# ŘÍZENÍ RIZIK ZACÍLENÉ NA ZAJIŠTĚNÍ BEZPEČNOSTI SLOŽITÝCH KRITICKÝCH OBJEKTŮ

# MANAGEMENT OF RISKS DIRECTED TO ENSURING THE COMPLEX CRITICAL FACILITIES SAFETY

**Dana Procházková**[65]

*ABSTRAKT:*

*Kritické objekty jsou složité technologické objekty a infrastruktury, které jsou nutné pro životy lidí v dnešním světě, a to při normálních, abnormálních i kritických podmínkách. Práce obsahuje recentní pokrokové způsoby řešení jejich bezpečnosti založené na: správném výběru kontextu pro chápání rizik, který zohledňuje schopnosti používaných konceptů zajistit bezpečnost a disponibilní zdroje, síly a prostředky; kvalitní práci s riziky; aplikaci dvou zásadních přístupů, a to All-Hazard-Approach a Defence-In-Depth, provázaných do pětistupňového systému pro zajištění bezpečnosti; a aplikaci procesního modelu pro řízení bezpečnosti v čase.*

*ABSTRACT:*

*Critical facilities are complex technological facilities and infrastructures that are important for human lives in the present world, namely at normal, abnormal and critical conditions. The work contains recent advanced ways of solution of their safety based on: correct selection of context for understanding the risks that taking into account the capabilities of used concepts to ensure the safety and the accessible sources, forces and means; qualified work with risks; application of two fundamental approaches, namely All-Hazard-Approach and Defence-In-Depth, interconnected into five degrees system for ensuring the safety; and application of process model for management of safety in time.*

*KLÍČOVÁ SLOVA:*

*Kritické složité systémy; interoperabilita; bezpečnost; riziko; bezpečí lidí; ochrana obyvatelstva.*

*KEYWORDS:*

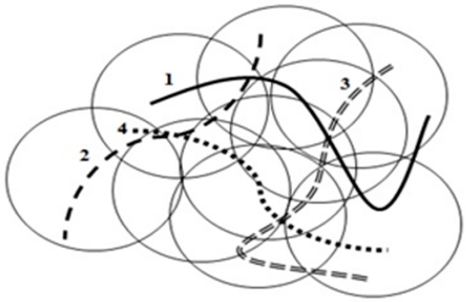
*Critical complex systems; interoperability; technological object; technological infrastructure; safety; risk; human security; public protection.*

## 1 ÚVOD

Kritické objekty jsou technologické (nebo přesněji socio-technologické) systémy, zahrnující budovy a infrastruktury, jsou nutné pro životy lidí v dnešním světě. Je však pravdou, že na jedné straně usnadňují život lidí, ale na straně druhé ho ohrožují, když dojde k haváriím. Největší rizika jsou spojená s objekty a infrastrukturami, které jsou složité a obsahují navíc nebezpečné chemické látky. Předmětné objekty jsou víc než jen množinou technických částí

[65] Procházková, Dana, doc., RNDr., PhD., DrSc., ČVUT v Praze, fakulta dopravní, konviktská 20, 110 00 Praha 1, ++420 224355027, prochazkova@fd.cvut.cz

zařízení a součástek. Jsou odrazem organizační struktury, managementu, provozních předpisů a kultury konstrukčních organizací, které je vytvořily a také jsou zpravidla i odrazem společnosti, ve které byly vytvořené [1-4]. Jejich model, nazývaný systém systémů je zobrazen na obrázku 1. Pro bezpečnost sledovaných objektů je důležitá interoperabilita za podmínek normálních, abnormálních i kritických [4].




***Obr. 1 - Schéma složitého objektu pomocí modelu systém systémů a vyznačení procesů, které v něm probíhají.***

***Fig. 1 –Scheme of complex facility by model „system of systems" and denotation of processes going inside.***

Je skutečností, že sice existuje řada přístupů, norem a standardů, jejichž aplikací se zajišťuje bezpečnost kritických objektů, ale havárie se vyskytují stále, a proto se hledají další účinnější přístupy pro jejich konstrukci a řízení během jejich provozu.

Předložená práce je syntetická, obsahuje recentní pokrokové způsoby řešení bezpečnosti komplexních kritických objektů a výsledky autorky získané v několika vybraných oblastech: procesní model pro práci s riziky; ocenění schopnosti používaných konceptů práce s riziky zajistit bezpečnost; výsledky aplikace dvou zásadních přístupů, a to All-Hazard-Approach [5] a Defence-In-Depth [6,7], které propojením vytváří pětistupňový koncept pro zajištění bezpečnosti složitého objektu; a procesní model pro řízení bezpečnosti v čase, kterým se zajistí, že složitý kritický objekt je bezpečný po celou dobu životnosti. Bezpečný kritický objekt je takový objekt, který je zabezpečen vůči všem vnitřním a vnějším pohromám, včetně lidského faktoru, a ještě neohrožuje své okolí, ani při svých kritických podmínkách, čímž výrazně přispívá k bezpečí a rozvoji lidí.

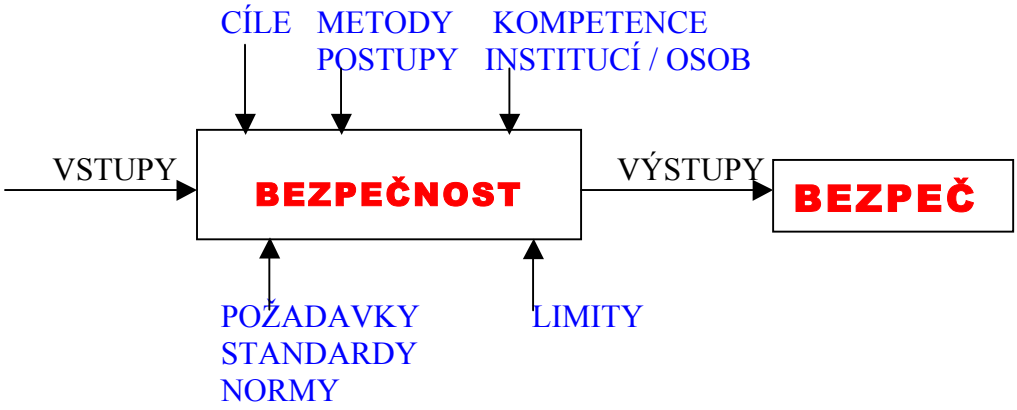
# 2 VYPOŘÁDÁNÍ RIZIK ZACÍLENÉ NA BEZPEČÍ

Svět, ve kterém žijeme (označovaný jako lidský systém), se dynamicky vyvíjí, tj. neustále v něm probíhají jisté procesy, jejichž výsledky jsou jevy, které nazýváme pohromy a které od určité velikosti působí člověku a jeho aktivům ztráty a škody [1,8]. Riziko je chápáno jako pravděpodobná velikost ztrát, škod a újmy na chráněných aktivech v konkrétním místě a je závislé na velikosti konkrétní pohromy a místní zranitelnosti aktiv [8].

