Sustainability - Environment - Safety ´2015
Zborník z medzinárodnej vedeckej konferencie, Bratislava, 4. december 2015
Proceedings of the International Scientific Conference, Bratislava, December 4, 2015, Slovak Republic
■ Žilina: Strix. Edícia ESE-25, Prvé vyd., ISBN 978-80-89753-01-7 ■ Rusko, M.- Kollár, V. [Eds.] ■

VYBRANÉ METODY POUŽÍVANÉ V BEZPEČNOSTNÍM INŽENÝRSTVÍ

Dana PROCHÁZKOVÁ

SELECTED METHODS USED IN SECURITY AND SAFETY ENGINEERING

ABSTRAKT
BEZPEČNOSTNÍ INŽENÝRSTVÍ V POJETÍ „INŽENÝRSTVÍ BEZPEČNOSTI“ JE SYSTEMATICKÉ VYUŽITÍ INŽENÝRSKÝCH ZNALOSTÍ A ZKUŠENOSTÍ PRO OPTIMALIZACI OCHRANY LIDSKÝCH ŽIVOTŮ, ŽIVOTNÍHO PROSTŘEDÍ, MAJETKU A EKONOMICKÝCH ZÁJMŮ, TJ. OPTIMÁLNÍ DOSAŽENÍ BEZPEČÍ A UDRŽITELNÉHO ROZVOJE LIDSKÉHO SYSTÉMU. JEHO HLAVNÍM CÍLEM JE SNÍŽENÍ VŠECH TYPŮ ŠKOD A ZTRÁT VYVOLANÝCH POHROMAMI VŠEHO DRUHU NA AKTIVECH LIDSKÉHO SYSTÉMU PROSTŘEDNICTVÍM CÍLENÉHO ŘÍZENÍ RIZIK. Z ODBORNÉHO POHLEDU JDE O PROCES HLEDAJÍCÍ VŠECHNY POTENCIÁLNÍ STAVY, KTERÉ BY OHROŽOVALY ÚSPĚŠNÉ FUNGOVÁNÍ JEDNOTLIVÝCH SYSTÉMŮ TVOŘÍCÍCH LIDSKÝ SYSTÉM VE VŠECH ETAPÁCH JEJICH ŽIVOTNOSTI, A IDENTIFIKUJÍCÍ MOŽNOSTI PRO JEJICH ZVLÁDNUTÍ PREVENCÍ, PŘIPRAVENOSTÍ, ODEZVOU A OBNOVOU. PŘITOM POUŽÍVÁ METODY, NÁSTROJE A TECHNIKY, KTERÉ INDIKUJÍ, JAK: STRUKTUROVAT PROBLÉM; STANOVIT TO, CO SE MÁ ŘEŠIT; SEBRAT A VYTVOŘIT DATA, ABY MĚLA VYPOVÍDACÍ HODNOTU K DANÉMU PROBLÉMU; VYBRAT METODU PRO ZPRACOVÁNÍ DAT, ABY VÝSLEDKY ZPRACOVÁNÍ BYLY RELEVANTNÍ K DANÉMU PROBLÉMU; INTERPRETOVAT VÝSLEDKY ZPRACOVÁNÍ DAT V DANÝCH PODMÍNKÁCH; A JAK IMPLEMENTOVAT VÝSLEDKY DO PRAXE S OHLEDEM NA CÍL. PŘEDLOŽENÁ PRÁCE OBSAHUJE PŘEHLED VYBRANÝCH ZÁSTUPCŮ ŘADY EXAKTNÍCH METOD, NÁSTROJŮ A TECHNIK.

Klíčová slova: *bezpečí, bezpečnost, systém, riziko, metody*

ABSTRACT
SAFETY ENGINEERING IN THE CONCEPT OF "SAFETY ENGINEERING" IS THE SYSTEMATIC USE OF ENGINEERING KNOWLEDGE AND EXPERIENCE TO OPTIMIZE THE PROTECTION OF HUMAN LIVES, THE ENVIRONMENT, PROPERTY AND ECONOMIC INTERESTS, I.E. THE OPTIMAL ACHIEVEMENT OF SECURITY AND SUSTAINABLE DEVELOPMENT OF THE HUMAN SYSTEM. ITS MAIN OBJECTIVE IS THE REDUCTION OF ALL TYPES OF DAMAGES AND LOSSES CAUSED BY DISASTERS OF ALL KINDS ON THE ASSETS OF THE HUMAN SYSTEM THROUGH TARGETED RISK MANAGEMENT. FROM THE PROFESSIONAL POINT OF VIEW, THE PROCESS OF SEARCHING FOR ALL THE POTENTIAL SITUATIONS THAT ENDANGER THE SUCCESSFUL FUNCTIONING OF THE VARIOUS SYSTEMS THAT MAKE UP THE HUMAN SYSTEM AT ALL STAGES OF THEIR LIFE, AND IDENTIFYING OPTIONS FOR THEIR MASTERY BY PREVENTION, PREPAREDNESS, RESPONSE AND RECOVERY. USING THE METHODS, TOOLS AND TECHNIQUES THAT INDICATE HOW TO: STRUCTURE THE PROBLEM; DETERMINE WHAT YOU WANT TO DEAL WITH; COLLECT AND CREATE DATA THAT DESCRIBE THE PROBLEM; SELECT A METHOD FOR PROCESSING THE DATA, THE RESULTS WERE RELEVANT TO THE PROCESSING OF THE PROBLEM; INTERPRET THE RESULTS OF PROCESSING DATA IN THE GIVEN CONDITIONS; AND HOW TO IMPLEMENT THE RESULTS INTO PRACTICE WITH REGARD TO THE TARGET. SUBMITTED WORK PROVIDES AN OVERVIEW OF SELECTED REPRESENTATIVES OF THE FAMILY OF EXACT METHODS, TOOLS AND TECHNIQUES.

