mezi kterými existují vazby různé povahy (fyzikální, kybernetické, sociální, organizační) a probíhají různé toky materiálové, energetické, informační apod.
- Popis a charakteristika souboru vzájemně propojených systémů.
- Odolnost, zranitelnost a adaptabilita jednotlivých systémů i celého systému systémů. Kdy (při jaké kombinaci vlastností) je systém bezpečný a udržitelný, tj. kdy má schopnost se dále rozvíjet?
- Určení integrálního rizika, protože v systému je více chráněných aktiv, která jsou propojená vnitřními vazbami a spřaženími a jejich cíle jsou v řadě případů konfliktní.
- Vztahy mezi riziky dílčími, integrovanými a integrálním rizikem systému.
- Vztahy mezi integrálním rizikem systému systémů a integrálními riziky dílčích systémů.
- Kritéria pro integrální bezpečnost systému systémů (soubor bezpečných systémů nemusí být bezpečný, protože existují vnitřní propojení stálá a občasná, tj. propojení, která nastávají jen za jistých podmínek, a jsou příčinou emergentních, tj. náhle se objevujících jevů, které poškozují veřejná chráněná aktiva) a pro zajištění jejich interoperability.
- Zásady pro řízení bezpečnosti systému systémů v dynamicky proměnném světě (nutné pro provoz kritických objektů i kritických infrastruktur).
- Legislativa pro podporu řízení bezpečnosti systému systémů.
- Kontrolní mechanismy pro monitorování úrovně bezpečnosti kritických systému systémů.

Nezbytným předpokladem pro řešení problémů je tudíž používání systémového myšlení a aplikace nejnovějších poznatků a zkušeností.

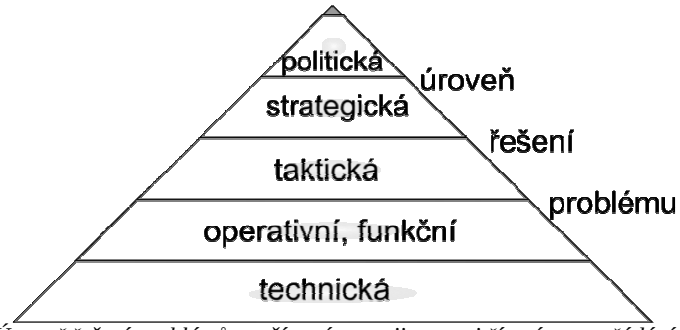
**2. Bezpečnost složitých kritických systémů**

Zásadním problémem existence bezpečného světa s ohledem na potřeby lidí je koexistence uvedených systémů v podobě, která zajistí existenci, bezpečí a rozvoj lidí, obrázek 1. V postavení, kdy člověk je pouze součástí existujícího světa, může pouze regulací svého chování a svých činností zamezit tomu, aby on sám jen v omezené míře přispíval k narušení příznivých podmínek pro svůj život. Jde o koncept, který na základě odborného poznání prosazuje jak pokroková odborná sféra, tak významné instituce, jako jsou OSN [2] a EU [3]. Předmětný aspekt autorka sleduje dále požadavkem, že člověk, jako tvůrce a provozovatel složitých technologických systémů, tj. objektů a infrastruktur, musí zajistit, aby složité technologické systémy byly bezpečné, a proto musí: odvracet dopady pohrom (tj. nepříznivých jevů) na sebe i na technologické systémy (objekty a infrastruktury) tak, aby udržel příznivé podmínky pro svůj život; a přitom dbát na to, aby konstruoval systémy bezpečně.




*Obr. 1: Prostor pro život lidí, lidský systém, je systém systémů [4] vzniklý propojením základních tří systémů, které člověk potřebuje pro svoji existenci*

Předmětem práce jsou složité technologické systémy, které člověk vytvořil a provozuje, tj. výstižnější název je socio-technologické systémy. Předmětné systémy ve formě objektů, zařízení a infrastruktur na jedné straně poskytují lidem výrobky a služby, které potřebují ke kvalitnímu životu a které jim též umožňují přežít za kritických situací, a na druhé straně je ohrožují jak svou činností, tak nebezpečnými látkami, které zpracovávají, a někdy i svými výrobky, které obsahují látky, jež ohrožují zdraví konzumentů anebo dokonce i zdraví příštích generací [5]. Proto je důležitá problematika řízení jejich bezpečnosti, která je dále sledována. Je si třeba uvědomit, že složitými systémy jsou de facto všechny existující objekty a infrastruktury kolem nás s tím, že v některých časových a prostorových měřítcích lze složitost (komplexnost) zanedbat a pro řešení praktických úloh použít jednoduché představy. ***Systémy, které jsou pro lidi životně důležité, se označují pojmem kritické systém*** [6].
Je skutečností, že o bezpečnosti složitých technologických objektů a infrastruktur se rozhoduje na mnoha úrovních, obrázek 2. Faktická opatření podporující bezpečnost se dělají na úrovni technické a jejich účinnost dosahuje až 80%, a na úrovni funkční, kde jejich účinnost dosahuje až 40% [7]. Pro aplikaci účinných opatření je nutno vhodné klima, protože opatření jsou náročná na zdroje, síly a prostředky, tj. je třeba podpora od řídících úrovní.
Dále stručně shrneme současné poznatky o bezpečnosti složitých technologických objektů a infrastruktur a ukážeme cesty, kterými se předmětná problematika řeší [1]. Koncept je založen na propojení přístupů All-Hazard-Approach [8] a Defence-In-Depth [9], přičemž All-Hazard-Approach je založen na seznamu pohrom, jejichž seznam je v práci [10].