V praxi dnes podle cíle práce s riziky rozlišujeme dva koncepty, a to řízení rizik a řízení bezpečnosti, přičemž je skutečností, že druhý jmenovaný naplňuje cíle lidí lépe [8]. Je to způsobeno tím, že riziko a bezpečnost jsou sice v určitém vztahu, ale nejsou komplementárními veličinami [9], protože bezpečnost lze zvýšit aniž bychom snížili riziko, např. aplikací varovacích systémů zvýšíme bezpečnost, ale riziko nesnížíme. Komplementární veličinou k bezpečnosti je kritičnost. Kritičnost je chápaná jako mezní stav systému, který je významný pro stabilitu systému [4] a posuzuje se podle:

- možných škod na životech a zdraví lidí. Usuzuje se na ní dle škod možných při haváriích, v jaderných nebo chemických provozech,
- ztráty funkčnosti cílené činnosti, která má jisté poslání (mission). Usuzuje se na ni dle rozsahu postiženého území, např. při selhání navigačního systému,
- ekonomických škod při podnikání. Usuzuje se na ni např. dle ztrát, které způsobí nefunkčnost bank.

Ze systémového hlediska je zajištění bezpečnosti základním požadavkem na systém jako celek, nikoli jen požadavkem na jeho komponenty, a poměrně snadno se dá odvodit systémové schéma řízení bezpečnosti v určité situaci uvedené na obrázku 2. Z obrázku je zřejmé, že tím jaká opatření používáme k zajištění bezpečnosti, tím určujeme výsledek, tj. bezpečí jako stav systému.




Obr. 2 - Procesní model vytváření aktuální bezpečnosti, jeho vstupy a výstupy.
Fig. 2 – Process model for formation of up-to-date safety, its inputs and outputs.

Úkolem vypořádání rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Snižování rizika je vždy spojeno se zvyšováním nákladů. Proto řízení rizika je vedeno snahou najít hranici, na kterou je únosné riziko ještě snížit, aby vynaložené náklady byly společensky přijatelné. Z pohledu praxe je třeba se dohodnout na tom, jaké požadavky bude výstup z hodnocení rizika splňovat. Při hodnocení rizik je nutné se snažit stanovené požadavky dodržovat a případné nedodržení odůvodnit. Jedná se především o splnění požadavků: provedení hodnocení v požadované šíři a kvalitě v souladu s přijatou metodikou hodnocení; úplnost hodnocení; zahrnutí nejnovějších poznatků vědy; odhad nejistot i neurčitostí v případě použití extrapolací; jednotné vyjádření charakteristik rizika; a průhlednost provedení procesu hodnocení rizik.

Svět je však složitý systém systémů ve vertikální i horizontální rovině, a proto jeho chování je heuristické, tj. je značně proměnné v závislosti na vnitřních a vnějších podmínkách, což znamená, že za určitých situací vznikají neočekávané jevy, které v reálném životě mohou přinést citelné ztráty a škody, protože jsou důsledky jevů, se kterými člověk na základě svých znalostí nepočítá [4,8], protože nejsou detekovatelné stochastickými metodami, které pracují s náhodnými nejistotami. Teprve dnes u zvláště složitých systémů systémů, abychom zabránili: atypickým haváriím a kaskádovitým selháním infrastruktur, se snažíme vyrovnat s riziky, jejichž zdroji jsou neurčitosti, tj. znalostní nejistoty. Používáme k tomu multikriteriální přístupy [4,8].

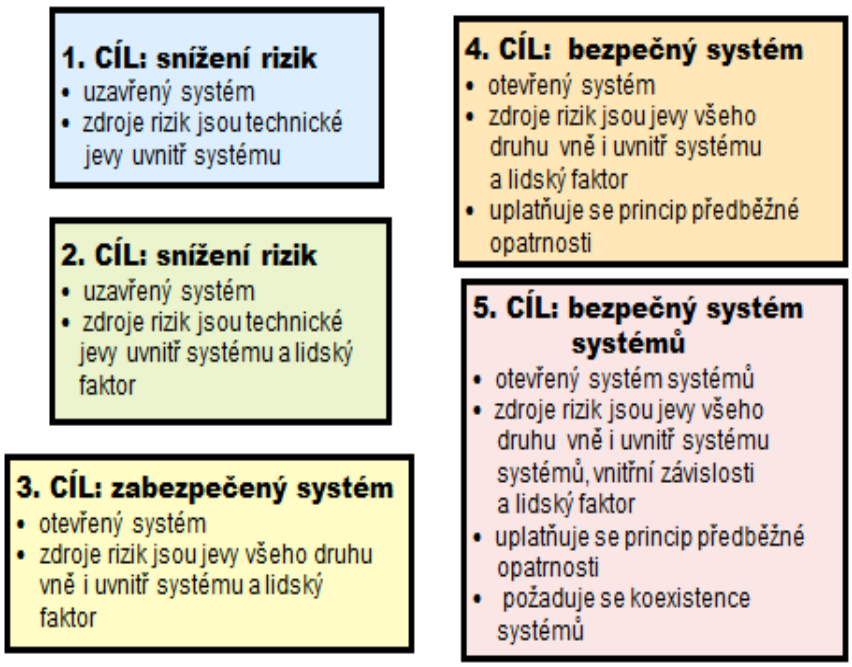
Na základě komplexní analýzy a kritického posouzení několika tisíc odborných prací a výsledků z praxe, jejichž výsledky jsou v pracích [1,3,4,8], je nutné při řešení problémů

bezpečnosti kritických objektů použít systémový přístup (tj. zaměřit se na integrální riziko) a nejprve vybrat správný koncept práce s riziky (tj. kontext, v němž rizika sledujeme) a poté respektovat logický model práce s riziky. Klíčové koncepty inženýrství zaměřených na bezpečnost jsou:

1. Přístupy jsou založené na riziku - intenzita prací a dokumentace je přiměřená úrovni rizika.
2. Odborný přístup je založen na tom, že se zvažují jen kritické atributy kvality a kritické parametry procesu.
3. Řešení problémů se orientuje na kritické položky – sledují a řídí se kritické aspekty technických systémů zajišťujících konzistenci operací systémů.
4. Prověřené parametry kvality se objevují již v návrhu projektu.
5. Důraz na kvalitní inženýrské postupy – musí se prokazovat správnost zvolených postupů v daných podmínkách.
6. Zacílení na zvyšování bezpečnosti - neustále zlepšování procesů s využitím analýzy kořenových příčin poruch a selhání.

## 3 KONTEXTY PRO VYPOŘÁDÁNÍ RIZIK A JEJICH SCHOPNOST ZAJISTIT BEZPEČNOST

Systematická práce s riziky zacílená na jejich redukci je doložena od 30. let minulého století. Na základě kritického vyhodnocení současných poznatků, jehož výsledky jsou shrnuty v pracích [3,4,8], rozlišujeme pět konceptů, ze kterých vycházíme při vyjednávání s riziky, a to: klasické řízení a inženýrství rizika; klasické řízení a inženýrství rizika zahrnující lidský faktor; řízení a inženýrství zaměřené na bezpečí (zabezpečovací řízení a inženýrství); řízení a inženýrství zaměřené na bezpečnost, tj. takové ovládání a vypořádání rizika, které zajistí jak zabezpečený systém, tak jeho bezpečné okolí; a řízení a inženýrství zaměřené na bezpečnost systému systémů (SoS); obrázek 3. Charakteristiky konceptů a praktické aplikace jsou popsány v citovaných pracích a konkrétní výsledky jsou uloženy v archivu [10].



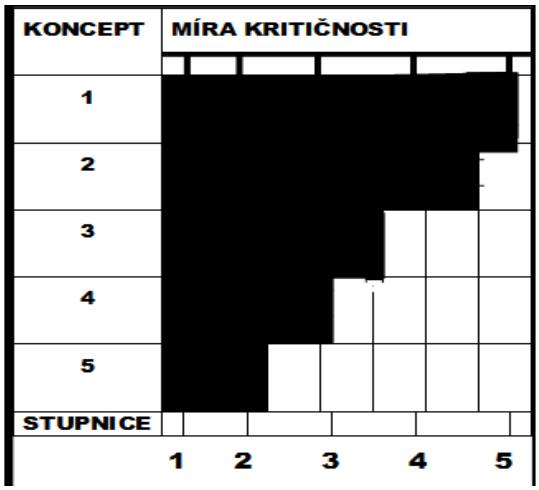

***Obr. 3 - Koncepty řízení a inženýrského vypořádání rizik a jejich cíle, uspořádané***

***chronologicky dle zavedení do inženýrské praxe.***
***Fig. 3 - Concepts of management and engineering trade-off with risks and their targets, arranged chronologically according ti introdustion into practic.e***

Dosažení cíle znamená dobře řídit a správně rozhodovat, přičemž dobré řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici [8]**.** *Poznámka:* nejčastější chyba v českých poměrech je podle zkušeností autorky fakt, že se neprověřuje kvalita datových souborů, vzájemný vztah mezi přesností dat a citlivostí metody, a hodnocení nerespektují systémovou podstatu objektů, tj. nezvažují vliv vazeb a toků.

Z výsledků výzkumu [9], založeného na aplikaci teorie maximálního užitku, který se zabýval hodnocením míry kritičnosti konceptů současného řízení a vypořádání rizik objektů, vyplývá, že žádný z dnes používaných konceptů pro řízení a vypořádání rizik nemá zanedbatelnou míru kritičnosti, obrázek 4; tj. míra kritičnosti při aplikaci:

- klasického konceptu řízení a inženýrského vypořádání rizik je extrémně vysoká,
- konceptu řízení a inženýrského vypořádání rizik zvažujícího lidský faktor, je velmi vysoká,
- konceptu řízení a inženýrského vypořádání rizik zaměřeného na zabezpečený systém je vysoká,
- konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém je střední,
- konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém systémů je nízká.




***Obr. 4 - Míry kritičnosti konceptů pro řízení a vypořádání rizik: 1 – klasický koncept řízení a vypořádání rizik; 2 – klasický koncept řízení a vypořádání rizik zvažující lidský faktor; 3 – koncept řízení a vypořádání rizik zaměřený na zabezpečený systém; 4 - koncept řízení a vypořádání rizik zaměřený na bezpečný systém; a koncept řízení a vypořádání rizik zaměřený na bezpečný systém systémů [11].***
***Fig. 4 – Criticality rates of concepts for management and trade-off with risks: 1 - classical concept of management and trade-off with risks; 2 - classical concept of management and trade-off with risks including the human factor; 3 – concept of management and trade-off with risks directed to secured system; -e security management and security engineering; 4 - concept of management and trade-off with risks directed to safe system; 5 - concept of management and trade-off with risks directed to safe system of systems [11].***

Uvedený výsledek také znamená, že ani nejpokrokovější koncept, kterým je řízení bezpečnosti systému systémů, nezaručuje zanedbatelnou míru kritičnosti. Důvodem jsou rizika napříč systémů náležejících do systému systémů (SoS) a do propojení SoS s okolím, která nejsme schopni na základě současných znalostí a zkušeností předem všechna odhalit.