Keywords: *security, safety, system, risk, methods*

1. Úvod do problematiky

Cílem každého člověka je být stále v bezpečí a rozvíjet se, tj. nacházet se v bezpečném lidském systému s udržitelným rozvojem; pojem lidský systém (Human System) se používá systematicky od r. 1994 a představuje minimální prostor pro život člověka a lidskou společnost, tj. dle současných znalostí zahrnuje aktiva, kterými jsou životy a zdraví lidí, životní prostředí, majetek, veřejné blaho, technologie, infrastruktury a vazby a toky mezi těmito prvky (v odborné literatuře se používají často pojmy: veřejná aktiva, chráněné zájmy, veřejné chráněné zájmy, právem chráněné zájmy; ve specifických podsystémech lidského systému jako jsou průmyslový podnik, služby apod. pak přibývají další aktiva, např. splnění požadavků statutu organizace, profit a soulad s požadavky zřizovatele). Bezpečí člověka (lidské bezpečí – Human Security) na základě současného poznání vyžaduje stav lidského systému, při kterém vznik újmy na lidech má přijatelnou pravděpodobnost. Bezpečí je narušováno mnoha jevy, které mají různou fyzikální, biologickou, chemickou, kybernetickou aj. povahu [1-3] a souhrnně se nazývají pohromy (Disasters). Bezpečnost lidského systému (Human System Safety) představuje uspořádaný soubor opatření a činností, kterými se zajišťuje bezpečí a udržitelný rozvoj lidského systému; analogicky pak představa platí pro další systémy jako systém biosféry, podnik jako technologický objekt nebo infrastruktura, území atd. [1,2]. Soubor opatření a činností vychází z logiky každého sledovaného systému a aplikací na základě sofistikovaného řízení

rizik zajišťuje, že každý člověk žije a pracuje v podmínkách, ve kterých jsou známá ohrožení (Hazards) a rizika (Risks) s nimi spojená mají přijatelnou úroveň [1,2,4].
Ochrana obyvatelstva, lidských životů, majetků, území i objektů vždy v historii lidstva náležela k základním nástrojům, kterým vědomě a nevědomě věnovali péči a pozornost náčelníci kmenů, později vládcové a vedoucí sociálních i státních struktur. Měla různé rozměry, různou intenzitu, ale i rozdílné důvody. Postupem doby se ochrana před přírodními pohromami a pohromami vlastními lidské společnosti (boj o jídlo, války) rozšířila i na ochranu před pohromami vyvolanými lidskými činnostmi (průmyslové havárie, znečištění životního prostředí, kontaminace potravního řetězce, eroze krajiny) a dnes člověk zvažuje ochranu před dopady velkých kosmických těles i před útoky mimozemšťanů na planetu Zemi. Všeobecně se již také přijímá, že bezpečnost každé osoby (Human Safety) je společnou odpovědností průmyslu, společenství a vlády (veřejné správy) [1,2,4].
Idea o bezpečnosti souvisí s historií lidí. Významně se začala rozvíjet v období průmyslové revoluce, když se ukázalo, že zvyšování bezpečnosti průmyslu je nákladově efektivní a tak se postupně přijaly i požadavky na bezpečné území, ve kterém jsou aktiva lidského systému v bezpečí.

2. Přehled poznatků používaných v inženýrství podporujícím bezpečnost

Inženýrství je široká disciplína, která řeší problémy od jejich pochopení, přes návrh řešení až po realizaci v daných podmínkách. Je hnací silou lidského vývoje, protože se zabývá i problémy, které je obtížné přesně řešit. K tomu používá kreativitu lidských jedinců a přístupy označované jako dobrá praxe. V současné době vychází ze systémového přístupu a pro zajištění současných cílů, kterými jsou bezpečný podnik, bezpečná komunita, bezpečný region atd. [1,2] používá specifické disciplíny, které budou dále analyzovány.

2.1. Inženýrská odbornost a dobrá inženýrská praxe

V pracích [4,5] je inženýrská odbornost chápaná jako výraz schopnosti při řešení problému: aplikovat znalosti matematiky, vědy a inženýrství; navrhnout a realizovat experimenty; analyzovat a interpretovat data; navrhnout komponenty nebo celý systém podle požadavků a v rámci realistických omezení identifikovat, formulovat a řešit inženýrské problémy; efektivní komunikace; chápat dopady inženýrských řešení v širším kontextu; využívat nejmodernější nástroje a metody v inženýrské praxi; dodržovat profesionální a profesní odpovědnosti a etiky; a vést interdisciplinární tým.
Dobrá inženýrská praxe (dobrý inženýrský postup) se pak definuje jako soubor inženýrských metod a standardů, které se používají během životního cyklu technického systému s cílem dosáhnout vhodné a nákladově efektivní řešení. Je podporována vhodnou dokumentací (konceptuální dokumentace, diagramy, manuály, zprávy z testování apod.). Jedná se o osvědčené postupy v jednotlivých oblastech, které na základě zkušeností vedou k dobrému výsledku. Uvedený postup se používá v případech, ve kterých nebyl schválen jednotný postup a je častý při měření v laboratořích, jednání s lidmi atd.

2.2. Disciplíny zaměřené na zajištění bezpečných objektů a jejich bezpečného okolí

Pokrok při řešení inženýrských problémů přineslo zapracování systémového pojetí a s ním spojená orientace na rizika a jejich řízení. Vznikly specifické disciplíny, které umožnily pokrokové řešení komplexních inženýrských problémů v oblastech jaderné energetiky, kosmonautiky apod. Řešením komplexních úkolů praxe se tvůrčími přístupy schopných odborníků vytvořily nové postupy a specifické soubory postupů, které propojily již známé metody, nástroje a techniky z různých oborů, mnohdy je dopracovaly do určitých praktických forem a tím vytvořily potenciál k úspěšnému řešení úkolů dalších.

2.2.1. Systémová bezpečnost

Aplikací systémového přístupu v inženýrských oborech vznikla disciplína „bezpečnost systému (System Safety)“ do češtiny převedená pod názvem systémová bezpečnost, která se aplikovala především v průmyslu a v odvětvích s ním souvisejících. Uvedená disciplína definovala: systém jako kombinaci lidí, postupů a zařízení, které jsou integrované tak, aby se prováděl specifický provozní úkol nebo funkce ve specifickém prostředí; a koncept bezpečnosti systému jako aplikaci speciálních technických a organizačních dovedností s cílem systematicky předcházet identifikací ohrožení a řízením rizik s nimi spojených škodám a ztrátám na aktivech lidského systému, a to během celé životnosti každého zařízení vytvořeného a realizovaného člověkem. OECD postupem doby rozpracovala samostatné koncepty pro jaderný a chemický průmysl [1,2].

