Motivation - Education - Trust - Environment - Safety 2018
METES
Recenzovaný zborník z III. medzinárodnej vedeckej konferencie, 19.IV.2018, Bratislava
Proceedings of the 3rd International Conference, Bratislava, April 19, 2018
Žilina: Strix et SSŽP. Edition ESE-42, ISBN 978-80-89753-29-1

INŽENÝRSTVÍ RIZIKA

Dana PROCHÁZKOVÁ

RISK ENGINEERING

METES
Motivation - Education - Trust - Environment - Safety 2018

ABSTRAKT
PRÁCE VYCHÁZÍ Z VÝSLEDKŮ, KTERÉ BYLY ZÍSKÁNY KRITICKÝM HODNOCENÍM SOUČASNÉHO POZNÁNÍ A ZKUŠENOSTÍ. PRO ZAJIŠTĚNÍ BEZPEČNOSTI TECHNICKÝCH DĚL I ÚZEMÍ SE POUŽÍVÁTŘÍSTUPŇOVÉ ŘÍZENÍ, JEHOŽ STUPNĚ MAJÍ STEJNÝ CÍL, AVŠAK S OHLEDEM NA PODMÍNKY, ZA KTERÝCH JSOU APLIKOVÁNY, VYUŽÍVAJÍ RŮZNÉ NÁSTROJE, ZDROJE, SÍLY A PROSTŘEDKY. PRÁCE UVÁDÍ VÝSLEDKY SPECIFICKÉHO VÝZKUMU, KTERÉ UKAZUJÍ, CO JE TŘEBA PŘI PRÁCI S RIZIKY RESPEKTOVAT, ABY TECHNICKÁ DÍLA BYLA BEZPEČNÁ.

KLÍČOVÁ SLOVA:*riziko, bezpečnost, bezpečí, inženýrství zacílené na rizika, řízení rizik, vypořádání rizik*

ABSTRACT
THE PAPER GOES FROM THE RESULTS THAT WERE OBTAINED BY CRITICAL JUDGEMENT OF PRESENT COGNITION AND EXPERIENCES. FOR ENSURING THE SAFETY OF BOTH, THE TECHNICAL FACILITIES AND THE TERRITORY, IT IS USED THREE DEGREED MANAGEMENTS, THE DEGREES OF WHICH HAVE THE SAME GOAL, HOWEVER, WITH REGARD TO CONDITIONS UNDER WHICH THEY ARE APPLIED, THEY USE DIFFERENT TOOLS, SOURCES, FORCES AND MEANS. THE PAPER GIVES THE RESULTS OF SPECIFIC RESEARCH THAT SHOW, WHAT IT IS NECESSARY TO ADHERE SO TECHNICAL FACILITIES MIGHT BE SAFE.

KEYWORDS: *risk, safety, security, risk engineering, risk management, trade-off with risks*

1. Úvod do problematiky rizik a bezpečnosti

Je skutečností, že všechna lidská společenství i všechna lidská sídla jsou čas od času postihována škodlivými jevy (pohromami). Rizika s nimi spojená jsou proměnná v čase i prostoru a závisí jak na proměnnosti pohrom, ke které dochází v důsledku dynamického vývoje světa, tak na zranitelnosti lidí a veřejných aktiv, která lidé potřebují k životu, a v neposlední řadě také na možnostech lidí při budování ochranných systémů. Proto vznikla disciplína inženýrství sledující rizika (risk engineering), jejímž cílem je řídit rizika tak, aby lidská sídla na všech úrovních byla bezpečnými systémy[1-4]. V důsledku dynamického vývoje světa jde pochopitelně o dynamickou disciplínu, která zohledňuje jak fakt, že pohrom je velké množství a v důsledku rozmanitosti jejich podstaty jejich dopady nejsou stejné, tak fakt, že území a lidská společenství, která je obývají, se odlišují vlastnostmi a proměnnými možnostmi, což se projevuje různou zranitelností aktiv a různými možnostmi lidí v čase a prostoru. Proto veličina riziko je místně a časově specifická, a při řízení a ovládání rizika je třeba předmětnou skutečnost zvažovat.

Od starověku v celé historii lidstva na různých místech světa jsou zřetelným příkladem rozvoje inženýrství (techniky) vojenské systémy, a to jak dobyvačné, tak ochranné. Jejich nedostatky a selhání ukazují mnohé historické události. Sledování historie z pohledu vývoje nástrojů zajišťujících bezpečí a rozvoj lidských komunit ukazuje, že každé lidské společenství v době minulé pečovalo na své úrovni znalostí a zkušeností o svá sídla a jejich materiální, technické, ekonomické a sociální zázemí, tj. provádělo jistá opatření a činnosti pro své bezpečí, tj. cíleně pracovalo na bezpečnosti. K zásadnímu rozdílu v pojetí došlo v polovině 90. let minulého století [5], kdy se přešlo od konceptu „bezpečný stát zajišťuje bezpečí pro lidi“ ke konceptu „bezpeční lidé zajišťují bezpečný stát“, tj. prioritou při volbě opatření a činností se stalo bezpečí lidí.

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 a přírodních zdrojů i kritické objekty a kritické infrastruktury, které představují složité kyber-socio-technologické systémy [6]. Technická díla jsou výsledkem lidského intelektu a jejich aplikace v praxi umožňuje lidem rozvoj a přežití nástrah přírody. Využití v praxi je spojeno s jejich rozšířením v území, což se mnohdy děje pomocí infrastruktur. Předmětem práce je jak území, tak technická díla, která jsou přínosná pro lidstvo, tj. nejsou řešena díla, kterými dochází ke zneužití technologií. Technická díla objektová i síťová byly, jsou a budou veřejným aktivem, protože zajišťují dennodenní potřeby občanů, tj. energii, vodu, jídlo, informace apod. a závisí na nich přežití lidí při kritických situacích. Představují otevřené systémy vzájemně propojených systémů, které popisujeme modelem systém systémů - zkratka SoS [7]. Jsou v dynamicky proměnném světě, který je ovlivňován jak procesy, které probíhají nezávisle na člověku, tak procesy, které člověk vytváří vědomě či nevědomě svou činností a chováním.

U procesů, které se odehrávají nezávisle na vůli a chování člověka, má člověk pouze možnost zmírňovat nepřijatelné dopady na sebe a aktiva, na kterých je závislá jeho existence a kvalita života. Šanci má však jen tehdy, když předmětné procesy důkladně pozná a najde opatření a činnosti, kterými zmírní dopady procesů, které poškozují jeho nebo aktiva, na nichž je závislý. U procesů, které člověk vyvolává svým chováním a činnostmi, má člověk šance vyšší, protože může cíleným chováním a cílenými činnostmi vytvářet jen procesy, které zlepší kvalitu jeho života a zároveň významně nenaruší prostředí, na němž je existenčně závislý, má možnost snižovat nebezpečnost objektů, infrastruktur i procesů. Šanci však má opět jen tehdy, když bude mít znalosti a když znalosti a zkušenosti správně a cíleně využije.