Z výše uvedených fakt vyplývají základní principy pro práci a riziky, a to: být proaktivní; domýšlet možné důsledky; správně určovat priority z pohledu veřejného zájmu; myslet na zvládnutí nepřijatelných dopadů; zvažovat synergie; a být ostražitý, což odpovídá filosofii prosazované v práci [11]. Proto při stanovení rizika pro strategické rozhodování je nutno používat hierarchický multikriteriální postup. Recentní odborné práce používají pojem hierarchické holografické modelování (HHM) [11]. Výsledky pak jsou vysoce kvalitní, protože zohledňují řadu faktorů, které jsou původci neurčitostí. Protože jde o postup náročný na data i zpracovatelské metody, tak se autorka domnívá, že by Rada vlády pro bezpečnostní výzkum měla dát prostředky na předmětnou problematiku odborníkům, kteří mají znalosti a schopnosti předmětné postupy do české praxe zavést.

Snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, apod., a proto se v praxi hledá hranice, na kterou je únosné riziko snížit tak, aby vynaložené náklady byly ještě rozumné. Tato míra rizika (určitá optimalizace) je většinou předmětem vrcholového řízení a výsledkem politického rozhodování, při kterém je z hlediska zajištění rozvoje nutné, aby se využily současné vědecké a technické poznatky a zohlednily ekonomické, sociální a další podmínky.

S vnímáním rizika souvisí přijatelnost rizika, která musí mít sociální rozměr. Je třeba zvažovat:

- pro koho má být riziko přijatelné?; pro původce rizika, pro politiky nebo pro veřejnou správu?
- kdo stanoví přijatelnost?; politici rozhodují o tom, co je zákonné, a tudíž by neměli rozhodovat o tom, co je přijatelné,
- zda při stanovení přijatelnosti rizik byla diskutována aktuálně tolerovatelná rizika, netolerovatelné prahové hodnoty a postoje veřejnosti k rizikům.

Při hodnocení přijatelnosti rizika se jedná o porovnání hodnoty / míry rizika zjištěné analýzou rizika sledovaného systému s mezní hodnotou přijatelnosti nebo stanovenou mezní funkcí přijatelnosti. Postoj jednotlivce k riziku závisí na vnímání rizika a stresu, který dané riziko způsobí danému jednotlivci (úmrtí, zranění, ztráta zaměstnání aj.). Postoj společnosti k riziku závisí také na celkovém vnímání rizika, dále na averzi vůči riziku, např. jedna havárie s vyšším počtem obětí v jednom případě je méně přijatelná než vyšší počet havárií s jednotlivými oběťmi, a to přesto, že celková suma obětí za určité období je stejná.

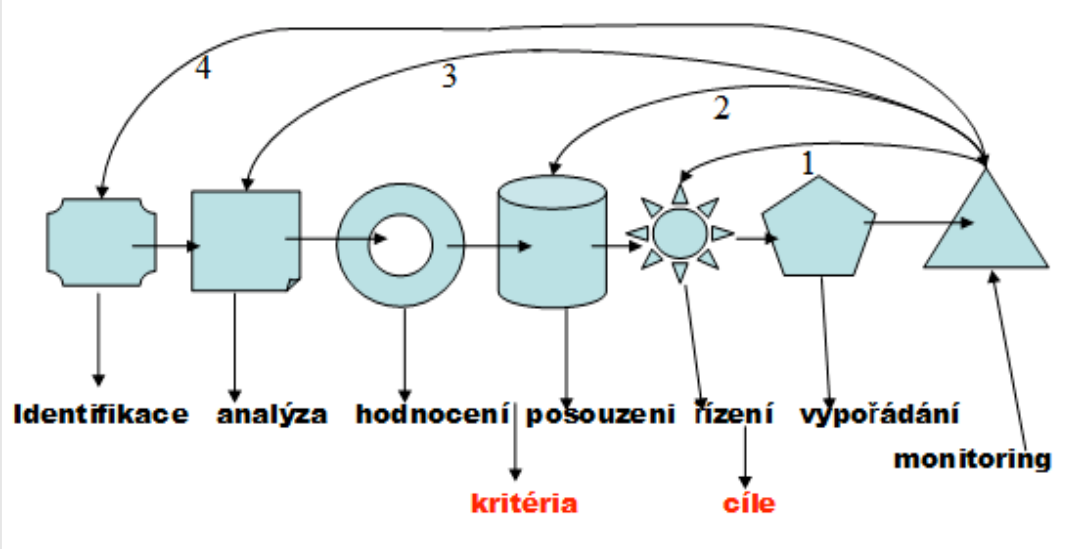
Společnost akceptuje, když určitá skupina lidí je vystavena riziku, aby se získaly výhody pro jiné skupiny lidí. Roli hraje poměr mezi náklady na zvyšování bezpečnosti a počty zachráněných životů, pozornost médií apod. Přijatelnost rizika závisí na sociálních, ekonomických a politických faktorech a na vnímaném prospěchu z činností, u kterých přínosy jsou podstatně vyšší než náklady na záchranné a likvidační práce při realizaci rizika.

Rizika byla, jsou a budou a neustále se budou objevovat nová. Řízení a vypořádání rizik, které způsobují pohromy, vyžaduje rozměr a měření rizika, které berou v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Většina technik na určování rizika nereprezentuje holistický přístup a nerespektuje, že riziko je rozdělené na lokální, regionální i státní úroveň.

Je zřejmé, že nejsme-li schopni riziko identifikovat a analyzovat, nejsme schopni se proti němu účinně bránit. Chyba, které se dopustíme při identifikaci, analýze a hodnocení rizika, se přenáší do nouzových a krizových plánů, do plánů kontinuity a snižuje jejich hodnotu ve vztahu k plánovaným opatřením směřujícím především k ochraně lidských životů a zdraví, ale i v oblasti akceschopnosti záchranných složek podílejících se na realizaci záchranných operací.