*Obr. 2: Úrovně řešení problémů používané v teorii a praxi řízení a vypořádání rizik*

Při výkladu problematiky autoři vychází z pojetí, že každá technologie představuje soubor znalostí, které řeší určitý problém, tj. uspokojují požadavky, kterými jsou užitečnost, disponibilita a bezpečnost, a z principů systémového inženýrství, tj. z cíleně orientovaného procesu, který je založen na propojení řady disciplín a zacílen na tvorbu a provoz bezpečného systému, který plní určité lidské potřeby, které velmi dobře definoval Maslow [11]. Bezpečný systém je chápán jako systém, který je zabezpečen vůči všem vnitřním a vnějším pohromám, tj. všem škodlivým jevům, a který ani při svých kritických podmínkách neohrožuje sebe a své okolí, tj. prostor, ve kterém žijí lidé [6]. To znamená, že ***bezpečnost systému*** je vlastnost systému, která je nadřazena spolehlivosti. Proto parametry, které určují kvalitu systému, jsou uspořádány do pořadí:

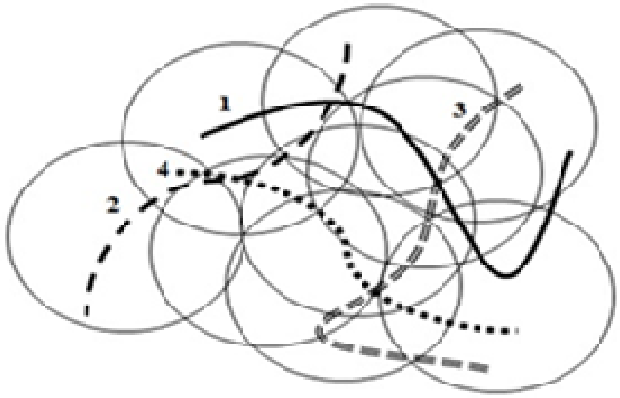
- *bezpečnost*, tj. schopnost systému předcházet kritickým stavům systému (aktivní bezpečnost využívá prvky řízení; pasivní bezpečnost využívá ochranné prvky) a při jejich výskytu neohrozit existenci ani sebe, ani svého okolí,
- *spolehlivost*, tj. schopnost sytému poskytovat požadované funkce za daných podmínek, v dané kvalitě a v daném časovém intervalu,
- *dostupnost*, tj. schopnost systému poskytovat požadované funkce při výskytu procesu, který danou funkci využívá,
- *integrita*, tj. schopnost systému poskytovat časově korektní a platná hlášení uživatelům o poruchách systému,
- *kontinuita*, tj. schopnost systému poskytovat požadované funkce bez přerušení během vyvolání procesu,
- *přesnost*, tj. schopnost systému zajistit požadované chování systému v požadovaném rozmezí.

U velmi složitých socio-technologických systémů, tj. systémů systémů, přistupuje k uvedeným parametrům další parametr kvality, kterým je interoperabilita, tj. schopnost propojených systémů plnit správně a včas v daném místě a čase požadované úkoly v požadované kvalitě.

Ze současného poznání i z výše uvedených faktů vyplývá, že bezpečnost složitých kritických technologických systémů, které představují soubory otevřených a vzájemně se prolínajících systémů (obrázek 3) uspořádaných tak, aby plnily určité úkoly v oblasti součinnosti (interoperability), závisí především na řízení integrálního rizika, a to hlavně dílčích rizik spojených s vazbami a toky v systému. Výběr vhodné strategie na zmírňování rizika je velmi komplexní a kritický úkol. ***Nejde jen o snížení pravděpodobnosti výskytu selhání, ale také o zlepšení podmínek provozních aktiv, jejichž selhání může vést k velkým provozním nákladům. Nesprávná strategie snižuje produktivitu a výnosnost technologického systému. Výběr strategie zmírňování rizika je proto typický multikriteriální rozhodovací problém.*** Nejlepší strategie se musí vybrat z možných alternativ. Musí být vzato v úvahu množství kritérií, z nichž některá jsou konfliktní [1,4,6], např. obrázek 4. Aby se zabránilo iniciaci velkých rizik, která při realizaci působí velké ztráty a škody lidem a dalším veřejným i privátním aktivům, tak základním cílem řízení technologických celků není dosáhnout velkého množství výrobků, ale i prevence ztrát na svých i veřejných aktivech, a proto se hledá konsensus mezi řízením rizik a řízením aktiv objektu. Jde o nalezení způsobu, kterým se nevyvolají rizika, která způsobí ztráty a škody na veřejných i privátních aktivech, které budou de facto vyšší než užitky ze zvýšené výroby.

Protože při orientaci na prevenci ztrát dle [1] nejde jen o snížení pravděpodobnosti výskytu selhání, technologického systému, ale také o zlepšení podmínek provozních aktiv, tak SMS (systém řízení bezpečnosti) technologických objektů musí být flexibilní a musí být zacílen na interoperabilitu veřejných a privátních aktiv.

Heterogenita a těsná propojení systémů v technologických objektech a infrastrukturách jsou příčinou obtížného popisu a emergentního (náhle vynořeného) chování předmětných systémů systémů [6,12]. Klasické analytické metody nemají schopnost poskytnout dostatečný pohled kvůli složitosti systémů systémů. K tomu je třeba hluboké porozumění a holistický přístup [6,12,13].




*Obr. 3: Schéma systému systémů a vyznačení procesů probíhajících uvnitř*


*Obr. 4: Příklad základního konfliktu při řízení kritických objektů [1]*

Kromě inherentní složitosti předmětných systémů jsou důležitá jejich propojení, označovaná jako interdependences. Zvláštní význam mají emergentní propojení, která vzniknou jen za specifických podmínek. Právě tyto nepředvídatelné závislosti jsou příčinou kaskádovitých selhání, anebo nežádoucích domino efektů a jiných nežádoucích jevů, které jsou důsledkem různých synergií a kumulací, a které jsou největší hrozbou pro dnešní společnosti

Modely řízení bezpečnosti složitých technologických objektů a infrastruktur, tj. především systémů systémů jsou teprve v počátku. Musí mít inherentní charakteristiky jako dynamické nelineární chování, spletitá pravidla interakcí, která jsou výsledkem jejich otevřenosti a vysoké propojitelnosti. Dále musí respektovat mnohaúrovňové vnitřní závislosti a nedostatek rozhraní v požadované: diverzitě podstaty poskytovaných služeb; koexistenci více časových stupnic; a úrovni vyřešení úkolu.