Cílem odborníků, kteří respektují veřejný zájem, je zavádět do praxe jen bezpečná technická díla, která jsou zabezpečená vůči všem vnějším i vnitřním pohromám, a to včetně lidského faktoru i pohromám, které jsou spojené s vnitřními vazbami a toky, a s propojeními technického díla s okolím, a zároveň neohrožují ani sebe, ani své okolí, tj. jsou bezpečná. Jelikož svět i technická díla se v čase mění, je důležité stále pečovat o jejich koexistenci.

Práce je věnována základům řízení bezpečnosti technických děl zacílené na bezpečné území a bezpečnou lidskou společnost. Přitom vychází z výsledků, které byly získány kritickým hodnocením současného poznání a zkušeností. Pro zvládnutí bezpečnosti technických děl si vyspělé státy cíleně vytvořily třístupňové řízení (řízení zacílené na rozvoj, nouzové a krizové), jehož stupně mají stejný cíl, avšak s ohledem na podmínky, za kterých jsou aplikovány, využívají různé nástroje, zdroje, síly a prostředky [8].

Základem pro řízení bezpečnosti technických děl i jejich okolí je především analýza a ocenění rizik spojených se vzájemnými propojeními; tj. při identifikaci rizik je třeba použít i průřezová kritéria. Posuzování kritičnosti jednotlivých systémů i jejich souborů není triviální záležitostí, protože v různých situacích jednotlivé systémy i celek mají různou roli aktivní, reaktivní, kritickou nebo tlumící (ne však aditivní). Např. existence více variant dodání elektřiny do určitého místa snižuje kritičnost energetické infrastruktury, ale zvyšuje náklady apod.

Protože připuštění existence rizik a zavedení práce s riziky s cílem zajistit bezpečí a rozvoj člověka do praxe znamená nový pohled na problémy reality a na způsob jejich řešení, je třeba postupovat způsobem, který do vědecké praxe zavedl francouzský vědec Descartes, což znamená dle konceptu založeného na práci s riziky, že se problémy reality musí nově strukturovat a dílčí problémy spolehlivě řešit (dnes jde o realitu, kterou představují vzájemně propojené systémy různé podstaty). Práce tudíž respektuje koncept OSN „Resilient Nation“ [9], tj. koncept, který je založen na předpokladu, že výskyt

pohrom, zranitelnost lidí a dalších veřejných aktiv a velikost dopadů pohrom na aktiva lidského systému se nebude v čase snižovat, ale spíše zvyšovat, a proto pro zajištění bezpečí a rozvoje lidí je důležitá funkcionalita vysoce spolehlivé veřejné správy, bezpečná technická díla a bezpečné infrastruktury. Jelikož legislativy vyspělých zemí vymezují pojem kritická infrastruktura a do něho zahrnují jen některé infrastruktury, např. [10], je třeba uvést, že životně důležité pro lidi jsou i zelené infrastruktury, infrastruktura výchovy a vzdělávání lidí a také infrastruktura výzkumu. Důležitost předmětného konceptu se v materiálech OSN dokumentuje také na potravinové bezpečnosti. V předmětné souvislosti se uvádí zlaté pravidlo pro schopnost přežití národa *„čím více potravin a průmyslových výrobků si národ umí vyprodukovat sám, tím méně je v krizích zranitelný“*.
Dále uvedené výsledky vychází ze systémového pojetí entity, která se nachází v dynamicky proměnném světě. Aplikace systémového pojetí vytváří nástroj, který pomáhá rozvíjet společný jazyk, který umožňuje specialistům z různých oborů a technologií vzájemně komunikovat. Jeho metodologie je založena na dvou klíčových principech:

1. Realita je chápána jako celek a celek je víc než suma prvků (sledují se prvky, vazby mezi prvky a spřažení mezi prvky spojená s toky mezi prvky).
2. Systém je definován jako soubor propojených entit. 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 pomocí souboru kritérií, která musí entita splnit, aby patřila do systému.

Základem řízení bezpečnosti světa i technických děl je model, který umožňuje identifikaci, analýzu a ocenění rizik všeho druhu, tj. i průřezových, která jsou spojená se vzájemnými propojeními v celku i v jeho okolí. Cíl práce s riziky je zajistit bezpečná území, kde žijí lidé, a proto je nutné, aby byla zajištěna koexistence technických děl s územím po celou dobu životnosti technických děl.
Práce se opírá o současné poznání. Navazuje na dřívější publikace autorky, jejichž seznam je v práci [11], které byly zpracovány na základě kritického vyhodnocení poznatků v dostupných stovkách odborných prací a zkušeností autorky z praxe. Předmětné poznatky jsou dále doplněny znalostmi získanými kritickou analýzou odborných prací, které se zabývají riziky v předních odborných časopisech a knihách. Jde především o práce, které jsou cíleně shromažďované evropskou agenturou ESRA (European Safety and Reliability Association), prezentované na světových konferencích ESREL od r. 1990 a následně publikované ve formě tištěných a elektronických knih, jejichž seznam je v práci [11], a také na specifických odborných konferencích, z nichž některé byly pořádány nebo spolupořádány VUT i ČVUT a jejich výsledky jsou v recenzovaných sbornících.

2. Souhrn použitých znalostí a zkušeností

Odborné práce i nákladné projekty EU z posledních let jako např. CASCADE, CIPRnet, EDEN [12] ukazují, že:

- pro zajištění bezpečného otevřeného systému, tj. i celku skládajícího se z území s technickými díly a příslušného lidského společenství, je nutné dané území a jeho obyvatele řádně poznat tím, že se analyzují a vyhodnotí historické pohromy v souvislostech, přičemž se zváží jak zranitelnosti aktiv, tak lidské schopnosti a možnosti v dané době,
- každá země EU si musí vytvořit systém ochrany aktiv, včetně technických děl takový, který navazuje na její historicky zavedené systémy ochrany, protože z pochopitelných důvodů není možné navrhnout a zavést jeden univerzální systém ochrany technických děl pro všechny země EU (každá unifikace vyžaduje čas, finance, nástroje pro změny a přizpůsobení lidí, a nemusí být přijatelná z hlediska národních tradic a kultur).