# 4 PROCESNÍ MODEL PRO PRÁCI S RIZIKY

Na základě současných poznatků a zkušeností, shrnutých a kriticky vyhodnocených v práci [8], je zpracován procesní model pro práci s riziky, zobrazený na obrázku 5. Model platí pro práci s riziky za normálních a abnormálních podmínek a platí pro všechny typy rizik, tj. dílčí, integrovaná i integrální (dílčí – zvažuje se jedno aktivum; integrovaná – zvažuje se agregace pro více aktiv; integrální – zvažují se aktiva i vazby a toky mezi nimi). V případě výskytu kritických podmínek je třeba zvážit příčinu kritických podmínek, tj. odhalit přispěvatele k riziku, který způsobil kritické podmínky a absolvovat proces od počátku.




***Obr. 5 - Procesní model práce s riziky. Kritéria = podmínky, které stanovují, kdy je riziko přijatelné, podmíněně přijatelné nebo nepřijatelné.***
***Fig. 5 – Process model of work with risks. Criteria = conditions determining when risk is acceptable, conditionally acceptable or non-acceptable.***

Z obrázku 5 je zřejmá zásadní role monitoringu. V případě, že se zjistí, že riziko je nepřijatelné, je třeba provést změny, jak naznačují zpětné vazby na obrázku 5. Protože změny vyžadují zdroje, síly a prostředky, tak na základě zajištění hospodárnosti se nejprve realizuje zpětná vazba 1, a teprve, když nepřinese žádoucí stav, tak se realizuje zpětná vazba 2; poté zpětná vazba 3, a když ani po ní není žádoucí výsledek, tak zpětná vazba 4. V případě výskytu extrémních jevů s katastrofickými dopady se přikračuje okamžitě k realizaci zpětné vazby 4.

Je třeba také poznamenat, že kritický je také výběr kvalitativního nebo kvantitativního přístupu při oceňování rizik, protože s kvantifikací rizika se musí zacházet obezřetně, jelikož výpočty rizika vytváří falešný pocit jistoty a bezpečí. Proto je třeba vždy porovnat pro a proti při použití kvantitativní a kvalitativní analýzy. Pokud se hovoří o kvantifikaci, je třeba zmínit a porovnat úrovně kvantifikace: verbální (velký, malý), ordinální (např. od 1 do 10), bodové

hodnocení, intervalové hodnocení, výpočet pravděpodobnosti, výpočet na základě důkazů (Bayesův teorém).

Na základě dosavadních znalostí a zkušeností, shrnutých v práci [4], platí:

1. Důvody podporující kvantitativní analýzu jsou: stanovení rizika je výsledkem objektivních metod a postupů včetně statistické analýzy dat; výsledky analýzy rizika jsou také v „manažerském jazyce" – procenta, finance apod.; poskytují se dostatečné podklady pro analýzu nákladů a přínosů; a je možné sledovat a kontrolovat výkonnost řízení rizika.
2. Důvody proti kvantitativní analýze jsou: výpočty mohou být někdy složité a mohou pro nezasvěceného vypadat jako černá skříňka; a ke kvantitativní analýze jsou potřebné znalosti a počítačové programy.
3. Několik doporučení ke kvantitativní analýze: riziko jako číslo často fascinuje, ale současně oslepuje vnímání souvislostí. Z hlediska komunikace s veřejností, je třeba upozornit na to, že velmi nízké pravděpodobnosti se obtížně vztahují ke každodenním zkušenostem. Například jeden/jedna z miliónu v čase znamená 30 sekund za rok. Proto je zde žádoucí jistá míra analogie; údaje typu $10^{-5}$ nevyjadřují aktuální riziko, nýbrž jsou statistickou horní hranicí možnosti, že riziko by se mohlo vyskytnout. Díky mocnině deseti se věří, že snížení rizika o řád nebo o dva řády je pouhým násobkem deseti. Snížení rizika $10^{-3}$ na $10^{-4}$ znamená, že riziko se sníží o devadesát procent. Následné snížení z $10^{-4}$ na $10^{-5}$ je desetkrát menší, a tudíž devíti procentní. Proto se doporučuje vyjadřovat snížení rizika graficky; a kvantitativní přístup k riziku musí tudíž vycházet z prosté zásady: spíše měřit to, co je měřitelné, než to, co je důležité. Pokud důležité je současně měřitelné, tím lépe.
4. Důvody pro použití kvalitativní analýzy jsou: výpočty, pokud se dělají, jsou jednoduché a snadno pochopitelné; není nutné kvantitativně určit četnost výskytu pohrom; není nezbytné určit náklady na opatření zmírňující působení rizikových faktorů; kvalitativní analýza uspořádá a doporučí oblasti pro hlubší a detailnější posouzení.
5. Důvody proti použití kvalitativní analýzy jsou: výsledky včetně stanovení rizika jsou převážně subjektivní; nepracuje se s žádnou hodnotou a hodnotovými ukazateli; pro návrh protiopatření jsou poskytnuty pouze náznaky problému; není možné sledovat účinnost a výkonnost procedur řízení rizika, protože chybí objektivní měřítko.
6. Několik doporučení ke kvalitativní analýze: kvalitativní přístup k riziku by se měl zabývat jen potenciálem / možností výskytu; kvalitativní přístup je založen na popisných hodnotách s relativní důležitostí, takže nelze opomenout následující problémy kvalitativního přístupu: Jak vysoké je vysoké riziko nebo jaká je porovnatelnost různě vysokých rizik? Jaké jsou rozdíly mezi vysokým–středním, vysokým–nízkým, středním–nízkým?; a skórování rizika může vést k chybnému rozhodnutí, které znamená, že opatření se dělají tam, kde by se dělat nemusela, a naopak kde by se měla dělat, se nedělají.