Interoperabilita (vzájemná schopnost spolupráce) dílčích systémů znamená, že dílčí systémy plní zadané úkoly tak, aby systém systémů plnil cíl v požadovaný čas, v požadovaném rozsahu a v požadované kvalitě, a to za normálních, abnormálních i kritických podmínek. To znamená, že chování prvků je koordinované a zacílené na určitý cíl, tj. vzájemným sdílením inherentních instrukcí (know-how systému) jsou v prostoro-časové oblasti zajištěny takové součinnosti prvků, kterými se dosáhne cílů. Jde o implicitní schopnost procesního systému (technologie), zajistit nejúčinnější, kvalitní, bezpečný, environmentálně šetrný, ekonomicky efektivní, automatizovaný a integrovaný průběh procesů přes rozhraní různých vnitřních entit a jejich okolí. Cílem je operabilní poskytování vzájemných služeb operačních objektů v souladu s požadavky jeho subjektů ve standardizovaném prostředí. Interoperabilita v kontextu rozsáhlé aplikace je schopnost systému spolupracovat s jinými systémy bez zvláštního úsilí zákazníka / uživatele. Jde vlastně o schopnost interakce a výměny informací mezi technologickými objekty a jejich informačními systémy jak uvnitř, tak vně objektu. Musí být řešena minimálně ve třech oblastech / úrovních: DATA, APLIKACE, ORGANIZACE [1]. Nejde tedy pouze o problém software a IT, ale i o komunikaci, technické a organizační záležitosti.

Složitost systému systémů vychází z požadovaných rysů systému, a to: velký rozměr; použití více technologií; složité funkční závislosti; velká interoperabilita; velký výkon; a vysoká bezpečnost, tj. funkčnost a spolehlivost, i nízké ohrožení chráněných aktiv při podmínkách normálních, abnormálních i kritických. Problémy SoS se těžko strukturují, a proto pro podporu rozhodování při jejich řízení se vytváří DSS (Decision Support System) [4].

### 3. Aplikace přístupu All Hazard Approach

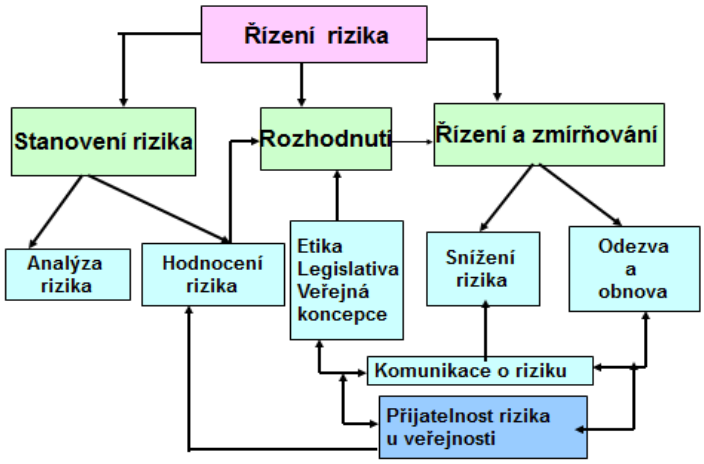
Přístup All-Hazard-Approach [7] aplikujeme způsobem, že pro technologický objekt zpracováváme bezpečnostní koncept pro všechny možné pohromy v daném místě a podle něho vypořádáváme rizika způsobem, zobrazeným na obrázku 5. Škody a ztráty, které působí pohromy, závisí na fyzikálních, chemických, biologických a časových charakteristikách pohromy a na charakteristikách lidského systému (tj. charakteristikách veřejných aktiv), a to technických a sociálních.

Škody přímé vznikají v důsledku přímého působení pohromy a škody nepřímé jsou způsobené poruchami infrastruktur, které vedou k neposkytování životodárných služeb. Kritičnost pohromy pro aktivum či entitu lze vyjádřit vztahem $\boldsymbol{C = S * O * B}$, ve kterém $\boldsymbol{S}$ je závažnost největšího dopadu, $\boldsymbol{O}$ pravděpodobnost výskytu jevu a $\boldsymbol{B}$ podmíněná pravděpodobnost, že se vyskytne nejzávažnější dopad.

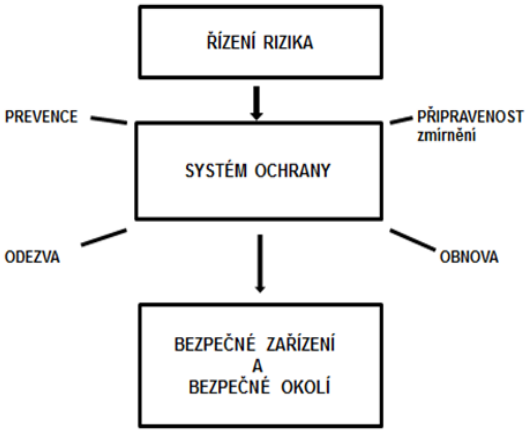

*Obr. 5: Rozčlenění opatření zacílených na zvládnutí pohrom ve střední Evropě*

Riziko v inženýrských disciplínách je chápáno jako pravděpodobná velikost ztrát, škod a újmy na chráněných aktivech v konkrétním místě, normovaná na zvolenou jednotku času [4]. Je závislé na velikosti konkrétního škodlivého jevu (pohromy) a místní zranitelnosti aktiv [4].