Vzhledem k uvedeným skutečnostem je třeba, aby každá země budovala systém řízení bezpečností, který zajišťuje jak ochranu lidí a životního prostředí, tak ochranu technických děl, základních infrastruktur a dodavatelských řetězců. Daný cíl lze efektivně dosáhnout jen kvalifikovaným přístupem a kvalitním řízením aktivit, zdrojů, sil a prostředků, což zajistí pouze dobré vzdělání.
Syntéza současného poznání zvažující dynamický vývoj světa [6] ukazuje, že neexistují uzavřené neměnné technologické ani jiné systémy v neměnném okolí. Při úvahách o bezpečnosti je třeba zvažovat nejen proměny prostředí a materiálů v čase, ale i skutečnost, že všechny technické, sociální i organizační systémy se mění v čase výskytem pohrom majících velikosti větší než projektové [4]. Při

výskytu nadprojektových pohrom vznikají kritické podmínky, na které nejsou technická díla konstruována a dochází k závažným selháním funkcí technických děl, která působí závažné ztráty lidem, ekonomice, životnímu prostředí i technickým dílům samotným.
Provedené analýzy dopadů pohrom, a to hlavně havárií a selhání [4] ukazují, že pro bezpečí a rozvoj lidí, je třeba s kritickými podmínkami počítat. Z důvodu omezených možností lidí, lidé jsou schopni technologické objekty vybudovat jako bezpečné systémy jen pro jistý interval podmínek, a pro případ jiných podmínek pak musí vytvářet nástroje, kterými sníží ztráty, újmy a škody na všech veřejných aktivech (tj. i na technických dílech a infrastrukturách, které poskytují výrobky nebo služby, a to ať jsou veřejné nebo soukromé).

2.1. Základní pojmy

Protože v České republice dosud nedošlo ke sjednocení pojmů v oblastech spojených s bezpečností a k jejich navázání na pojmy, které používají odborné asociace, OSN, OECD, EU, IAEA, WB, tak uvedeme základní z nich. Předmětná terminologie vychází z konceptu:

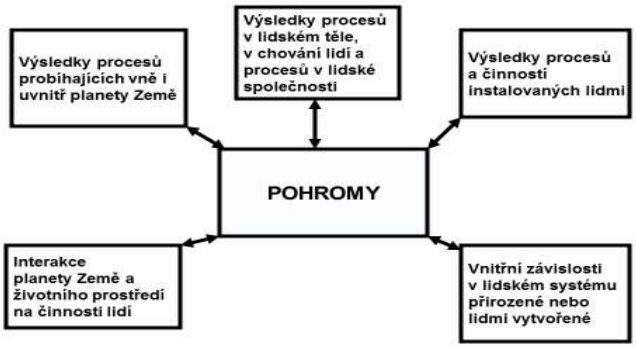
- v území, objektech i komunitách probíhají procesy, jejichž výsledky jsou jevy, přičemž některé jevy mají dopady, které nejsou příznivé pro člověka a aktiva, na nichž je člověk závislý, a proto předmětné jevy od r. 1811 v našich zemích nazýváme pohromy (což odpovídá anglickému ekvivalentu „disaster“),
- dopady pohrom na člověka a aktiva, na nichž je závislý, jsou tím větší, čím je člověk a aktiva zranitelnější a méně odolné,
- antropogenní ochranná opatření spočívají ve snižování zranitelnosti lidí a aktiv, na nichž jsou lidé závislí, a také ve zvyšování odolnosti lidí a aktiv, na nichž jsou lidé závislí,
- strategické, proaktivní a systémové řízení a provedení antropogenních opatření je prováděno inženýrstvím zacíleném na rizika (risk engineering).

V oblasti spojené s riziky existují tři pojmy, které jsou jistým způsobem propojeny, a mají zcela vymezený a vysoce rozdílný význam. Jde o pojmy: nebezpečí, ohrožení a riziko.
Nebezpečí (angl. Danger) označuje stav lidského systému, při kterém vznik újmy, škody či ztráty na chráněných aktivech (zájmech) má vysokou pravděpodobnost; tj. je téměř jisté, že újma, škoda nebo ztráta vznikne [7]. Jde o označení možnosti vzniku újmy, ztráty či škody na jednom aktivu či více aktivech. Nebezpečí je určeno vlastnostmi látek, které se nachází v zařízení, objektu či území, anebo vlastnostmi procesů, které probíhají v zařízení, objektu či území. Je bezprostřední, když vývoj nezadržitelně směřuje k pohromě, a tím k vyvolání nouzové situace; a je plíživé, když vývoj směřuje k pohromě nenápadně a bez zřejmých příznaků [7]. Nebezpečí pro člověka znamenají jak velké jevy (např. živelní pohromy, průmyslové havárie, ekologické či sociální pohromy), tak zdánlivě malé jevy z denního života (pád tašky ze střechy, pád rampouchu nebo sněhu ze střechy, nerovný chodník apod.). Nebezpečí je tudíž míra současného stavu.
Ohrožení (angl. Hazard) vyjadřuje potenciál pohromy působit újmy, ztráty a škody na chráněných aktivech v daném místě, který je určený normativně. Jde o normativní míru nebezpečí, která je spojená s danou pohromou. Pro potřeby strategického plánování se nejčastěji počítá se stoletou pohromou, tj. ohrožení je velikost pohromy, která se vyskytne jedenkrát za sto let nebo přesněji má periodu návratu 100 let; u speciálních technických děl (přehrady, jaderné elektrárny, průmyslové komplexy s nebezpečnými technologiemi, mosty, tunely apod.) se pak z důvodu bezpečnosti zvažuje ohrožení jako velikost tisícileté či deseti tisícileté pohromy [7,8].
Riziko (angl. Risk) spojené s danou pohromou, činností či procesem je pravděpodobná velikost škod, ztrát a újmy na chráněných aktivech, které v daném místě vzniknou při výskytu pohromy mající velikost normativně stanoveného ohrožení, která je normovaná na stanovenou jednotku území či jednotku počtu jedinců a jednotku času [7]. Rozdíl mezi nebezpečím a rizikem spočívá v tom, že nebezpečí je určité (označuje aktuální stav) a riziko je jen očekávaná možnost.
Dominantním zájmem naší doby je riziko – jde nám o odvrácení ztrát a škod na chráněných aktivech, a to nejen okamžitých, ale i těch očekávaných v bližší nebo vzdálenější budoucnosti; a proto se často mluví o analýze rizik, řízení rizik, zvládání rizik, vnímání rizik atd. V předmětné oblasti panuje mezi sektory lidských činností dosud velká nejednotnost, která brání objektivnímu porovnávání míry rizika

v prostoru i čase. Jedním z problémů je skutečnost, že v některých případech se zvažuje jen jeden chráněný zájem (jedno aktivum), tj. určuje se dílčí riziko, a v jiných případech se zvažuje více chráněných zájmů (aktiv) a určuje se integrované riziko (součet nebo jiná agregace dílčích rizik) či integrální riziko (vycházející ze systémové podstaty entity, tj. rizika jsou spojená s prvky, vazbami a toky v systému). Podrobné údaje o problematice jsou shrnuty v práci [11].
Bezpečnost představuje soubor antropogenních opatření a činností, kterými lidé brání sebe nebo aktiva, na kterých jim záleží proti škodlivým jevům všeho druhu. Bezpečnost a riziko jsou v určitém vztahu, ale nejsou komplementárními veličinami, např. aplikací varovacích systémů zvýšíme bezpečnost, ale riziko nesnížíme. Antonymem bezpečnosti je kritičnost.