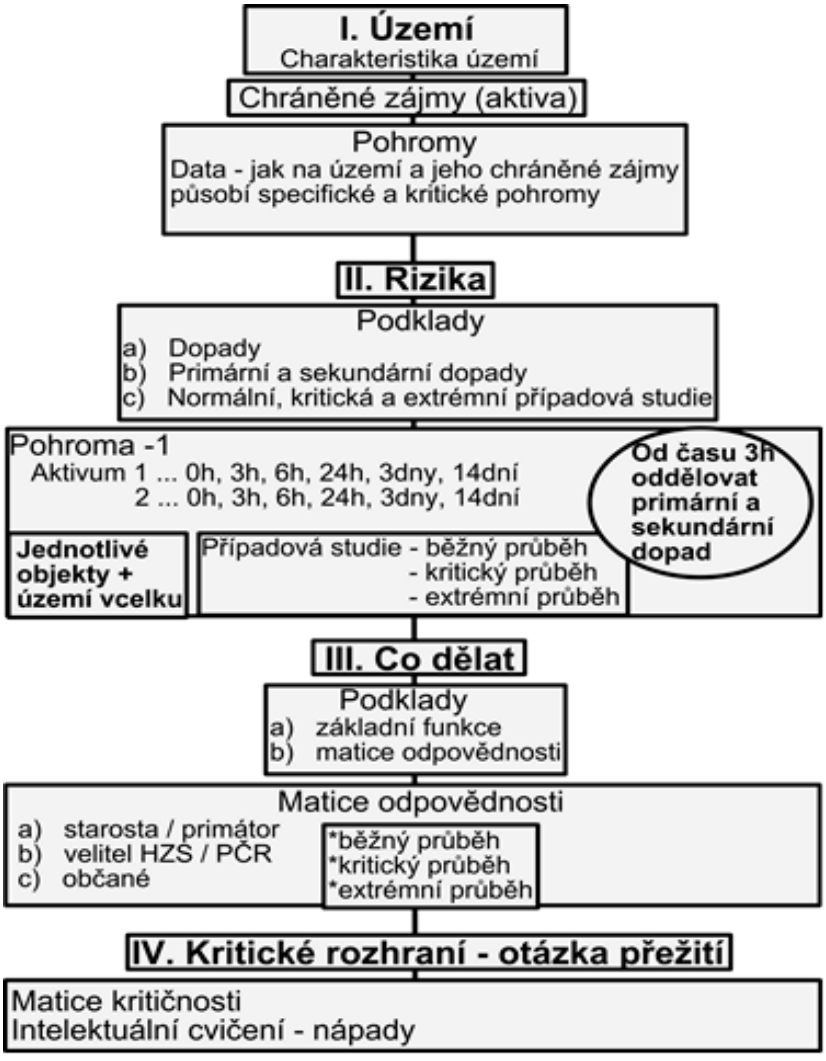
# 5 PĚTISTUPŇOVÝ SYSTÉM PRO ZAJIŠTĚNÍ BEZPEČNOSTI

Zajištění bezpečnosti kritického objektu na základě recentních znalostí provádíme způsobem, že propojujeme dva přístupy, a to All-Hazard-Approach a Defence-In-Depth.

## 5.1 Aplikace přístupu All-Hazard-Approach

Jestliže vezmeme v úvahu koncepty stanovené OSN [12] a EU [13], tak řízení území či jiného systému znamená řízení bezpečnosti příslušné entity. Přístup All-Hazard-Approach [5] znamená zvažovat při řízení bezpečnosti všechny možné druhy pohrom, tj. jevů, které mohou

způsobit škody, ztráty a újmy člověku a aktivům, na kterých závisí jeho život [1]. Logickou syntézou údajů získaných výzkumem, popsaným v práci [14], byl navržen procesní model pro řízení bezpečnosti území zacílené na bezpečí a rozvoj lidí, který zohledňuje přežití lidí při kritických podmínkách, obrázek 6. První dva kroky se dělají pro každou pohromu odděleně. Ve třetím kroku se provádí hodnocení opatření a činností vůči jednotlivým pohromám a zvažuje se fakt, že některá opatření a činnosti jsou v reálném území konfliktní, a proto se provádí jejich optimalizace při zvážení všech možných pohrom do velikostí, kterou jsou hodnoty projektových pohrom. Vyžadují se doklady o zajištění odezvy, jejím materiálním, technickém, personálním a znalostním zajištění, a také průkaz příslušných kompetenci a odpovědností.. Ve čtvrtém kroku se zvažují nadprojektové pohromy a závažnost jejich dopadů, identifikují se rozhraní pro vznik sociální krize a hledají se nápady pro zajištění přežití obyvatel území.




***Obr. 6 – Procesní model řízení bezpečnosti území.***
***Fig. 6 – Process model of management of safety of territory.***

Uvedený procesní model byl vyzkoušen v praxi specifickým šetřením (123 specialistů) pro: kategorie území - vesnické osídlení, městská zástavba, průmyslový region, zemědělský region, a zalesněné území s tím, že kategorie se určuje dle převládajícího charakteru daného území; a osm vybraných pohrom (povodeň, zemětřesení, ztráta kontroly na nebezpečnými látkami, výpadek elektřiny, výpadek kybernetické infrastruktury, hromadné onemocnění,

úmyslný útok na lidskou společnost, selhání vazeb v lidské společnosti) o velikosti podprojektové, projektové a nadprojektové, a osvědčil se [10,14,15]. Proto se aplikoval i na entity další, tj. i kritické komplexní objekty [10] a jeho výsledky se použily pro zvýšení odolnosti, a tím i bezpečnosti konkrétních komplexních objektů. Protože kritické objekty jsou důležité pro lidi při stabilizaci situace, obnově území po pohromě a pro další rozvoj (konkurenceschopnost, zaměstnanost apod.), tak je třeba dbát i o zajištění kontinuity kritických objektů. Jelikož zde vznikají konflikty, tak se zpracovává speciální nástroj, kterým je plán řízení rizik [16].

### 5.2 Aplikace přístupu Defence-In-Depth

Na základě znalostí uvedených v pracích [3,4,6,8,17-19] a zkušeností z praxe, autorka ***metodou analogie*** uspořádala základní principy pro řízení bezpečnosti kritických objektů typu systém systémů (obrázek 7) takto:

**Error! Objects cannot be created from editing field codes.**

***Obr. 7 - Pětistupňový systém řízení bezpečnosti složitého objektu.***
***Fig. 7 – Five steps system of complex facility safety management.***

1. V návrhu, výstavbě a konstrukci inherentně používat principy bezpečného projektu (přístupy: All-Hazard- Aproach, proaktivní, systémový aplikující integrální riziko, tj. i 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 (tj. aplikace All-Hazard-Approach). Na základě recentního poznání, shrnutého v pracích [3,4], 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.
2. Řídicí systém objektu musí mít základní řídicí funkce, alarmy a reakce operátora zpracované tak, aby objekt byl udržen v normálním (stabilním) stavu za normálních podmínek.
3. 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…).
4. 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).
5. 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.