Na obrázcích 6 a 7 jsou zobrazeny struktury procesů, které jsou používané při jeho řízení a vypořádání v praxi [4]; další podrobnosti o zmíněném procesu jsou uvedeny v citované práci.




*Obr. 6: Schéma procesu pro řízení a vypořádání rizika z pohledu rozdělení úkolů mezi odborníky, řídící sféru a realizátory konkrétních opatření a činností; další detaily jsou v [4]*




*Obr. 7: Schéma procesu pro řízení a vypořádání rizika z pohledu budování ochrany systému zacílené na bezpečný systém a jeho okolí*

Na obrázku 8 je pak koncept procesu, používaný v praxi, který je zacílen na bezpečnost, tj. na vyšší cíl (nejde jen o snížení rizika, ale o zvýšení bezpečí lidí a dalších veřejných aktiv, na kterých jsou lidé závislí). Bezpečnost a riziko spolu jistým způsobem souvisí, ale nejsou komplementární veličiny (komplementární veličinou k bezpečnosti je kritičnost [7]).

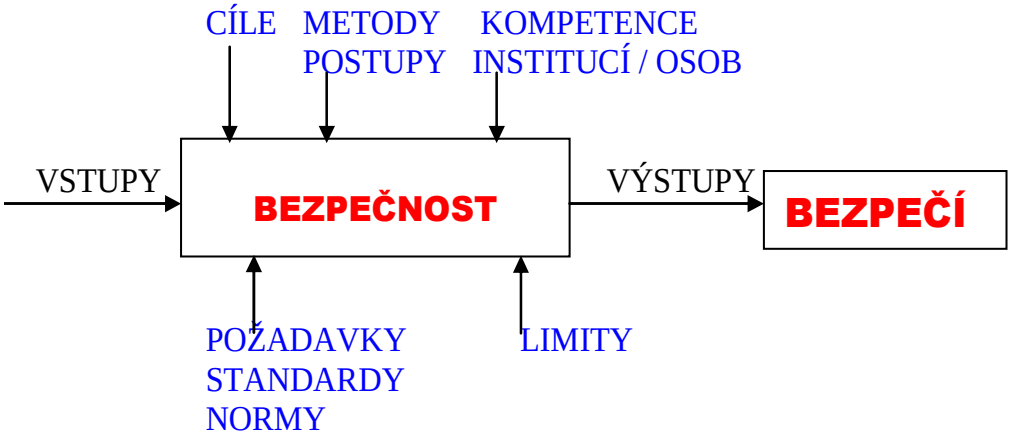
Logickou syntézou údajů získaných výzkumem [1], byl navržen procesní model pro řízení bezpečnosti území a všech entit, které se v něm nachází, zacílený na bezpečí a rozvoj lidí, který zohledňuje přežití lidí při kritických podmínkách, obrázek 9.

Postup zobrazený na obrázku 9 byl oponován a doporučen odborníky z výzkumného týmu projektu FOCUS [14]. Byl též otestován v praxi vybranými odborníky a studenty z oborů zabývajících se bezpečností z pohledu technického a manažerského.

Pro široké využití v praxi, je vytvořen nástroj, který je pochopitelný, poskytuje profesionální přesnost a informačně hodnotné výsledky, transparentnost získaných výsledků, je uživatelsky přívětivý a je možné pro něho vytvořit nástroje IT, což poskytuje zvážit technické údaje, jejich správné zpracování, a podporu pro rozhodování (kritéria, limity, ukazatele, atd.).

Procesní model obsahuje čtyři hlavní části zvané:

- území;
- rizika;
- co dělat;
- a kritické rozhraní – otázka přežití.