2.2. Zdroje rizik

Na základě současného poznání jsou pohromy výsledky pěti procesů, které probíhají v lidském systému, obrázek 1 [7,8]. Podrobné jednotným způsobem provedené studium pohrom v ČR i v Evropě v rámci projektu FOCUS [13] ukázalo jejich rozložení a vlastnosti a také odhalilo nedostatky v jejich řízení. Hlavní nedostatky v současném řízení pohrom jsou:



Obr. 1 *Procesy, jejichž výsledkem jsou pohromy v lidském systému*

- přístup All-Hazard-Approach [14] není systematicky aplikován, tj. při zjišťování bezpečí lidí, území i objektu nejsou zvažovány všechny pohromy možné v dané entitě,
- pohromy způsobené člověkem jsou řešeny odděleně od přírodních, technických a dalších, a tím vznikají problémy mezi bezpečností (safety) a zabezpečením (security) entity. Jejich špatné logické pochopení se pak projevuje i ztrátami lidských životů [4],
- dopady a velikost některých pohrom (hlavně v sociální oblasti) jsou podceňovány, což vede ke snížení obranyschopnosti entit,
- systémové, strategické a proaktivní řízení není v řadě případů entit (a to včetně technických děl) implementováno do praxe,
- není sledována koexistence základních životodárných systémů, které mají různou podstatu,
- existují závažné mezery v řízení rizik, inženýrství rizika a ve vyjednávání s riziky (např. neberou se v úvahu všechna důležitá aktiva, proměnnost zranitelností aktiv v čase a prostoru),
- strategie nejsou založeny na dlouhodobých prioritách respektujících veřejný zájem, jejich cíle jsou ovlivňovány politiky nebo lobby,
- postupy aplikace a orientace strategií nejsou pravidelně ověřovány na základě kvalitního monitoringu, což zamezuje přizpůsobení prováděných opatření a činností změnám entit,
- chybí rozumná strategie pro řízení pohrom, tj. pravidla optimalizace opatření s ohledem na konkrétní podmínky a možnosti entity, jelikož např. kvalitní opatření vůči jedné pohromě jsou kontraproduktivní vůči jiné pohromě, která je také možná v entitě [15],
- řízení pohrom často nerespektuje cyklus výskytu pohrom (velké pohromy se vyskytují zřídka a nepravidelně, proto rozhodování a řízení se musí opírat o dostatečně dlouhé časové řady – teorie o černých labutích nebo královských dracích sice utěšují tvůrce strategií, ale nepředstavují racionální řešení problémů),

- chybí důraz na řešení problémů entit spojených s konkrétními riziky, je jen mnoho diskusí o problémech,
- nedostatek zdrojů pro implementaci lidských potřeb,
- nedostatek nástrojů pro zajištění finanční stability EU, která by umožnila vysokou úroveň prevence závažných pohrom,
- nedostatek nástrojů řízení, které podporují ochranu obyvatelstva a udržitelný rozvoj.

Faktem je, že se stále objevují nové zdroje pohrom (jde hlavně o projevy možných propojení mezi systémy v reálném světě), a tím roste počet pohrom. Některé z pohrom mohou lidé zvládnout pomocí preventivních opatření, pro jiné je třeba mít připravena opatření odezvy, zmírňující opatření a standardní zdroje s tím, že pro velké pohromy je třeba mít připraveny nadstandardní zdroje, síly a prostředky [7,8].

Na základě současného poznání je třeba věnovat specifickou pozornost rizikům, spojeným s chováním člověka, a to především při řízení a rozhodování [8]. Tzv. organizační havárie jsou dle současného poznání způsobeny jednou nebo několika dále uvedených příčin: řídící pracovník přecenění vlastní rozhodnutí; neznalost a nezkušenost řídícího pracovníka; neschopnost řídícího pracovníka zajistit včasné a správné předání zásadních informací; malé oprávnění řídícího pracovníka při řešení problémů; řídící pracovník podcenění závažnost situace; řídící pracovník při rozhodování nerespektuje zákonitosti přírodní, technické, ekonomické či sociální. Proto je důležité neustálé vytváření kultury bezpečnosti [4,6,11].

2.3. Rizika, jejich řízení a vypořádání

Riziko je nyní dominantním konceptem v naší společnosti. Je spojeno se složitými podmínkami nebo faktory jako jsou: nejistá přírodní ohrožení; nejistoty, které zahrnují věda a technologie a jejich působení na zdraví a kvalitu života; zranitelnost lidí a nedostatek konzistentního vysvětlení životních strastí a jejich významu; a také lidské hry se strachem, šancemi a možnostmi.

Přijatelná úroveň rizika je subjektivní. U známých a častých pohrom je lidmi vnímaná úroveň rizika blízká skutečné míře rizika. U málo častých a málo známých pohrom je lidmi vnímaná úroveň rizika jako neskutečná a vzdálená. Vnímání rizika ovlivňují i jiné faktory – např. u činností, které děláme dobrovolně (horolezectví, skoky na lyžích apod.), předpokládáme, že úroveň rizika je zanedbatelná. Přijatelnost rizika ve skutečnosti je výsledkem porovnávání několika typů přijatelnosti – technická přijatelnost (spolehlivost a složitost technologií, strojů a zařízení), ekonomická přijatelnost (náklady) a socio-politická přijatelnost (vnímání rizik).

Obecně lze tvrdit, že přijatelné riziko se stanovuje na sociálním a znalostním základě a přitom se zvažují sociální, ekonomické a politické faktory. To mimo jiné znamená, že úroveň přijatelného rizika pro bohaté země či entity je vyšší než pro chudé, protože redukce rizika něco stojí. Proto také platí, že přijatelná úroveň neznamená bezpečnou úroveň rizika, tj. že pravděpodobnost vzniku ztrát, škod a újmy na chráněných aktivech je malá až zanedbatelná.