## 6 PROCESNÍ MODEL PRO ŘÍZENÍ BEZPEČNOSTI V ČASE

Na základě současného poznání, shrnutého v pracích [1-4,8,20], systém řízení bezpečnosti (tzv. SMS – Safety Management System) komplexního objektu je postaven na zásadách

procesního řízení a zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v území. Zpravidla se týká řady otázek, kromě jiného i organizace, pracovníků, identifikace a hodnocení ohrožení a z nich plynoucích rizik, řízení chodu organizace, řízení změn v organizaci, nouzového a krizového plánování, monitorování bezpečnosti, auditů a přezkoumávání [1,20]. Skládá se z šesti procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií. Uvedené procesy se dále dělí na podprocesy.

První proces se skládá z podprocesů pro: celkovou koncepci; dosahování dílčích cílů bezpečnosti; vedení / správu bezpečnosti; systém řízení bezpečnosti; personál a zahrnuje úseky pro: řízení lidských zdrojů, výcvik a vzdělání, vnitřní komunikaci / informovanost a pracovní prostředí; revize a hodnocení plnění cílů v bezpečnosti. Druhý proces se skládá z podprocesů pro: identifikaci ohrožení od možných pohrom a hodnocení rizika; dokumentaci postupů (včetně systémů pracovních povolení); řízení změn; bezpečnosti ve spojení s kontraktory; a dozor nad bezpečností výrobků. Třetí proces zahrnuje podprocesy pro: výzkum a vývoj; projektování a montáže; inherentně bezpečnější procesy; technické standardy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů. Čtvrtý proces obsahuje podprocesy pro: spolupráci se správními úřady; spolupráci s veřejností a dalšími zúčastněnými (včetně akademických pracovišť) ; a spolupráci s dalšími podniky. Pátý proces obsahuje podprocesy pro: plánování vnitřní (on-site) připravenosti; usnadnění plánování vnější (off-site) připravenosti (za kterou odpovídá veřejná správa); a koordinaci činností resortních organizací při zajišťování nouzové připravenosti a při odezvě. Šestý proces má podprocesy pro: zpracování zpráv o pohromách, haváriích, skoro nehodách a dalších poučných zkušenostech; vyšetřování škod, ztrát a újmy a jejich příčin; a odezvu a následné činnosti po pohromách (včetně aplikace poučení a sdílení informací). Koordinace procesů je zacílena na zajištění bezpečného objektu za podmínek normálních, abnormálních a kritických.

Na základě analýz existujících systémů řízení bezpečnosti, popsaných v odborné literatuře, o nichž jsou údaje shrnuté v pracích [1-4,8,20], a především poznatků shromážděných OECD [2,21-23] autorka sestavila metodou analogie k existujícím modelům řízení bezpečnosti obecný procesní model systému řízení bezpečnosti entity, ověřila ho na datech shromážděných v archivu [15] a metodou analogie převedla pro kritické složité objekty, obrázek 8. Z obrázku 8 je zřejmá zásadní role konceptu bezpečnosti objektu průběžného hodnocení integrálního rizika a závažných dílčích rizik. V případě, že se při hodnocení zjistí, že riziko je nepřijatelné, je třeba provést změny, jak naznačují zpětné vazby na obrázku 7. Protože změny vyžadují zdroje, síly a prostředky, tak na základě zajištění hospodárnosti se nejprve realizuje zpětná vazba 1, a teprve, když nepřinese žádoucí stav, tak se realizuje zpětná vazba 2; poté zpětná vazba 3, a když ani po ní není žádoucí výsledek, tak zpětná vazba 4. V případě výskytu extrémních jevů s katastrofickými dopady se přikračuje okamžitě k realizaci zpětné vazby 4.

**Error! Objects cannot be created from editing field codes.**

***Obr. 8 - Procesní model řízení bezpečnosti komplexního kritického objekt.u v čase. Procesy:*** *1-* *koncepce a řízení; 2 - administrativní postupy;3 - technické záležitosti; 4 - vnější spolupráce; 5 -* ***nouzová připravenost; a 6 - dokumentace a šetření havárií.***

***Fig. 8 - Process model of management of safety of complex critical facility in time. Processes: 1- concept and management; 2 - administrative procedures; 3 – technical matters; 4 – outside co-operation; 5 – emergency preparedness; and 6 – documentation and accident examination.***

Systém řízení bezpečnosti (SMS) kritického objektu se opírá o koncepci prevence pohrom či alespoň jejich závažných dopadů [1,2,21], která zahrnuje povinnost zavést a udržovat systém řízení, ve kterém jsou zohledněny dále uvedené problémy:

1. Role a odpovědnosti osob podílejících se na řízení závažných nebezpečí, která jsou spojená s možnými pohromami na všech organizačních úrovních kritického objektu a opatření na zajištění výcviku, která jsou sladěna s identifikovanými potřebami výcviku.
2. Plány pro systematické identifikování závažných nebezpečí spojených s možnými pohromami a z nich plynoucích rizik, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti).
3. Plány a postupy pro zajištění bezpečnosti všech komponent, systémů a funkcí v kritickém objektu a v jeho okolí, a to včetně údržby objektů, zařízení.
4. Plány na implementaci změn v kritickém objektu a v objektech i zařízeních, které jsou v okolí.
5. Plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na možné nouzové situace.
6. Plány pro průběžné hodnocení souladu s cíli vyjasněnými v koncepci bezpečnosti a zabudovanými v SMS, a účinné mechanismy pro vyšetřování a provádění korekčních činností v případě selhání s cílem dosáhnout stanovené cíle.
7. Plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků kritického objektu.