2.2.2. Rizikové inženýrství

Cílem inženýrství rizika (Risk Engineering) v češtině označovaného jako rizikové inženýrství bylo a je snížit jen rizika technických systémů spojená s vnitřními zdroji rizik. Riziko - pro potřeby praxe je vyjádřeno jako pravděpodobná velikost ztrát, škod a újmy na sledovaných aktivech, které způsobí daná pohroma o specifikované velikosti a která se rozpočítá na určitou časovou jednotku (obvykle 1 rok) a určitou územní jednotku. Při úvahách v praxi rozlišujeme, zda realizace rizika probíhá stále stejným způsobem nebo různě v závislosti na momentálních místních a časových podmínkách aktiv. V případě prvním určujeme jakousi střední hodnotu a její oprávněnost pro použití v praxi je spojena s podmínkou, že je zvážen nejméně příznivý případ (nacházíme ho v normách a standardech založených na deterministickém přístupu). Druhý přístup odpovídá skutečnosti, a proto se zvažuje při přípravě všech podkladů pro strategické řízení. Určují se variantní scénáře realizace rizika a pravděpodobnosti jejich výskytu; a z nich se jasným matematickým přístupem určuje střední hodnota a její rozptyl (nacházíme ho v normách a standardech založených na pravděpodobnostním přístupu). V současné praxi se při řešení komplexních případů praxe používají také přesně definované heuristické postupy [6].
Hlavními znaky každého rizika jsou ***nejistota a neurčitost***. Jejich příčiny dělíme na odchylky vznikající při průběhu děje, který je: obvyklý za normálních podmínek systému a vznikají malé variace (zdroj nejistot); skutečný a je vyvolán

príležitostnými změnami procesu v systému vedoucími k výskytu příležitostných extrémních hodnot (zdroj nejistot a příležitostných neurčitosti); a proměnný a je vyvolán změnami procesu v systému způsobeném vnějšími příčinami (zdroj neurčitostí).
Nejistota souvisí s rozptylem pozorování a měření. Lze ji do hodnocení a predikce zapracovat pomocí aparátu matematické statistiky. ***Neurčitost*** souvisí jak s nedostatkem znalostí a informací, tak s přirozenou variabilitou procesů a dějů, které vyvolávají pohromy. Pro zapracování a zvážení neurčitostí je aparát matematické statistiky nedostatečný a je třeba používat jiný, modernější matematický aparát, který poskytují např. teorie extrémních hodnot, teorie mlhavých množin, teorie fraktálů, teorie dynamického chaosu, vybrané expertní metody a vhodné heuristiky [6-8].
Neurčitost dat vyplývá ze skutečnosti, že data jsou neúplná, nehomogenní (tj. jejich přesnost závisí na jejich velikosti nebo na čase výskytu) a nestacionární, tj. data mají značný rozptyl a jsou zatížená náhodnými a někdy i systematickými chybami, jejichž funkce rozdělení obvykle není možno stanovit. Protože není nic absolutně přesného, tak obecně u každé veličiny, kterou zkoumáme, musíme zvažovat nejistoty a neurčitosti dat. Proto bezpečnostní i rizikové inženýrství vyžadují, aby se při řešení úkolů ověřovala kvalita datových souborů z hlediska jejich věrohodnosti s ohledem na daný úkol.

V rizikovém inženýrství [4-7] se pro stanovení rizika používají dále uvedené zásady:

- riziko se stanovuje až po návrhu systému,
- stanovení rizika se zaměřuje na úroveň systému a jeho komponent, tj. nebere se v úvahu vnější prostředí a ochrana veřejných aktiv, která stanovuje veřejný zájem,
- vyžadují se znalosti systému a procesů, tj. nevyžadují se znalosti vnějšího prostředí a ochrana aktiv, která stanovuje veřejný zájem,
- existuje-li riziko, pak se blíže určuje, ale reálně se nikdy neodstraní rizika spojená s nevhodným řešením pro dané místo.

Rizikové inženýrství se opírá se o řízení rizik a hledá řešení problému tak, že zvažuje pohromu po pohromě a vyžaduje vypořádání všech rizik, jejichž pravděpodobnost výskytu je větší nebo rovna 0.05. Obvykle zahrnuje jen pohromy, jejichž zdroje jsou uvnitř systému, velmi často řeší jen technické aspekty problému, tj. zabývá se jen systémovou bezpečností.

2.2.3. Recentní inženýrské disciplíny zaměřené na bezpečnost

Řízení bezpečnosti systému je disciplína, která aplikuje metody, nástroje a techniky založené na inženýrských a manažerských přístupech tak, aby systém i okolí byly bezpečné. Opírá se o řízení rizik, ve kterém je zapracován princip předběžné opatrnosti. V případě komplexního řízení bezpečnosti jde o řízení komplexního (integrálního) rizika. Komplexní (integrální) řízení bezpečnosti je pak disciplína pro řízení bezpečnosti SoS (systému systémů) [4-8].
V průběhu posledních cca 30 let se vytvořily ***dvě inženýrské disciplíny*** zaměřené na zajištění bezpečnosti systému, ***které mají nestejné cíle***, ale v češtině se obě označují jako bezpečnostní inženýrství. Jedná se o:

- Disciplínu mající cíl zajistit, aby každý technický systém vytvořený člověkem a implementovaný do lidského systému nebyl zdrojem nepřijatelných rizik ani v technickém systému, ani v lidském systému. Zabývá se proto jak technickým systémem, tak jeho okolím, a to po celou dobu životnosti systému, tj. neřeší jen technické problémy systému, ale respektuje také veřejná aktiva v okolí systému (tj. životy a zdraví lidí, majetek, veřejné blaho, životní prostředí a okolní technické objekty a infrastruktury). Nazývá se inženýrství bezpečnosti (Safety Engineering) [4]. Používá se v souvislosti s jadernými, chemickými a jim podobnými objekty, leteckou dopravou, přepravou nebezpečných látek atd. Je třeba poznamenat, že inherentně v sobě zahrnuje ochranu životního prostředí (viz aktivity Technology Assessment [2]) a jeho konflikty s pravověrnými ekology zpravidla pramení z nedostatku znalostí a z nedostatečné schopnosti této skupiny ekologů pochopit priority, které musí člověk v zájmu svého přežití aplikovat při strategickém řízení území.
- Disciplína mající cíl zajistit, aby každý jednotlivý technický systém byl v bezpečí s ohledem na vnitřní i vnější zdroje rizik. Nazývá se inženýrství bezpečí (Security Engineering) [5]. Aplikuje se např. při zajištění informačních systémů, bank, hranic, kybernetických sítí před útoky, specifických objektů apod.