Riziko je místně specifické a určuje se z velikostí místních ohrožení, která vytváří možné pohromy v daném místě s ohledem na míry zranitelnosti místa vůči konkrétním možným pohromám. Z uvedených skutečností vyplývá, že pro kvalifikované řízení území či jiného subjektu je důležité znát riziko, a to v pochopitelném vyjádření. V praxi veřejné správy se osvědčilo vyjádření rizika ve formě údaje, že na základě analýzy a hodnocení rizik v území bylo zjištěno, že na specifikovaném úseku:

- je třeba 5 miliónů každý rok na nápravu škod, způsobených existujícím rizikem,
- každých 10 let zemře 10 lidí v důsledku sledované pohromy,
- každých 5 let škody na majetku způsobené pohromou přesáhnou 5 miliard.

Z právě uvedeného vyplývá, že abychom určili riziko, musíme pochopitelně nejdříve znát velikost ohrožení pro každou pohromu, která je důležitá pro bezpečné území a bezpečnou lidskou společnost a pak zranitelnosti území vůči každé vybrané pohromě, která je předmětem našeho zájmu. Proto postupy pro stanovení velikosti rizik respektují jak podstatu jevů, které jsou jejich zdrojem (tj. charakteristiky a fyzikální podstaty pohrom), tak parametry prostředí, ve kterém se jevy vyskytují. Pro určení ohrožení se používají jak metody založené na matematické statistice, mlhavých množinách, přístupech operační analýzy apod., které inherentně předpokládají určitý model výskytu jevů, tj. nepřipouštějí, že tyto jevy

jsou mimořádné, tak i metody založené na scénářích dopadů pohrom simulovaných nebo empirických, viz údaje shrnuté např. v pracích [6-8,11,15,16].

Při úvahách v praxi zvažujeme buď jednoduchý případ, a to průběh realizace rizika probíhá stále stejným způsobem, anebo složitější případ, který zvažuje dynamiku vývoje, dle které průběh realizace rizika je proměnný, a to jak v závislosti na změnách parametrů pohrom, tak i v závislosti na momentálních místních a časových podmínkách chráněných aktiv. V prvním případě určujeme jakousi střední hodnotu a její oprávněnost pro použití v praxi spojujeme s podmínkou, že je zvážen nejméně příznivý případ (nacházíme ho v normách a standardech založených na deterministickém přístupu). Druhý přístup odpovídá více 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). První případ používáme v souvislosti s výstavbou složitých technických děl při jejich projektování, druhý pak při inspekcích [4,6,11]. Cílem řízení a vypořádání rizik v každém případě je zajistit, aby nebezpečí spojená s realizací rizika byla přijatelná.

2.3.1. Druhy rizik

Historie odhadu rizika je velmi dlouhá a srovnatelná s historií bankovnictví a pojišťovnictví. Např. bez znalosti rizika nelze pojišťovat, nelze poskytovat úvěry, bankovní záruky a jiné finanční služby. Pro posuzování rizik byl vyvinut bezpočet pomocných pracovních pomůcek, metodických návodů, uživatelských příruček a software. Jejich struktura je značně vertikálně a horizontálně diferencována a vyčerpávající klasifikace je obtížná.

Na základě současných znalostí jsou rizika pro potřeby řízení bezpečnosti území, objektu či lidské komunity [7,11] stanovena správně a mají zřejmou vypovídací hodnotu, jestliže jsou stanovena:

- s ohledem na všechna definovaná chráněná aktiva (zájmy),
- definovaným postupem,
- na základě kvalifikovaného datového souboru se stanovenou vypovídací hodnotou a hranicí homogenity,
- na základě kvalifikovaného zpracování kvalifikovaného souboru dat pro dané zadání.
- Rizika se liší podle toho:
- jaká jsou zvolena chráněná aktiva, zda je sledován jeden chráněný zájem (a pak jde o dílčí riziko), anebo soubor chráněných zájmů (a pak jde o integrované nebo integrální / komplexní riziko),
- jaké pohromy, tj. zdroje rizik se berou v úvahu. Pro některé úlohy postačuje omezený počet pohrom, např. jen těch, které mohou mít nepřijatelné dopady ve sledovaném prostoru třeba dvakrát za sto let apod.

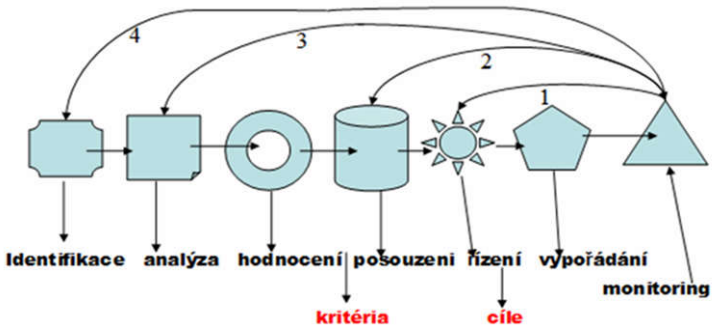
Dílčí rizika jsou rozmanitá, např. zdravotní rizika, technologická rizika, riziko požáru atd. Pro výpočet dílčích rizik již existuje řada právních předpisů, norem a standardů a s nimi souvisejících podpůrných software. Např. dílčí rizika, která se musí zohlednit, při žádosti o projekty EU, anebo pro zajištění úspěšnosti projektů PPP (Public Private Partnership), se dělí do sedmi skupin [7,11]:

1. Bezpečnostní rizika spojená s chováním a činností lidí.
2. Stavebně-technologická a projekční rizika.
3. Kreditní rizika.
4. Tržní rizika.
5. Vnější rizika spojená s přírodními pohromami.
6. Provozní rizika.
7. Rizika spojená s řízením a rozhodováním.

Každá základní skupina dílčích rizik se dále dělí na další dílčí rizika [7,8]. Výběr z těchto rizik pro konkrétní případ se provádí podle formulace problému a podle stanovených cílů, které jsou v daném případě sledovány, a podle pohrom, které se zvažují jako zdroje rizik.

2.3.2. Koncept práce s riziky

Koncept práce s riziky, tj. procesní model je zobrazen na obrázku 2. Další modely jsou uvedeny v práci [7], popř. v pracích, které jsou v předmětné práci citovány.
Podle úvah současných filosofů, rizika ve společnosti mají svoji objektivní i subjektivní stránku, navíc nestojí mimo kulturní a hodnotové souvislosti (nejsou v tomto směru ani „čistě vědeckým" problémem a zasluhují pozornost i z hlediska občanské participace). I když moderní společnost uplatňuje onu pohodlnou strategii pojištění a odškodnění, nelze na ni plně spoléhat, neboť některá rizika jsou schopna zasáhnout podstatu sociálního systému, což platí pro některá rizika bezpečnostní. Proti „zvědečtění bezpečnostní politiky" nelze nic namítnout, pokud dokážeme být reflexivní, což znamená především odhadovat důsledky jednotlivých aktů a nepodléhat iluzi o možnosti „dokonalého řešení". Spoléhání veřejnosti na experty (a vědecké instituce) může přivodit oslabení schopnosti podílet se aktivně na řešení problémů a dokonat tak odtržení privátního a veřejného (což se pak projeví jako inherentní riziko, na kterém expertíza ztroskotá). Podle odborných koncepcí při vypořádání s riziky mají dle svých možností povinnosti a odpovědnosti všichni zúčastnění (tj. všechny zájmové skupiny).