# 7 ZÁVĚR

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie. Analýzy havárií: rozlomení plošiny Alpha v r. 1988 v Severním moři; havárie skladu leteckého petroleje v Buncefieldu 11. 12. 2005; neobjasněné námořní, vlakové a letecké havárie v posledních letech; havárie v jaderné elektrárně Fukushima 11. 3. 2011 (pozn. - nebyly respektovány vypočtené scénáře havárií), ukázaly , že řada odborníků bývá postižena provozní slepotou a po splnění požadavků norem a standardů nevidí zbylá rizika nebo rizika spojená s různými vazbami a spřaženími s okolím. Např. prosté srovnání intervalů používaných při pravděpodobnostních hodnoceních ukazuje, že: interval $(-\sigma,+\sigma)$ pokrývá 68.5 % případů; interval $(-2\sigma,+2\sigma)$ pokrývá 95.4 % případů; a interval $(-3\sigma,+3\sigma)$ pokrývá 99.8 % případů [4].

Proto nyní připouštíme, že složité kritické objekty 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. Z důvodu zajištění bezpečnosti kritických objektů a ochrany lidí hledáme řešení odezvy pro možné případy, které nelze odhalit pravděpodobnostními přístupy a budujeme pro ně náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik záchranářů.

***Dosažení požadované úrovně bezpečnosti znamená dobře řídit a správně rozhodovat.*** Dobré / správné řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici. Data musí být: správná, tj. zná se jejich velikost a přesnost; a musí mít vypovídací schopnost pro řešený problém, tj. musí být validovaná. Datové soubory musí být reprezentativní, tj.: úplné; obsahovat správná data; mít dostatečný

počet dat; data musí být rozprostřena homogenně v celém sledovaném intervalu a musí být validovaná. Při aplikaci modelů musí být správně zváženy nejistoty a neurčitosti v datech.

Je si nutno uvědomit, že v reálném světe při zajišťování bezpečnosti kritických objektů řešíme netriviální problémy, tj.: je více chráněných aktiv, jejichž cíle jsou konfliktní; aktiva se mění v čase a prostoru; a prostředí, ve kterém jsou aktiva, tj. lidský systém se dynamický vyvíjí.

## LITERATURA

[1] PROCHÁZKOVÁ, Dana: *Strategické řízení bezpečnosti území a organizace*. ČVUT, 2011 Praha, 483p. ISBN 978-80-01-04844-3.

[2] OECD: *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. OECD, 2002, Paris, 191p.

[3] PROCHÁZKOVÁ, Dana: *Bezpečnost kritické infrastruktury*. ČVUT, 2012 Praha, 318p. ISBN: 978-80-01-05103-0.

[4] PROCHÁZKOVÁ, Dana: *Základy řízení bezpečnosti kritické infrastruktury*. ČVUT., 2013 Praha, 223p. ISBN 978-80-01-05245-7.

[5] FEMA: *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. FEMA, 1996 Washinton.

[6] IAEA: Assessment of defence in depth for nuclear power plants. Safety report series No. 46. IAEA, 2005 Vienna, 119p. ISBN: 92–0–114004–5.

[7] PROCHÁZKOVÁ, Dana: *Řízení rizik složitých technologických systémů.* STRIX, 2014 Žilina, 98-115, ISBN 978-80-89281-91-6.

[8] PROCHÁZKOVÁ, Dana: *Analýza a řízení rizik*. ČVUT, 2011 Praha, 405p. ISBN 978-80-01-04841-2.

[9] PROCHÁZKOVÁ, Dana: *Optimum Concept of Management and Trade-off with Risks.* In: Safety and Reliability: Methodology and Application. Taylor & Francis Group, 2014 London, pp 1463-1471. ISBN 978-1-138-02681-0.

[10] PROCHÁZKOVÁ, Dana: *Archiv řešených úloh z oblasti řízení bezpečnosti a krizového řízení.*ČVUT v Praze, fakulta dopravní, ústav bezpečnostních technologií a inženýrství.

[11] HAIMES, Y,.Y.: *Risk Modeling, Assessment, and Management*. John Wiley & Sons 2009. 1040p. ISBN: 978-0-470-28237-3.

[12] UN: *Human Development Report*. UN, 1994 New York, www.un.org.

[13] EU: *The Safe Community Concept*. EU, 2004 Brussels, PASR project.

[14] PROCHÁZKOVÁ, Dana: *Nástroj pro sestavení podkladů pro řízení bezpečnosti.* In: Bezpečnost a ochrana zdraví při práci 2011. VŠB-TU, 2011 Ostrava, 157-169. ISBN 978-80-248-2424-6.

[15] PROCHÁZKOVÁ, Dana: *Critical Infrastructure Safety Management.* In: Reliability, Risk and Safety. Theory and Applications. Balkema, 2009 Leiden, pp 1875-1882. ISBN 978-0-203-85975-9.

[16] PROCHÁZKOVÁ, Dana: *Plány pro řízení rizik jsou též nástroje podporující optimální řešení konfliktů u kritických objektů*. In: Fire Safety 2014. SPBI, 2014 Ostrava. ISBN: 978-80-7385-149-1.

[17] NOWAKOWSKI Tomasz et al. (eds): *Safety and Reliability: Methodology and Application.* Taylor & Francis Group, 2014 London, 2453p. ISBN 978-1-138-02681-0.

[18] SEVCIK, A., GUDMESTADO. T.: *Solutions and safety barriers: The holistic approach to risk-reducing measures*. In: Safety and Reliability: Methodology and Application. Taylor & Francis Group, 2014 London, ISBN 978-1-138-02681-0.

[19] VATN, J.: *Structuring contributors to successful operation*. In: Safety and Reliability: Methodology and Application. Taylor & Francis Group, 2014 London. ISBN 978-1-138-02681-0.

[20] PROCHÁZKOVÁ, Dana: *Ochrana osob a majetku*. ČVUT, 2011 Praha, 301p. ISBN: 978-80-01-04843-6.

[21] OECD: *Guiding Principles on Chemical Accident Prevention, Preparedness and Response*. OECD, 2003 Paris, 192p.

[22] OECD: *Environmental Indicators: Overview of Work Programme and Publications.Group on the State of the Environment*. OECD, 1993 Paris.

[23] OECD: Indicators to measure decoupling of environmental pressure from economic growth. OECD SG/SD(2002)1/FINAL, 16. 5. 2002.