Z uvedeného je zřejmé, že ***cíle první disciplíny jsou širší, a tudíž jejich dosažení je podstatně náročnější než dosažení cílů druhé disciplíny***. Protože obě disciplíny se liší souborem aktiv, která sledují (první případ – veřejná aktiva + aktiva technického systému, pohromy vnitřní i vnější; druhý případ - aktiva technického systému; pohromy vnitřní i vnější), tj. první disciplína v sobě zahrnuje druhou disciplínu, tak ***se v dalším textu soustředíme na inženýrství bezpečnosti*** a dle zvyklostí v českém jazyce začneme používat pojem „bezpečnostní inženýrství“, i když z věcného hlediska nevystihuje správně cíle.

2.2.4. Aparát pro řešení problémů

Všechny uvedené inženýrské disciplíny pracují s riziky a aplikují metody, nástroje a techniky založené na matematických, inženýrských a manažerských přístupech, které byly postupně na základě zkušeností upraveny do jistých forem, aby řešily problémy praxe tak, aby bylo dosaženo požadovaného cíle. Vznikly velmi specifické formy, které si zaslouží vlastní disciplínu, protože potřebují znalosti metodologické a inženýrské v oblasti technické, ekonomické a organizační, tj. především schopnost řešit problémy praxe a řešení realizovat ve zcela konkrétních podmínkách.
Slovo exaktní v bezpečnostním a rizikovém inženýrství je chápané jako přísně vědecký, tj. fakta jsou zjištěna strukturovatelným, přesně popsaným a opakovatelným způsobem z validovaných dat, tj. data mají oceněné nejistoty a neurčitosti a mají oceněnou vypovídací schopnost ke sledovanému problému.

3. Bezpečnostní inženýrství a jeho specifika

Bezpečnostní inženýrství ve sledovaném pojetí je založeno na řízení bezpečnosti, které je založeno na specifickém řízení rizika [1,2], které se vyznačuje zejména těmito znaky:

- umísťování - projektování - konstrukce - návrh s minimalizaci rizik,
- provozování se začleněním systému včasného varování a procedur pro řízení přijatelné úrovně rizik,
- zvládnutí abnormálních, nouzových a kritických stavů při provozu i odstavení [4-6].

Specifičnost řízení rizik je v tom, že jde o řízení rizik od všech možných pohrom najednou s tím, že aktuální výčet pohrom se určí přístupem All Hazard Approach [3] (tj. zvažuje všechny možné pohromy bez ohledu na to, zda jejich zdroje leží uvnitř nebo vně systému) a že se hledá optimální řešení pro relevantní možné pohromy a přitom používá princip předběžné opatrnosti, do kterého se zahrnuje i udržitelný rozvoj [2].
I když koncepce bezpečnostního inženýrství byla výše vyjádřena technickými pojmy a byla spojená s technickými systémy, tak platí ve všech ostatních oblastech (řízení environmentální bezpečnosti, řízení zdravotní bezpečnosti, řízení mezinárodní bezpečnosti apod.), které jsou důležité pro bezpečný lidský systém s udržitelným rozvojem; jen je třeba použít vhodné převedení pojmů, aby se stala srozumitelnou odborníkům z dílčích disciplín, kteří jsou zvyklí na vlastní terminologii [2].
Bezpečnostní inženýrství při stanovení rizika [4,5] používá zásady:

- riziko se stanovuje během celého životního cyklu sledovaného systému, tj. při umísťování, projektování, výstavbě, provozu i při odstavení z provozu, a popř. i při uvedení území do původního stavu,
- stanovení rizika se zaměřuje na požadavky uživatelů a úroveň poskytovaných služeb,
- rizika se stanovují podle kritičnosti dopadů na procesy, poskytované služby a na aktiva, která stanovuje veřejný zájem,
- nepřijatelná rizika se zmírňují prostřednictvím nástrojů řízení rizik, tj. pomocí technických a organizačních návrhů, standardizací operačních postupů nebo automatizovanou kontrolou.

V technickém slangu mluvíme o tom, že řízením bezpečnosti vytváříme inherentní bezpečnost lidského systému vůči projektovým pohromám a implementací principu předběžné opatrnosti zajišťujeme zvýšení odolnosti vůči nepřijatelným dopadům nadprojektových pohrom, jejichž výskyt je tak málo pravděpodobný, že je nepředvídatelný [2]. V praxi se pak zavádí principy jako „selži bezpečně“, „prováděj jen určené funkce, tj. když nemůžeš splnit cíl, tak nic nedělej“ apod.
Bezpečnostní inženýrství je z odborného pohledu proces, který hledá všechny potenciální stavy, které by ohrožovaly úspěšné fungování sledovaného systému ve všech etapách jeho životnosti, a identifikuje možnosti pro jejich zvládnutí prevencí, připraveností, odezvou a obnovou. Klíčové koncepty bezpečnostního inženýrství jsou:

- Přístup k problému je založený na riziku s tím, že intenzita prací a dokumentace je přiměřená úrovni rizika.
- V odborném postupu, který respektuje logiku řešeného problému, se zvažuji kritické atributy kvality a kritické parametry procesu.
- Řešení problému se orientuje na kritické položky, tj. předmětem je sledování a řízení kritických aspektů technických systémů zajišťujících konzistenci operací systémů.
- Prověřené parametry kvality se objevují již v návrhu projektu řešení problému.
- Klade se důraz na kvalitní inženýrské postupy, což znamená, že se musí prokazovat správnost zvolených postupů v daných podmínkách.
- Během celého životního cyklu je zacílení na zvyšování bezpečnosti (pomocí systémů řízení bezpečnosti), tj. jde o neustále zlepšování procesů s využitím analýzy kořenových příčin poruch a selhání.

Pro dodržení výše uvedených zásad se musí při zpracování podkladů používat relevantní soubory dat a jen ověřené metody, které dají výsledky se stanovenou vypovídací schopností. Kvůli tomu, že v řadě případů se nelze dobře vypořádat s neurčitostmi v datech, se v praxi rizikového i bezpečnostního inženýrství používají postupy označované jako ***postupy dobré praxe*** / postupy dobré inženýrské praxe.