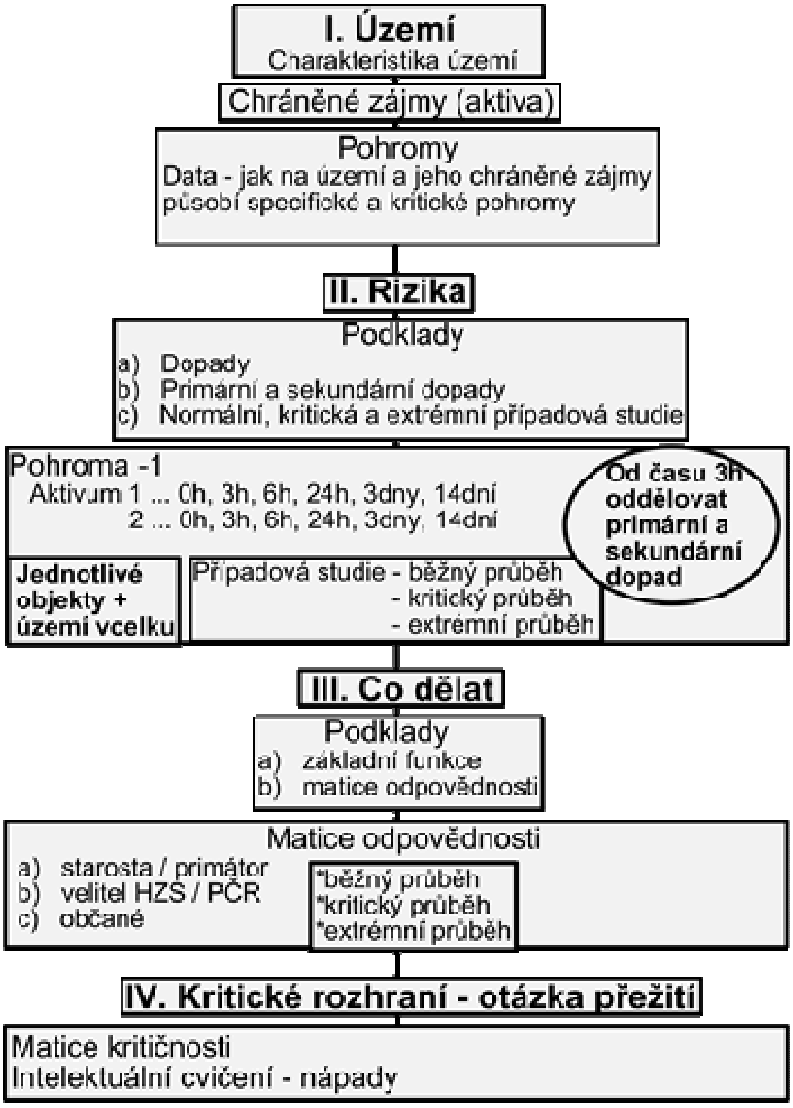

*Obr. 8: Schéma procesu pro řízení a zajištění bezpečnosti*

Obecný ***nástroj pro řízení bezpečnosti SoS se skládá ze 4 částí***, obrázek 9:

- Screening SoS.
- Vyhodnocení rizik SoS.
- Screening existujících opatření a činností pro řízení rizik SoS a pro zvyšování bezpečnosti SoS a vyhodnocení úrovně vyjednávání s riziky.
- Identifikace kritických položek řízení rizik SoS a návrh řešení gapů spojených s přežitím lidí či kontinuitou aktiv při kritických pohromách.

Přístup All-Hazard-Approach [8] znamená zvažovat při řízení bezpečnosti všechny možné druhy pohrom, tj. jevů, které mohou způsobit škody, ztráty a újmy sledovaným aktivům, tj. lidem i příslušným entitám v daném území [7].

V EU na základě výsledků projektu FOCUS (FOresight SeCUrity Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles) je třeba v současné době sledovat 77 pohrom, tj. zdrojů ohrožení, a do r. 2035 se jejich počet na základě výzkumu zvýší až na 105 [10].




*Obr. 9: Procesní model řízení bezpečnosti území. Fáze: I- charakteristika území, tj. aktiv, zdrojů domino efektů a možných pohrom; II-stanovení rizik pro 3 velikosti každé možné pohromy; III-souhrnné posouzení zacílené na identifikaci konfliktů, nepokrytých závažných problémů a chybějících odpovědností; IV-stanovení kritických situací a opatření pro přežití lidí*

**4. Aplikace přístupu Defence in Depth**

Na základě [9] představuje Defence-In-Depth (ochrana do hloubky) komplexní přístup, který zajišťuje, že lidé i životní prostředí budou ochráněny i při kritických podmínkách v objektu s jadernou technologií. Jde o komplexní filosofii bezpečnosti, která se začala aplikovat v 80. letech minulého století. Zahrnuje všechny činnosti zacílené na bezpečnost objektu i území, ve kterém se objekt nachází, a to počínaje umísťováním, přes navrhování a projektování, výstavbu, konstrukci, uvedení do provozu, provoz a odstavení objektu z provozu. Pro zajištění bezpečného systému systémů používá systémy bariér a režimová opatření. Jejím cílem je:

- kompenzovat lidská a technologická selhání,
- udržovat účinné bariéry, které odvrátí poškození zařízení i bariér samotných,
- ochránit lidi a životní prostředí, když bariéry nesplní své úlohy.

Koncept bezpečnosti kritických objektů je založený na komplexním přístupu, zvaném obrana do hloubky [9], který byl vyvinut odborníky z oblasti jaderné energetiky s cílem, aby veřejnost i životní prostředí byly ochráněny před veškerými riziky spojenými s provozem energetických jaderných zařízení.

> *Přístup All-Hazard-Approach, koncept Defence-In-Depth (ochrana do hloubky) a kultura bezpečnosti slouží proto jako základní filozofie pro bezpečný projekt a bezpečný provoz kritických objektů.*

Podle údajů v uvedených citacích správně použita obrana do hloubky zajišťuje, že žádná jednotlivá lidská chyba nebo jednotlivé selhání zařízení na jedné úrovni obrany, ani kombinace selhání na více než jedné úrovni obrany, nemůže ohrozit obranu v hloubky na následující úrovni nebo vést poškození veřejnosti nebo životního prostředí.

Obecným cílem obrany do hloubky je zajistit, aby jednotlivá porucha, selhání zařízení nebo selhání lidského faktoru na jedné úrovni obrany, a dokonce i kombinace selhání na více než jedné úrovni obrany, se nešířily do dalších úrovní obrany do hloubky. Nezávislost různých úrovní obrany je rozhodující pro splnění uvedeného cíle [15].

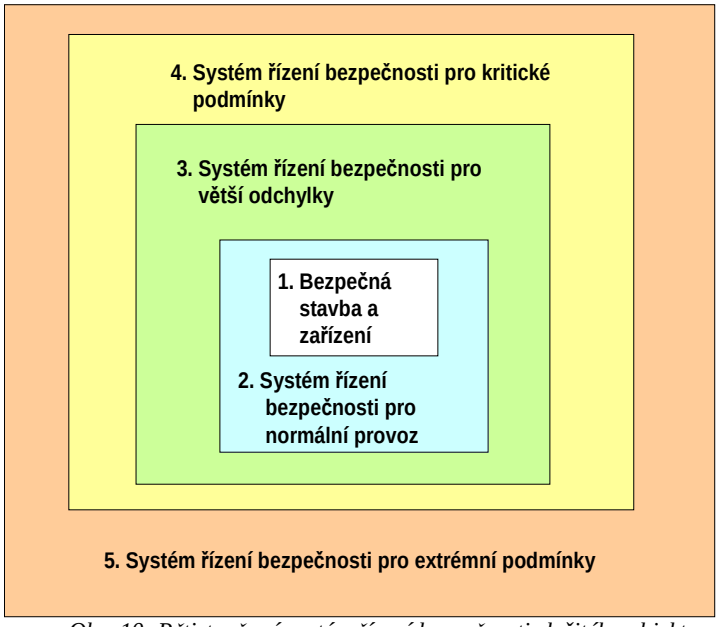
Na základě práce [1] je třeba pomocí kvalitních zadávacích podmínek vybudovat kvalitní objekt (umístění, materiál a konstrukce stavby, zařízení a jejich propojení). Pak je třeba mít:

- způsob ovládání socio-technologického systému při normálních podmínkách, tj. způsob prevence abnormálního provozu a selhání;
- způsob ovládání socio-technologického systému při abnormálních podmínkách, tj. způsob ovládání abnormálního provozu a detekce selhání;
- způsob ovládání socio-technologického systému při kritických podmínkách, tj. ovládání havárií pomoci projektových opatření;
- způsob ovládání socio-technologického systému při extrémních (nadprojektových) haváriích včetně prevence dalšího rozvoje havárie a zmírnění dopadů havárie vně objektu.

Základní prostředky pro splnění jsou: konzervativní návrh objektu a vysoká kvalita konstrukce a provozu; zabudování ovládacích, omezovacích a ochranných systémů a další typické znaky dohledu nad provozem; naprojektovány (inherentní) vlastnosti podporující bezpečnost; alternativní opatření a řízení havárie – vnitřní plán odezvy; a vnější plány odezvy.

Protože sledované SoS jsou základem pro život a rozvoj lidí, je nutné i při nadprojektových podmínkách zajistit, aby kritické objekty po vyřazení z provozu bylo možno zprovoznit v jisté dohledné době, protože na jejich funkčnosti závisí životy lidí. Proto na základě znalostí shrnutých v práci [1] a zkušeností z praxe, autorka metodou analogie uspořádala základní principy pro řízení bezpečnosti objektů a infrastruktur typu systém systémů (obrázek 10) takto:

- V návrhu, výstavbě a konstrukci inherentně používat principy bezpečného projektu (přístupy: All-Hazard-Approach, proaktivní, systémový aplikující integrální riziko, a také významná dílčí rizika spojená s vazbami a toky hmotnými, energetickými, finančními a informačními v dílčích systémech i napříč nich; správná práce s riziky; a monitoring, ve kterém jsou zabudovány korekční opatření a činnosti). Důležité je sestavení zadávacích podmínek spojených s daným územím, které vyjadřují způsob ocenění místních zranitelností vůči všem relevantním pohromám, které mohou postihnout dané místo, a také ocenění všech místně specifických rysů, které mohou způsobit specifické dopady. Na základě recentního poznání, shrnutého v pracích [6,9], je třeba u kritických složitých objektů zohlednit nejistoty náhodné i znalostní, tj. neurčitosti v datech, aby se předešlo atypickým haváriím, které jsou důsledkem nepředvídatelných jevů, které nelze odhalit běžnými stochastickými metodami.
- Řídicí systém objektu musí mít základní řídící funkce, alarmy a reakce operátora zpracované tak, aby objekt byl udržen v normálním (stabilním) stavu za normálních podmínek.
- Objekt musí mít speciální řídicí systémy orientované na bezpečnost a ochranné bariéry, které ho udržují v bezpečném stavu i při větší změně provozních podmínek (tj. při abnormálních podmínkách) a zabraňují vzniku nežádoucích jevů, což znamená, že má dobrou resilienci. Předmětné systémy udržují bezpečný provoz i za změny podmínek nebo mají schopnost zajistit normální provoz po aplikaci nápravných opatření (vyčištění, oprava…).
- Pro případ, že se vyskytnou kritické podmínky, které způsobí, že dojde ke ztrátě ovládání objektu, musí mít objekt systém opatření pro vnitřní nouzovou odezvu, zmírnění dopadů, a pro návrat do normálního provozu (plán kontinuity a vnitřní nouzový / havarijní plán).
- Pro případ, že dopady ztráty ovládání systému postihnou okolí objektu, musí mít objekt opatření i pro vnější odezvu, zmírňující opatření pro prevenci ztrát v objektu; a kapacitu pro překonání obtíží, aby byla schopnost objekt obnovit.




*Obr. 10: Pětistupňový systém řízení bezpečnosti složitého objektu*

V odborné oblasti se výše zmíněné vrstvy považují za ochranné bariery (tzv. ochrana do hloubky - Defence-In-Depth) a při rozlišení objektů z hlediska bezpečnosti se používá bezpečnostní charakteristika, že objekt má jednostupňovou nebo až pětistupňovou ochranu do hloubky. Jednotlivé systémy řízení bezpečnosti zajišťují aplikaci technických, provozních a organizačních opatření a činnosti, které jsou navrženy tak, aby buď zabránily iniciaci řetězce škodlivých jevů, anebo ho zastavily [16].
Protože deterministický přístup k ochraně do hloubky nezvažuje explicitně pravděpodobnost výskytu výzev ani mechanismů, ani nezahrnuje kvantifikaci pravděpodobnosti úspěchu spojeného s provedením prvků a systémů na každé úrovni obrany do hloubky, je deterministický přístup doplňován pravděpodobnostní analýzou bezpečnosti (PSA) v oblasti spolehlivosti systémů, pravděpodobných cílů apod. s cílem zajistit adekvátní úroveň bezpečnosti, která zajišťuje dobře vybalancovaný projekt [1].
Z důvodu existence neurčitostí, které nelze postihnout stochastickým přístupem [1,17], se v dnešní praxi kombinují stochastické postupy s expertními údaji získanými vyhodnocením řady případových studií [6].
Pro úspěšné zvládnutí rizik u složitých technologických systémů je dle [1,16] třeba:

- udržovat provoz ve středních provozních podmínkách, což lze zajistit tím, že provozní personál: je řádně vycvičený; má potřebné dovednosti; a chápe podstatu řízení základních provozních funkcí,
- zajistit bezpečný provoz za proměnných podmínek, což lze zajistit tím, že provozní personál: je řádně vycvičený; zná plány provozu za proměnných podmínek; a respektuje požadavky kultury bezpečnosti,
- ovládnout kritický stav zařízení pomocí preventivních mechanismů (např. pomocí kritických systémů bezpečnosti), což lze zajistit: aplikací pracovních postupů podle jistých přijatých standardů; a výcvikem ve vypořádání odchylek od normálního provozu,
- při ztrátě ovládání je třeba znovu získat nadvládu nad systémem, k čemuž je třeba vzdělat personál, aby byl schopen: získat povědomí o situaci; pochopit podstatu problému; porozumět omezení základních stejně jako preventivních funkcí ovládání; improvizovat,
- při neschopnosti zvládnout zařízení, je třeba vzdělat personál, aby byl schopen: odstavit technologii tak, že zajistí, co nejmenší ztráty u technologie; a aktivovat vnější nouzový plán (tj. aplikovat ochranná opatření a činnosti, uvolnit rezervy, provést evakuaci).

Z výše uvedených skutečností vyplývá, že čím vyšší velikost projektové pohromy zvolíme pro umístění, projektování, výstavbu a konstrukci objektu, tj. zajistíme pasivní ochranu, tím vyšší bezpečnost dosáhneme, protože účinnost organizačních opatření v oblasti řízení je vždy nižší než u opatření technických, u kterých dosahuje až 80%.

Zvážení poznatků:

- kritická analýza prací provedená v práci [1] ukazuje, že požadavky kladené na zařízení, systémy a komponenty kritických objektů nezvažuji systematicky kaskádová selhání,
- použití nejlepšího současného konceptu pro zajištění bezpečnosti objektů nemá zanedbatelnou kritičnost (tj. po jeho aplikaci některé zdroje rizika zůstávají) kvůli kaskádovým selhání způsobeným znalostními nejistotami [6],
- příliš velké spolehnutí na účinnost PSA, která hodnotí rizika spojená s procesním modelem výroby a neuvažuje selhání bezpečnostních prvků, tj. ochranných bariér

ukazuje, že přes všechna dosud aplikovaná opatření existují zdroje rizik, které mohou mít extrémní dopady.

**Závěr**

Analýza současné situace ukazuje, že umíme systematicky zvládnout u složitých kritických technologických systémů řadu nežádoucích procesů, tj. poruch a selhání, které dokážeme předem odhalit. Umíme aplikovat příkazy „selži bezpečně“, „když nemůžeš splnit úkol v požadované kvalitě, nic nedělej“ apod., ale někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit, složitých vazeb a spřažení v systému vznikají atypické havárie, které působí velké ztráty a škody. Proto již připouštíme, že složité systémy jsou z různých důvodů čas od času v nestabilním stavu a vznikají organizační havárie, kaskády selhání bez zjevné příčiny, tj. připouštíme nejistoty náhodné i epistemické (znalostní) v jejich chování.
Pro zvýšení bezpečnosti se stále více propojují výsledky analytických a heuristických postupů – a vytváří se zkušenostní databáze. V praxi je nutno aplikovat propojení principů All-Hazard-Approach a Defence-In-Depth. Je pochopitelné, že dobré by bylo, kdyby jednotlivé vrstvy pro řízení bezpečnosti byly nezávislé, což de facto nelze zajistit, protože tam jsou fyzické vazba. Základním principem řízení bezpečnosti je kvalifikované propojení oblastí technické, organizační, finanční, personální, sociální, znalostní; a jasné role a povinnosti všech zúčastněných. Systém řízení bezpečnosti kritických zařízení, tedy pokrývá řadu oblastí, a to technickou, vojenskou, legislativní, finanční, ekonomickou, sociální, ekologickou, vzdělávací, výzkumnou, atd. Úkoly v oblasti bezpečnosti, na základě současných znalosti a současného pojetí důmyslných bezpečnostních systémů, mají všichni účastníci. Úkoly jednotlivých zúčastněných a jejich propojení v různých situacích musí být stanoveny zákony, morální a dalších standardů a norem.
Protože skutečnost je taková, že neumíme identifikovat neurčitosti, musíme při řízení bezpečností velmi výrazně spoléhat na odezvu, tj. na přípravu provozních předpisů v případě výrazných změn podmínek a v případě jejího neúspěchu i na odezvu aplikující ochranná opatření pro základní veřejná aktiva. Proto pro zajištění bezpečnosti složitých objektů a ochrany lidí hledáme řešení odezvy i pro možné případy, které nelze odhalit pravděpodobnostními přístupy a budujeme pro ně náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik inženýrů a techniků aplikujících zásahy do technologických procesů a záchranářů.
V rámci strategie pro zajištění bezpečnosti a udržitelného rozvoje se musí v kritických objektech nastavit: program pro neustálé zvýšení bezpečnosti kritických objektů; míry pro posuzování úrovně bezpečnosti z hlediska účinnosti bezpečnostního systému (ukazatele); program, který zajišťuje bezpečnost, který je sestaven z provázaných projektů; a projekty, které jsou naplněné provázanými procesy.