Obr. 2 *Procesní model práce s riziky. Kritéria = podmínky, které stanovují, kdy je riziko přijatelné, podmíněně přijatelné nebo nepřijatelné. Cíle označují žádoucí stavy. Čísla 1,2,3,4 označují zpětné vazby, které se používají, když monitoring ukáže, že nejsou splněny stanovené požadavky na bezpečnost*

Lidé proto mají mít možnost zúčastnit se rozhodování o vypořádání rizik, projevit své potřeby a názory, a to bez obavy z postihů. Obvykle je snaha o zapojení co největšího počtu lidí (i za cenu zvýšených nákladů na počátku procesu), dosahování konsensu a shody. Je to také respektování odlišných názorů a vyjasňování pozic a záměrů různých skupin i jednotlivců. Jestliže zapojujeme do procesu rozhodování veřejnost tak zapojujeme všechny zúčastněné, podle jiných materiálů tzv. podílníky (stakeholders) nebo také dotčené osoby a skupiny. Podílníkem je ten (jedinec, skupina, organizace), kdo může ovlivnit nebo kdo může být ovlivněn (pozitivně i negativně) výsledkem rozhodnutí, plánu, programu nebo i procesem, který k výsledku vede.
Problém nastává v odborných záležitostech, ve kterých podklady pro rozhodování jsou založené na hodnoceních, která jsou složitá a pro řadu normálních občanů nepochopitelná. Situace v těchto případech je proto často válkou lobbistů různých skupin, které usilují o zakázku. Proto je třeba, aby se postupy hodnocení opíraly o legislativu a aby kritéria výběru konkrétních řešení byla zaměřena na veřejně prospěšné cíle (tj. veřejný zájem), umožňovala transparentnost rozhodování při výběru správného řešení s ohledem na zdroje, síly a prostředky veřejné správy, které má k dispozici.

2.3.3. Řízení rizik

V rozhodování o rizicích se řeší dále uvedená dilemata:

- vztah mezi riziky a přínosy (často větší přínos pro lidi znamená zvýšené škody a ztráty pro ekosystémy),
- časový konflikt mezi současnými a budoucími potřebami lidí,
- sociální konflikt (vztah potřeb jedince a celku).

Je obtížné řešit inverzní problémy pro složitost systémů. Zkušenosti ukazují, že když se stanoví a utřídí nějaké příznaky spojené s riziky, vynoří se příznaky nové. Z toho vyplývá, že praktický přístup k řízení udržitelnosti musí být iterační, interaktivní a adaptivní [7,8]. To znamená, že žádná opatření

řízení a vypořádání rizik nejsou trvalá, ale jen dočasná, a proto lidé, a zvláště vytvářené řídicí systémy lidské společnosti, musí podmínky monitorovat a antropogenní opatření činnosti a opatření přizpůsobovat situaci.

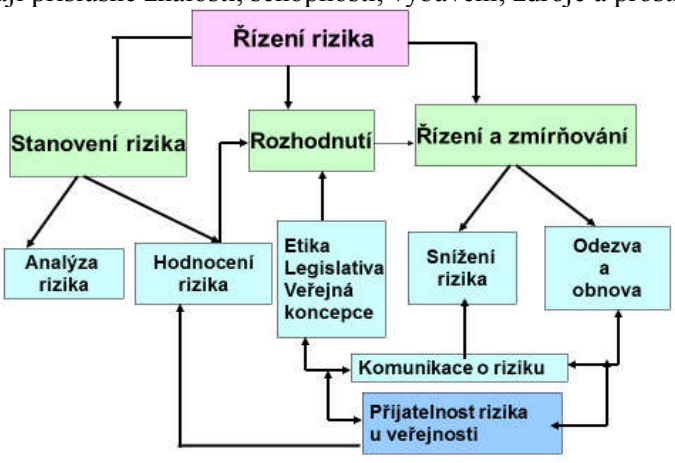
Cílem strategického, tj. komplexního řízení je za každé situace zajistit ochranu životů, zdraví a bezpečí lidí, majetku, životního prostředí, infrastruktur a technologií, které jsou nezbytné pro přežití lidí, tj. vždy mít schopnost zajistit mobilizaci a koordinaci využití zdrojů (energie, pracovní síla, výrobní schopnosti, jídlo a zemědělství, suroviny, telekomunikace aj.), koordinaci činností takových, jako je systém vyrozumění, systém záchrany a zdravotnické služby, které snižují dopady pohrom a také kontinuitu činnosti státní správy a dodržování zákonů.

Pro cíle lidské společnosti, tj. především pro její bezpečí a udržitelný rozvoj je nutno vzájemně kombinovat opatření a činnosti na snižování zranitelnosti, na zvyšování pružné odolnosti (resiliency) a schopnosti adaptace, které respektují všechna základní chráněná aktiva (veřejná i podniková) v jednotlivostech i celku. Současným nástrojem založeným na znalostech a zkušenostech je na všech úrovních řízení implementovat proaktivní systém řízení bezpečnosti, ve kterém se upraví práce s riziky do takové formy, která respektuje všechna chráněná aktiva a bere v úvahu existující a prokázané vnitřní závislosti. S ohledem na současné poznání je třeba provádět a sledovat výzkum vnitřních závislostí, které zprostředkovávají sekundární a další dopady pohrom na životy, zdraví a bezpečí lidí [7,8].

Na základě současného poznání a zkušeností musí být svět chápán systémově a pro zajištění bezpečí a rozvoje lidí musí lidská uskupení, tj. obce, kraje, státy a společenství států dobře pracovat s riziky. Pro práci s riziky je třeba zvažovat: koncept světa v systémovém pojetí; pojmy důležité pro chápání a řízení bezpečnosti; zdroje rizik a chápat jejich dopady na chráněná aktiva; metody pro hodnocení a posuzování rizik; způsoby řízení rizik; způsoby inženýrského vypořádání rizik; a způsoby práce s riziky v čase.