4. Specifika metodologie bezpečnostního inženýrství

Jak již bylo výše uvedeno, tak bezpečnostní inženýrství vychází ze systémového pojetí, a proto kromě běžné metodologie používá také ***systémovou metodologii***, která se zabývá: analýzou systému; projektem systému; implementací řešení sledovaného úkolu; a provozem systému [4,5].
Metodologie bezpečnostního inženýrství při řešení problémů zvažuje, že všechny procesy probíhají v dynamicky proměnném světě, a proto používá speciální aparát, kterým je soubor používaných výzkumných postupů za účelem optimálního řízení rizik [2,4-13].
Na základě ocenění disponibilních datových souborů, existujících nejistot a neurčitostí u dostupných dat rozděluje úkoly praxe, které lze řešit deterministicky nebo stochasticky či jen heuristicky [6]. Využívá integrovaným způsobem kvalitativní a kvantitativní přístupy k riziku a k bezpečnosti systému. V obecné rovině, sestává z dále uvedených kroků:

- definice systému a okolního prostředí,
- identifikace možných nebezpečí, tj. relevantních pohrom,
- ***stanovení ohrožení při extrémních událostech (nadprojektových pohromách),***
- vyhodnocení rizik,

- návrh korekčních a nápravných akcí podle kritérií bezpečnosti s cílem zajistit přijatelné bezpečí,
- verifikace přijatelnosti rizika.

Ve všech úlohách používá metody, nástroje a techniky, které závisí na kvalitě disponibilních dat a na cílech řízení bezpečnosti [6,8].

5. Exaktní metody, nástroje a techniky bezpečnostního inženýrství

Protože bezpečnostní inženýrství je obor, který řeší problémy, tak používá nástroje, metody a techniky, které indikují, jak: strukturovat problém; stanovit to, co se má řešit; sebrat a vytvořit data, aby měla vypovídací hodnotu k danému problému; vybrat metodu pro zpracování dat, aby výsledky zpracování byly relevantní k danému problému; a jak interpretovat výsledky zpracování dat z pohledu bezpečnosti lidského systému, která zahrnuje funkčnost a spolehlivost daného systému.
Z dříve uvedených skutečností vyplývá, že při výběru metod, nástrojů a technik musíme respektovat, že bezpečnostní inženýrství je mnoha oborový a průřezový obor, který používá jak obecné, tak specifické metody, nástroje a techniky. Specifické metody, nástroje a techniky jsou buď jednoduché či komplexní [7,8,10,13]. Komplexní pak představují uspořádané použití několika obecných či jednoduchých metod, nástrojů a technik. Jednotlivé metody, nástroje a techniky, respektují skutečnost, že cílené komplexní řízení bezpečnosti každého systému nelze dosáhnout jenom technicky nebo znalostně, ale kombinací možných a dostupných oborových nástrojů lidské činnosti, tj. musí se používat metody, nástroje a techniky logické, technické, finanční, manažerské a rozhodovací, protože nedílnou součástí bezpečnostního inženýrství je rozhodování o technických problémech, lidském faktoru, nákladech a časovém plánování apod.
To znamená, že pro řešení současných úloh bezpečnostního inženýrství, které vyžadují netriviální řešení problémů, používat vícekriteriální metody, nástroje a techniky [8], ve kterých musíme respektovat, že aktiva i zdroje rizik mají rozdílnou podstatu, která je zdrojem nesouměřitelnosti kritérií, a při jejich výběru musíme: respektovat kvalitu dat, strukturu problému, který řešíme i požadavky na kvalitu výsledku; a speciálně prověřovat jak kvalitu dat (správnost, úplnost, vypovídací schopnost k danému problému), tak při použití expertů jejich kvalifikovanost (IAEA, OECD, USA, WB apod. mají přísná kritéria na posuzování kvalifikace experta).

Podle způsobu získávání dat dělíme metody, nástroje a techniky bezpečnostního inženýrství takto:

- ***Empirické*** - vychází ze zkušeností. Zjišťování faktů se provádí pomocí anket a dotazníků. Používají se při sběru dat o chování člověka a lidské společnosti v sociologii, ale i třeba při zjišťování rozložení dopadů zemětřesení, vichřice či dalších pohrom v území. V exaktních vědách jsou používány pro svoji rychlost a nenáročnost. Přesnost získaných dat ve srovnání s měřením pomocí přístrojů je menší, ale kvalifikované statistické zpracování dává dobré a spolehlivé informace pro rozhodování a řízení.
- ***Teoretické*** - vytvářejí poznatky, hypotézy, teoretické konstrukty na základě obecně vědních postupů, tj. jsou založené na používání algoritmů, které vedou k vyřešení všech úloh daného typu. Nejjednodušší příklady algoritmů jsou aritmetická pravidla, sčítání, odčítání atd.
- ***Expertní*** - využívají odborníka (odborníky) pro činnost, která vyžaduje zvláštní znalosti. Jsou používány v mnoha situacích, jejichž společným znakem je nutnost odborného (expertního) posouzení problému a jeho dalšího vývoje v budoucnosti. K použití vede i situace, kdy je třeba vyloučit lokální pohled na předmětnou problematiku a posoudit ji nezávisle v novém, širším nebo specializovanějším pohledu / rámci.

Podle způsobů získávání znalostí dělíme metody, nástroje a techniky bezpečnostního inženýrství následovně:

- ***Postupy pro získání základních (obvykle jednotlivých) znalostí*** – jako zjištění vlastností a chování sledovaného objektu za různých podmínek, např. zjištění typických vlastností určité látky, chování nanomateriálů za různých fyzikálních a chemických podmínek apod.
- ***Postupy pro řešení jednoduchých úkolů praxe – jako alokace a aplikace základních znalostí v praxi***, např. typický scénář dopadů zemětřesení z jedné ohniskové oblasti v určitém území, způsob odezvy na únik chlóru ze sledovaného objektu apod. Zde již musíme řešit, zda při získání dat jsme závislí na tom, zda sledovaný jev je opakovatelný či nikoliv (např. měření jistého přírodního jevu je neopakovatelné) a jak nepřesnosti zjišťování faktů ovlivní nejistoty a neurčitosti v datech, a tím i ve znalostech.
- ***Postupy pro řešení úloh strategického rázu*** – jako zjištění základních znalostí pro podporu schopnosti řešit efektivně současné a budoucí problémy sledovaného objektu, např. spojené s bezpečím a udržitelným rozvojem lidského systému, spojené s rozvojem lidské společnosti v určitém území. Zde již musíme řešit, jak jsme při získání dat závislí na tom, zda sledované procesy jsou či nejsou stabilní v prostoru a čase (např. proces výskytu povodní, zemětřesení atd. není stabilní v čase – extrémní jevy se vyskytují řídce a nepravidelně v čase a prostoru) a jak nepřesnosti zjišťování faktů ovlivní nejistoty a neurčitosti v datech, a tím i ve znalostech, a co z toho vyplývá pro predikci a následně řízení, tj. jde o kvalifikovaný výběr z variant jistého řešení problémů, které připouští rozmanité kombinace sledovaných parametrů.