Nástroje pro ovládání kritických komplexních objektů a infrastruktur, zajišťující bezpečnost a rozvoj, tedy jinými slovy, zachování, ochranu a rozvoj chráněných aktiv jsou:

- umístění a výstavba objektů,
- promyšlený několika úrovňový řídicí systém zahrnující řízení strategické, taktické a operativní, který je založen na kvalifikovaných datech, odborných znalostech, expertních hodnoceních a dobrých metodách rozhodování; vzdělávání a výcvik zaměstnanců,
- věda, výzkum a TSO (profesní organizace zajišťující profesionální podporu provozovatele kritického objektu a veřejné správy),
- specifické vzdělávání technických a řídících pracovníků,
- technické, zdravotní, ekologické, sociální, cyber a dalších standardy, normy a předpisy, tedy nástroje pro řízení procesů, které mohou nebo by mohly vést k výskytu (vzniku) pohromy nebo k zvětšení jejich dopadů,
- inspekce,
- systém spolupráce vedení komplexního objektu s veřejnou správou, s organizacemi na území a s organizacemi, které používají podobné technologie,
- personál pro zvládání nouzových situací,
- komponenty a systémy pro zvládání kritických situací (tj. všemi způsoby zajistit řízení kontinuity a krizové řízení),
- bezpečnostní, nouzové (a to včetně plánování kontinuity kritických objektů) a krizové plánování.

Je si třeba uvědomit, že systémové myšlení je nástroj, který pomáhá rozvíjet společný jazyk, který umožňuje specialistům z různých oborů a technologií vzájemně komunikovat. Jeho metodologie je založena ve dvou klíčových principech: realita je chápána jako celek a celek je víc než suma komponent; a pouze uzavřený systém je definován jako soubor propojených entit, z nichž žádný podsoubor není vztažen k nějakému dalšímu podsouboru.

Systémy jsou vždy v interakci se svým okolím. Proto je důležité znát, co patří do systému, a co patří do okolí. Vědci definují hranici systému větším či menším počtem kritérií, které musí entita splnit, aby patřila do systému. Skutečností však v reálném světě je, že hranice není ostrá, protože některá kritéria jsou konfliktní. Dnešní realitou jsou soubory otevřených a vzájemně propojených objektů, jejichž model je systém systémů.

Výsledky uvedené jasně dokládají, že je skutečně změnit styl řízení bezpečnosti a inženýrské postupy zacílené na bezpečnost. Zkušenosti z praxe v ČR a SR však bohužel dokládají tristní skutečnost – někteří profesoři a docenti z technických universit, kde učí bezpečnost, přednášejí výsledky, které jsou hloupé a působí společenské škody; sesuv půdy na dálnici D8, propadnutí mostů ve výstavbě v ČR i v SR, nekvalitní dálniční mosty na D1 u Ostravy, propady ve Stromovce při výstavbě tunelu Blanka a další, které měly za důsledek velké materiální škody, které zaplatili daňoví poplatnici a v několika případech i ztráty na lidských životech, zcela jasně ukazují, že v obou zemích by měla být upřednostněna odbornost a veřejný zájem před korupcí a zájmy jednotlivců a zájmových seskupení.

## ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů.* ISBN: 978-80-01-05771-1. Praha: ČVUT 2015, 208p.
[2] UN. *Human development report.* New York: UN 1994, www.un.org.
[3] EU. *The safe community concept*. Brussels: EU, 2004, PASR project.
[4] PROCHÁZKOVÁ, D. *Analýza a řízení rizik.* ISBN: 978-80-01-04841-2. Praha: ČVUT 2011, 405p.
[5] EUROPEAN FOOD AUTHORITY. *Regulation 1169/2011*. http://eur-lex.europa.eu
[6] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN:978-80-01-05245-7. Praha: ČVUT 2013, 223p.
[7] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN:978-80-01-04844-3. Praha: ČVUT 2011, 483p.
[8] FEMA. *Guide for all-hazard emergency operations planning*. State and Local Guide101, Washinton 1996.
[9] IAEA. *Assessment of defence in depth for nuclear power plants*. ISBN:92–0–114004–5. Safety report series No. 46. IAEA, 2005 Vienna, 119p.
[10] PROCHÁZKOVÁ, D. *Study of disasters and disaster management*. ČVUT study in frame of FOCUS project. ISBN: 978-80-01-05246-4. Praha: ČVUT 2013, 207p.
[11] MASLOW, A. H. *Motivation and personality*. New York: Haper 1954, 236p
[12] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. ISBN: 978-80-01-05103-0. Praha: ČVUT 2012, 318p.
[13] BRIŠ, R., SOARES, C.G., MARTORELL, S. (eds). *Reliability, risk and safety. Theory and applications*. ISBN:978-0-415-55509-8. Leiden: CRC Press / Balkema 2009, 2367p.
[14] PROCHAZKOVA, D. *Results of project FOCUS*. ISSN 1814-4225. Radioelectronic and Computer Systems. 70 (2014) No 6, pp 23-26.
[15] IAEA. *Safety of Critical Power Plants: Design, Safety Standards Series No. NS-R-1*. Vienna: IAEA 2000.
[16] SEVCIK, A., GUDMESTADO, T. *Solutions and safety barriers: The holistic approach to risk-reducing measures.* In: Safety and Reliability: Methodology and Application. ISBN:978-1-138-02681-0. London: Taylor & Francis Group 2014.
[17] VATN, J. *Structuring contributors to successful operation.* Safety and Reliability: Methodology and Application. ISBN 978-1-138-02681-0. London: Taylor & Francis Group, 2014.

## ADRESY AUTOROV

**Dana PROCHÁZKOVÁ, Doc. RNDr., PhD., DrSc.,** ČVUT v Praze, fakulta dopravní, Konviktská 20, 110 00 Praha 1, Česká republika, prochazkova@fd.cvut.cz

**Jan PROCHÁZKA, RNDr., Ph.D.,** České vysoké učení technické v Praze, fakulta dopravní, Konviktská 20, Praha 1,japro@seznam.cz

***RECENZIA TEXTOV V ZBORNÍKU***
*Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.*

***REVIEW TEXT IN THE CONFERENCE PROCEEDINGS***
*Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.*