Jak již bylo řečeno, rizik však existuje velké množství, protože jejich zdrojů je velké množství. Navíc rizika stále přibývají a lidská společnost nemá zdroje, síly a prostředky, aby tomu zabránila, tak musí cíleně řídit rizika. Aby řízení bylo úspěšné, tak se musí zaměřit na prioritní rizika a jejich aspekty, jak požaduje typ řízení TQM (Total Quality Management), který je základem norem v Evropě [17]. Řízení rizik entit není záležitosti, ani jednotlivce, ani jednoho sektoru, jak ukazuje obrázek 3. Předmětný obrázek ukazuje základní strukturu řízení rizik, další členění je v práci [7]. Ze základní struktury je zřejmé, že:

- stanovit riziko mohou odborníci, kteří mají znalosti, data a schopnost aplikovat vhodné metody,
- rozhodnout o riziku mohou jen ti, co mají příslušné oprávnění (tj. právně určený subjekt veřejné správy nebo v případě technického díla právně určený subjekt podniku, jemuž entita patří,
- řízení a zmírňování, tj. vlastní aplikace opatření a činností vedoucí ke zvládnutí rizika mohou jen odborníci, kteří mají příslušné znalosti, schopnosti, vybavení, zdroje a prostředky.



Obr. 3 *Základní rámec pro řízení rizik*

Obrázek 3 ukazuje, že veřejnost by měla být platným účastníkem při vypořádání rizik, protože jde o její bezpečí a kvalitu života. Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá v rozdělení opatření a činností na vypořádání rizik do kategorií, ve kterých se příslušná část rizika zajistí tak, že:

- preventivními opatřeními se sníží nebo odvrátí realizace rizika,
- účelovými preventivními opatřeními odezvy a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se zmírní dopady, tj. sníží nebo odvrátí se nepřijatelné dopady při realizaci rizika,
- pojištěním se zajistí zdroje na krytí možných ztrát a škod při realizaci rizika,
- přípravou rezerv a záloh na odezvu a obnovu se zajistí přežití lidí a kontinuita provozu území, objektu či organizace,
- přípravou plánu pro odezvu na nepředvídané situace (Contingency Plan) se zajistí odezva na realizaci rizik neřiditelných nebo příliš nákladných, anebo málo častých.

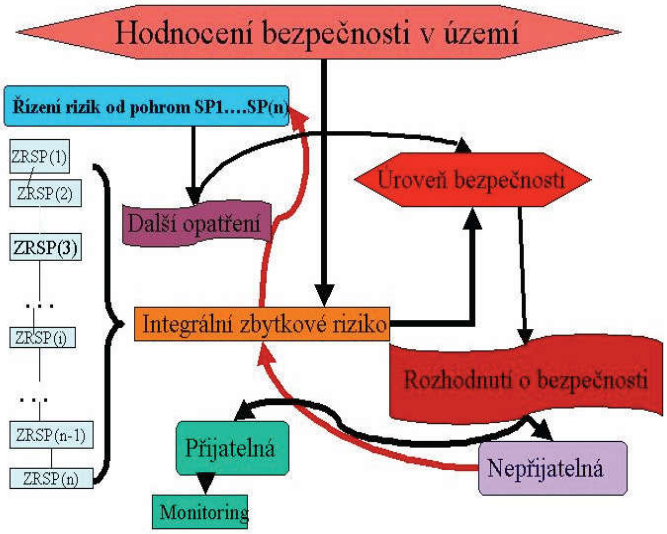
Řízení rizik zacílené na bezpečnost objektu je zobrazeno na obrázku 4 [7]. Přechod od klasického řízení rizik (obrázek 3) na řízení rizik zacílené na bezpečnost (anglicky Risk Governance), znázorněném na obrázku 4 v praxi znamená:

- stanovit synergické vztahy mezi riziky, zranitelností a bezpečím,
- modelovat proces rozhodování správy organizace s ohledem na rizika, nejistoty a neurčitosti (viz podpůrné systémy rozhodování),
- specifikovat rámcové právní podmínky a ochranná opatření,
- zlepšovat činnosti institucí (institucionální změny).

Základním rozdílem mezi řízením rizik (obrázek 3) a řízením bezpečnosti (obrázek 4) je v tom, že v druhém případě se rozhodování provádí na základě míry bezpečnosti, která se stanovuje podle integrovaného rizika, které zvažuje všechny specifické pohromy (tj. pohromy, které mohou způsobit ztráty, škody a újmy na sledovaných aktivech) a bere se v úvahu princip předběžné opatrnosti.

Při práci s riziky je důležité aplikovat výsledky poznání, tj. aby řízení dosáhlo cílů, je nutné:

- používat jen podklady získané na základě kvalifikovaných dat, která splňují požadavky na reprezentativní datové soubory (úplnost, ocenění nejistot, vypořádání s neurčitostmi v datech pomocí specifických matematických přístupů),
- aplikovat správné metody rozhodování, které jsou adekvátní problému.



Obr. 4 *Model řízení bezpečnosti entity*

Dle zásad uvedených v pracích [4,6-8,11] platí, že pro:

- strategické řízení entity, které z pohledu zajištění existence je zacílené na bezpečnost, je třeba používat integrální riziko, a pro jeho zjištění ověřené reprezentativní datové soubory, ověřené metody pro zpracování dat a ověřené metody pro rozhodování, protože na tomto úseku je důležitá

dlouhodobá udržitelnost,

- střednědobé (taktické) řízení možno používat integrované riziko, a pro jeho zjištění méně přesná data, metody zpracování dat i metody rozhodování (je možné použít software) s tím, že při rozhodování se budou respektovat záměry dané strategickým řízením,
- operativní řízení je možno používat dílčí rizika a na základě cíleně získaných znalostí a zkušeností použít naučené a procvičené postupy a nouzové situace zvládnout s tím, že se především soustředíme na životy a zdraví lidí a na další chráněná aktiva v technické entitě a jejím okolí.

Pro klasické řízení rizik i pro řízení rizik ve prospěch bezpečnosti je nutné:

- Rozumět procesu vzniku pohrom a podmínkám, ve kterých proces probíhá.
- Znát, ve kterých místech pohroma může vzniknout a jaké může mít fyzikální a jiné charakteristiky.
- Identifikovat ohrožení, které představuje v daném místě pohroma dle stanovených standardů.
- Stanovit dopady pohrom o velikosti ohrožení na chráněné zájmy.
- Eliminovat nepřijatelné dopady pohrom v případech, ve kterých to jde za přijatelných nákladů.
- U zbylých dopadů vypočítat pomocí prognostických modelů pravděpodobnost jejich realizace s tím, že se vezmou v úvahu i možná selhání preventivních opatření.
- Vypočítat možné škody na chráněné zájmy v konkrétním území podle chráněných zájmů, které jsou skutečně v území a na základě pravděpodobností určit výši rizika.
- Identifikovat a realizovat zmírňující opatření s ohledem na lidi, majetek a životní prostředí tak, aby byla ALARP (tak malá, jak je rozumně možné dosáhnout).
- Prokázat, že byla provedena všechna opatření k zabránění a zmírnění dopadů pohrom.