6. Příklady metod, nástrojů a technik, které používá bezpečnostní inženýrství

Metod, nástrojů a technik, které jsou používány v bezpečnostním inženýrství, je mnoho. Některé jsou všeobecně známé, např. metody aritmetiky, algebry, geometrie, logiky apod. Následují metody matematické statistiky, shluková a faktorová analýza, aplikace časových řad apod., metody operačního výzkumu, metody síťové analýzy, specifické metody pro podporu

rozhodování a řízení, a specifické pro bezpečnostní a rizikové inženýrství; viz [8,14,15]. Z hlediska použití v praxi jsou příklady rozděleny do tří skupin, a to: obecné postupy; specifické nebo speciálně upravené postupy; a zvláštní postupy.

6.1. Příklady používaných obecných postupů

V práci [8] jsou popsány dále uvedené metody, nástroje a techniky:

- *Analytical Hierarchy Process (AHP);*
- *Analýza metodou křížových interakcí;*
- *Analýza metodou stromu událostí* (ETA – Event Tree Analysis);
- *Analýza příčin a důsledků;*
- *Analýza nákladů a efektivity* (CEA - Cost - Effectiveness Analysis);
- *Analýza nákladů a užitků* (CBA - Cost - Benefit Analysis);
- *Analýza s cílem stanovit nejmenší náklady* (CMA - Cost - Minimize Analysis);
- *Analýza nákladů a přínosů podle užitečnosti* (CUA - Cost - Utility Analysis);
- *Aplikace myšlenkové mapy;*
- *Aplikace stromu problému;*
- *Aplikace obrazových a myšlenkových schémat;*
- *Benchmarking;*
- *Citlivostní analýza a testy citlivosti;*
- *Diagram příčin a následků;*
- *Fullerova metoda;*
- *Gordonova metoda;*
- *Heuristické metody pro strukturování problémů* (metody založené na heuristických algoritmech jsou např.: analýza aktérů (Stakeholders analysis); analýza hranic (Boundary analysis); analýza událostí (Event analysis); brainstorming; brainwriting; diagram proč-proč (Why-why diagram); diagram rybí kosti (Fishbone diagram); dimenzionální analýza (Dimensional analysis); hierarchická analýza (Hierarchy analysis); kauzální model (Causal loop models); klasifikační analýza (Classificational Analysis); myšlenkové mapy (Mind maps); a strom problémů (Problem Tree);
- *Hodnocení techniky* (Technology Assessment);
- *Išikavův diagram* (Ishikawa Diagram = graf rybí kosti, graf rybí páteře);
- *Kauzální analýza* (analýza příčin);
- *Kvantifikace rizika; Riziková matice;*
- *Marginální analýza* (tj. analýza mezních nákladů, mezních přínosů a mezních stavů posuzovaného problému / úkolu);
- *Matematické programování;*
- *Matice odpovědnosti;*
- *Metody cílového prognózování;*
- *Metoda delfská* (DELPHI) jednostupňová a vícestupňová;
- *Metoda duální ALO-FUL;*
- *Metoda extrapolace;*
- *Metoda hlavního článku;*
- *Metoda hodnocení dosažitelnosti* (Goals Achievement Matrix – GAM);
- *Metoda hodnocení variant* - obvykle vícekriteriální;
- *Metoda hodnotové analýzy;*
- *Metoda mezních odhadů;*
- *Metoda mlhavých množin* (Fuzzy Set);
- *Metoda Monte Carlo;*
- *Metoda orientovaná na cíle* (MBO - Management by Objectives);
- *Metoda známkovací* neboli bodovací metoda;
- *Metoda párového srovnávání kritérií;*
- *Metoda pořadí;*
- *Metody operační analýzy*, resp. *operačního výzkumu* (Operation Research);
- *Metoda použití případové studie* (tj. technika používaná při vytváření variant v případě nestrukturovaných nebo špatně strukturovaných procesů);
- *Metody pro multikriteriální (vícekriteriální) hodnocení;*
- *Metody pro stanovení vah* variant nebo kritérií (např. kompenzační metody jako metoda kompromisu, swingující metoda, metoda nazývaná odpor ke změnám, MACBETH a holistická metoda);
- *Metody pro zlepšení práce s informacemi a pro strukturování problému* (příklady jsou: makro blokové schéma - vytváří vizuální schéma obecného procesu a používá maximálně šest kroků, kontrolní tabulka, Pareto diagram (pravidlo 80/20), afinitní diagram, kauzální diagram (rybí kost, Ishikawa diagram), analýza silového pole, orientovaný graf vzájemných vztahů, Jak-jak diagram, priorizační matice, mřížka úsilí - znázorňuje jednoduchý kontrolní seznam (a to popisný, škálovací, dotazovací) a rozhodovací matice;

- *Metody síťové analýzy* (příklady jsou: CPM (Critical Path Method); MPM; PERT (Program Evalution and Review Technique); RAMPS (metoda analýzy síťových grafů); GERT, Petriho sítě,.Colour Petri Net, Fuzzy Colour Net atd.);
- *Metoda stromu významnosti* (příklady jsou: PATTERN, QUEST, SEER);
- *Modelování;*
- *Panelová diskuse; PCDA* (Plánuj-Dělej-Kontroluj-Jednej, Plan-Do-Check-Act);
- *Saatyho metoda; SWOT analýza; Systémové metody* (např. aplikace analýzy změn, HAZOP, FMEA, Co - Kdyby, FTA, ETA, analýza spolehlivosti; analýza přežití systému – SSA Survivability systém Analysis - analýza odchylek a identifikace zranitelnosti částí systému z hlediska houževnatosti a obnovy; analýza rizik spojených s lidskou činností - HRA, funkční analýza, a Technique for Human Error Analysis); analýza rizik spojených se zařízením (PSA, Event and Barrier Function, Discrete Event Analysis);
- *Technika aplikace DSS* (systémů na podporu rozhodování);
- *Technika stanovení vah kritérií* (např. se používají metody: alokace 100 bodů; aplikace bodové stupnice, postupný rozvrh vah, Saatyho metoda;
- *Teorie extrémů* (příklady jsou – výpočet ohrožení dle teorie velkých čísel, aplikace Probit funkce;
- *Teorie her* atd. [10].

6.2. Příklady používaných specifických nebo speciálně upravených obecných postupů jsou v práci [8], tj. jsou popsány dále uvedené metody, nástroje a techniky:

- Metody pro analýzu a hodnocení rizik:
  - *tradiční metody jako*: Check List (kontrolní seznam); Safety Audit (bezpečnostní kontrola); What – If Analysis (analýza toho, co se stane když); Preliminary Hazard Analysis (předběžná analýza ohrožení); HAZOP Analysis (Hazard Operation Process Analysis – analýza ohrožení provozního procesu); QRA (Process Quantitative Risk Analysis – kvantitativní analýza rizik procesu); ETA (Event Tree Analysis – analýza stromu událostí); FMEA (Failure Mode and Effect Analysis – analýza poruch a jejich dopadů); FTA (Fault Tree Analysis – analýza stromu poruch; HRA (Human Reliability Analysis - analýza lidské spolehlivosti; FL-VV (Fuzzy Set Method - metoda fuzzy logiky a verbálních výroků; RR (Relative Ranking – relativní klasifikace); CCA (Causes and Consequences Analysis - analýza příčin a důsledků); PSA (Probabilistic Safety Assessment – pravděpodobnostní hodnocení bezpečnosti),
  - *specializované metody jako:* CRAMM, COBRA, MELISA. Pravděpodobně nejznámější je metodika CRAMM (CCTA Risk Analysis and Management Methodology), která byla původně vyvinuta pro potřeby vlády Velké Británie, ale v současné době je široce využívána jako uznávaný prostředek pro analýzu rizik v případech, kdy je vyžadován souhlas s normou ČSN ISO/IEC 13335 a mezinárodním standardem ISO/IEC 17799; *Metodika @RISK* využívá k analýze rizik simulační metody Monte Carlo; *Metodika RiskPAC* slouží k automatizaci dotazníkových přístupů; *RiskWatch* je programový produkt, který poskytuje metodický soubor pro zjištění, simulaci a následnou změnu parametrů jednotlivých rizik systému. Metoda je založena na vytvoření modelu, který je postavený na získaných datech nebo na simulační metodě Monte Carlo.

  Pozn. Na adrese http://www.riskworld.com lze najít více než 1000 specializovaných metod, které jsou podporovány software a byly vyvinuty pro specifické případy, a proto před jejich použitím je třeba ocenit, zda jsou splněny požadavky transferu technologií.
- Soubor provázaných metod pro hodnocení pohrom a řízení rizik, který tvoří:
  - metoda pro stanovení relevantních pohrom v území či objektu,
  - metoda na stanovení největší očekávané velikosti pohromy (má dvě modifikace - metoda, když zdrojem ohrožení je jeden zdroj pohromy; a metoda, když zdrojem ohrožení je více zdrojů pohromy,
  - metoda pro stanovení poklesu velikosti dopadů pohromy se vzdáleností od místa vzniku pohromy,
  - metoda na stanovení anomálií v územním rozložení dopadů,
  - metoda výběru nepřijatelných dopadů v území či objektu,
  - metoda ocenění potenciálních škod na majetku způsobených nepřijatelnými dopady pohrom v území či objektu,
  - metoda pro určení vhodných nápravných opatření pro očekávané pohromy v území či objektu,
  - metoda pro výběr optimálních nápravných opatření pro obnovu území či objektu,
  - metoda implementace nápravných opatření pro zajištění obnovy majetku v území či objektu,
  - metoda pro stanovení databáze nápravných opatření,
  - metoda pro stanovení parametrické závislosti nákladů na obnovu území či objektu vs. velikost pohromy,
  - metoda pro stanovení finanční rezervy na obnovu [6,10].
  - Příklady aplikací jsou: USA – FEMA; Švýcarsko – program PLANAT (veřejná správa), Holandsko, UK atd.
- Metody pro zkoumání interdependences v systémech systémů (SoS). Pro studium SoS, jejich chování a selhání se kromě analytických metod, tradičních metod rizikové analýzy, scénářů, deterministické a pravděpodobnostní analýzy bezpečnosti, bezpečnostní analýzy sítí, analýzy spolehlivosti, expertních odhadů, rozhodovacích matic (risk matrix, criticality matrix), Monte Carlo atd., nejčastěji používají specifické metody pro sestavení modelů, a to: Bayesian Method, Bayesian Network, Mixed Bayesian Network, Fuzzy Bayesian Network Model, Bayesian

Reliability Model, Fuzzy Rule-based Bayesian Reasoning (FuRBaR); Petri Nets (PN), Coloured Petri Nets (CPN), Stochastic Petri Nets (SPN), Coloured Stochastic Petri Nets (CSPN); Case Study (CS); Multi-Attribute Utility Theory (MAUT); Multi-Criteria Analysis (MCA); Weighted Sum Approach (WSA); Concordance, Discordance Analysis (CDA); Technique for Order Preference by Similarity to Ideal Solution (TOPSIS); Ideal Point Analysis (IPA); Aggregation Preferences (AGREPREF), Preference Ranking Organisation Method; for Enrichment Evaluations (PROMETHEE); Markov Chain (MC); Multi-Objective Genetic Algorithm (MOGA); Multiplicative Intuitionist Linear Logic (MILL) atd. [7,8].

6.3. Příklady používaných zvláštních inženýrských postupů

V práci [8] jsou popsány dále uvedené zvláštní inženýrské metody, nástroje a techniky, které nazýváme inženýrské pracovní metody. Zahrnují metody:

- výpočetní, které jsou používané pro: hodnocení pohromy (tj. místo, maximální očekávaná velikost, pravděpodobnost či četnost výskytu, rozložení a velikost dopadů); hodnocení ohrožení (stanovení normativní velikosti pohromy - nejčastěji projektové pohromy = stoleté pohromě); a pro hodnocení rizik (v určitém místě podle velikosti ohrožení a dle množství a zranitelnosti chráněných zájmů). Obecně se musí pro každý specifický objekt či sledované místo určit: velikost největšího očekávaného ohrožení od dané pohromy; soupis jevů, které vyvolá dopad pohromy o velikosti rovné největšímu očekávanému ohrožení, tzv. sekundární dopady a popř. další úrovně dopadů, s ohledem na stavbu podloží daného místa, konstrukci sledovaného objektu, technologii v daném objektu dle nejnovějších poznatků i na množství lidí; hodnocení sekundárních dopadů; velikost sekundárních dopadů a z nich plynoucí škody a ztráty; a zvážit bezpečnostní rezervu,
- průkaz odolnosti, což je technika důkazu, že sledovaná rizika jsou konstrukcí zařízení i konstrukcí staveb a bezpečnostními systémy zvládnuta, tj. je zajištěna požadovaná bezpečnost. Průkaz odolnosti tvoří soubor výpočtů, testů, analogií, úsudků, kterými lze s jistou spolehlivostí stanovit, že sledované zařízení či jeho části jsou odolné až do stanovené (specifikované) úrovně pohromy. U běžných technických zařízení a objektů se prokazuje odolnost na stoleté pohromy. U důležitých mostů, přehrad pro tisícileté pohromy a pro běžná jaderná zařízení na deseti tisícileté pohromy (pozn. úložiště aktivního plutonia vyžadují prokázání odolnosti na sto tisíciletou pohromu) [8].
- průkaz bezpečnosti začíná dříve než průkaz odolnosti zařízení a staveb, protože se začíná od pohrom ve smyslu All Hazard Approach [3], tj. ne od souboru sledovaných rizik, které mohou být neúplné. Tyto průkazy jsou v projektové a provozní dokumentaci a v dokumentech typu Bezpečnostní program, Bezpečnostní zpráva a Bezpečnostní list,
- vyjednávání s riziky je technika, pomocí které rozdělíme zvládání rizika do kategorií: část rizika, u které se realizace rizika odvrátí preventivními opatřeními a činnostmi; část rizika, u které se dopady realizace rizika odvrátí připraveností, tj. zmírňujícími opatřeními a činnostmi, varovnými systémy, výcvikem a vzděláním potenciálních postižených i záchranných složek, náhradními řešeními (např. příprava míst pro přemístění výroby předem); část rizika, která se pojistí (aby byly prostředky na stabilizaci a obnovu chráněných zájmů); část rizika, na kterou se připraví odezva a obnova a jejich znalostní, personální, materiálně technické a finanční zázemí; a část rizika, pro kterou se připraví contingenci plan (nejsou řiditelná, protože nejsou k tomu znalosti a schopnosti), málo častá nebo příliš nákladná.

V procesním řízení platí pravidla: všichni se podílejí na zvládání rizik a zvládání konkrétního rizika se přiděluje tomu subjektu, který je na to nejlépe připravený. Uvedená pravidla jsou základní součástí bezpečnostního inženýrství.
Příklad nástroje pro strategické řízení bezpečnosti území (zpracovaného jako DSS) je uveden v práci [11]. Aplikace SWOT analýzy a metodiky případových studií je v práci [15].

7. Závěr

Abychom dosáhli cílů a splnili lidská přání, musíme kvalifikovaně řídit rizika, tj. rizika musíme: chápat v souladu s přístupem All Hazard Approach; správně identifikovat, analyzovat a vyhodnotit, tj. použít správné METODY a relevantní data; vypořádat, tj. opatření na snížení a zmírnění rizik provést v detailech i souvislostech, aby nedošlo ke vzniku nového nebo k růstu rizika jinde v lidském systému; neustále systém a jeho procesy sledovat a korigovat s ohledem na nové znalosti a zkušenosti. Ve všech činnostech je nutné přemýšlet v detailech i v souvislostech (lidský intelekt je studnicí tacitních znalostí), používat kvalifikovaná data, kvalifikované metody, metody kvalifikovaně aplikovat a používat zkušenosti (zásady dobré praxe jsou velmi užitečné).

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] PROCHÁZKOVÁ, D., 2007: Bezpečnost lidského systému. ISBN 978-80-86634-97-5. Ostrava: SPBI, 139p.
[2] PROCHÁZKOVÁ, D., 2011: Strategické řízení bezpečnosti území a organizace. ISBN: 978-80-01-04844-3. Praha: ČVUT, 483p.
[3] FEMA,1996: Guide for All-Hazard Emergency Operations Planning. State and Local Guide (SLG) 101. Washinton: FEMA.
[4] ROLAND, H.E., MORIARITY, B., 1990: System Safety Engineering and Management. ISBN 0-471-6186-0. London: J. Willey, 321p.
[5] ANDERSON, R., 2008: Security Engineering- A Guide to Building Dependable Distributed Systems. ISBN 978-

0-470-068552-6. London: J. Willey, 1001p.
[6] PROCHÁZKOVÁ, D., 2011: Analýza a řízení rizik. ISBN: 978-80-01-04841-2 Praha: ČVUT, 405p.
[7] ESRA, 2009: Reliability, Risk and Safety: Theory and Applications. ISBN 978-0-415-55509. Leiden: CRC Press / Balkema, 2367 p.
[8] PROCHÁZKOVÁ, D., 2011: Metody, nástroje a techniky pro rizikové inženýrství. ISBN: 978-80-01-04842-9. Praha: ČVUT, 369 p.
[9] ISO, 2008: Draft International Standard ISO/DIS 31000, Risk management – Principles and guidelines on implementation, 18 p.
[10] PROCHÁZKOVÁ, D., 2007: Metodika pro odhad nákladů na obnovu majetku v územích postižených živelní nebo jinou pohromou. ISBN 978-80-86634-98-2. Ostrava: SPBI SPEKTRUM XI Ostrava, 251p.
[11] PROCHÁZKOVÁ, D., 2010: Metodika pro výběr optimálního modelu strategického řízení bezpečnosti území. In: Požární ochrana 2010. ISBN: 978-80-7385-087-6, ISSN: 1803-1803, Ostrava: SPBi, pp 260-265.
[12] KAUFMANN, A., GUPTA, M. M., 1988: Fuzzy Mathematical Models in Engineering and Management Science. Amsterdam: North Holland, 338p.
[13] IAEA,1954-2015: Safety Guides. Vienna: IAEA.
[14] CHISA, 2002: Prevention/Process Safety/Risk Assessment Metodology. Pratur: CHISA.
[15] PROCHÁZKOVÁ, D., 2010: Aplikace SWOT analýzy a vybraných typů případových studií při výběru modelu pro strategické řízení bezpečnosti území. In: ENVIRO, STRIX n.f. Žilina 2010, ISBN 978-80-89281-56-5, pp 348-384.

ADRESA AUTORA:

Dana Procházková, doc., RNDr., PhD., DrSc., ČVUT v Praze, fakulta dopravní, Konviktská 20, 110 00 Praha 1, Česká republika, e-mail: prochazkova@fd.cvut.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.