Přijatelné riziko pro technické dílo i jeho okolí lze dosáhnout snížením ohrožení od konkrétních pohrom, což však jde jen u pohrom, které souvisí s činností člověka, a především snížením zranitelnosti technického díla, která je předmětem hodnocení rizika.

Na základě práce [4] bezpečný systém je chápán jako systém, který je zabezpečen vůči všem vnitřním a vnějším pohromám včetně lidského faktoru, tj. všem škodlivým jevům, a který ani při svých kritických podmínkách neohrožuje sebe a své okolí, tj. prostor, ve kterém žijí lidé. 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 kyber-socio-technologických systémů majících formu 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. Tvorba a provoz bezpečného systému jsou podstatně náročnější na znalosti, zdroje, síly a prostředky, a proto v běžné praxi jsou používány zabezpečené systémy, které jsou v případě potřeby doplněny organizačními opatřeními, která zajišťují ochranu veřejných aktiv, když předmětné systémy ohrožují sebe a své okolí.

Řešení žádného úkolu není možné uskutečnit izolovaně, tj. bez ohledu na okolí. Proto se dnes provádí strategické řízení, jehož základní principy jsou ukázány na obrázku 5. Obrázek 5 ukazuje základní mezníky, které rozhodují o tom, zda chování entity je bezpečné nebo nebezpečné při výskytu nebezpečné situace.

Obr. 5 *Mezníky rozhodující o bezpečném nebo nebezpečném chování entity při výskytu nebezpečné situace.*

2.4. Specifika složitých technických děl

Námi sledované složité kyber-socio-technologické systémy zahrnují jednak složité objekty a jednak infrastruktury, které mohou pracovat samostatně a dohromady pak plní zcela jedinečný úkol, který je vzdálený od úkolů jednotlivých složitých systémů (např. systémy pro výrobu, distribuci a spotřebu elektřiny, plynu apod.). Podle prací uvedených v [4] jsou pro ně důležité dvě systémové vlastnosti, a to interaktivní složitost a těsná spojení. Složité interakce jsou neplánované, neočekávané a většinou neznámé sekvence, které nejsou bezprostředně srozumitelné. Složité interakce v systémech systémů mají za následek nejednoznačná rozhodnutí, nestabilní preference a konfliktní cíle. Těsná spojení jsou nutnou podmínkou k eskalaci nežádoucích jevů vedoucích až k selhání či havárii. Charakterizují se jako proces, který je časově závislý, má malé časové rezervy, je invariantní (v procesu je jediné pokračování – B musí následovat po A), a v důsledku předmětných charakteristik je u něho omezený prostor pro improvizaci.

Interaktivní složitost a těsná spojení mezi prvky v sociotechnickém systému mohou vést ke kritické situaci v důsledku systémového selhání. To znamená, že riziko se tak stává systémovou vlastností. Kvůli složitosti a vysoké propojenosti sledovaných objektů je systematická analýza zranitelností a robustností s ohledem na selhání obtížná, a proto se používají výsledky simulací. Bezpečnost je definována jako nefunkční požadavek a je spojena s vynořujícími se vlastnostmi systému. Zvažované nefunkční vlastnosti nemohou být přiřazeny k jednotlivým komponentám systému. Vynořují se jako integrující výsledek chování systému. Proto požadavky na bezpečnost jsou formulovány na úrovni celého socio-technologického systému a poté sestupným procesem na dílčí systémy. Výsledek působení pohromy o jisté velikosti závisí na okamžitém stavu systému.

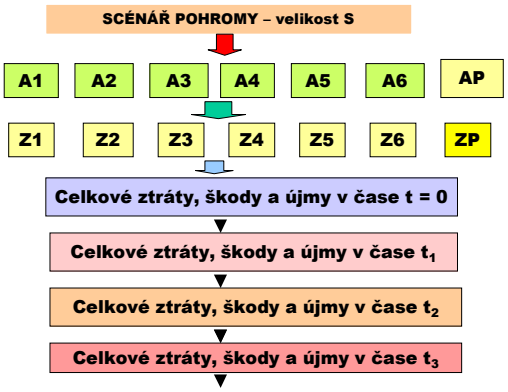
3. Nástroje pro práci s riziky technických děl

Výzkum zacílený na zajištění bezpečných technických děl a jejich bezpečného okolí [4,6,11] vyšel z poznání chování složitých technických děl za různých podmínek na základě sběru a zpracování konkrétních dat s použitím kritického myšlení a metod inženýrství zacíleného na práci s riziky. Jeho výsledky jsou reálné nástroje a postupy, kterými lze buď zabránit realizaci nepřijatelných rizik, anebo zmírnit jejich dopady na veřejná aktiva, tj. i na technická díla.

3.1. Výsledek výzkumu

Na základě současných znalostí přímé škody, ztráty a újmy na aktivech umíme určit, když vybereme správný scénář pohromy. Neumíme správně určovat škody, ztráty a újmy spojené s vazbami a toky ve složitých systémech [4]. Proto v případě potřeby zajistit bezpečnost závažných objektů stanovíme

expertním způsobem řadu relevantních scénářů prioritních pohrom. Jejich rizika určíme způsobem zobrazeným na obrázku 6 a expertním způsobem stanovíme ochranná opatření s tím, že největší váhu budou mít údaje pro scénáře s největší pravděpodobností výskytu, která bude stanovena na základě posouzení případových studií sestavených pro možné situace na základě reálných dat.



Obr. 6 *Vývojový diagram pro stanovení rizik pro potřeby strategického řízení bezpečnosti; A – aktiva a Z ztráty, škody a újmy na aktivech; označení: 1- životy a zdraví lidí, 2- bezpečí lidí, 3 – majetek, 4 – veřejné blaho, 5 – životní prostředí, 6 – infrastruktury a technologie, P – privátní*

Úkolem řízení rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Proto je třeba se dohodnout na tom, jaké požadavky bude výstup z hodnocení rizika splňovat a při vypořádávání rizik je nutné se snažit tyto požadavky dodržovat a případné nedodržení odůvodnit. Na základě poznání moderní způsob práce s riziky požaduje:

- riziko stanovovat během celého cyklu životnosti objektu (umísťování, projektování, výstavba, provoz,
- stanovení rizika zaměřovat na požadavky uživatelů a úroveň poskytovaných služeb,
- stanovovat rizika podle kritičnosti dopadů na procesy, poskytované služby a na aktiva, která stanovuje veřejný zájem,
- nepřijatelná rizika zmírňovat prostřednictvím nástrojů řízení rizik, tj. pomocí technických a organizačních návrhů, standardizací operačních postupů nebo automatizovanou kontrolou.

Postup v případě, že riziko není přijatelné dle údajů shromážděných v práci [7] spočívá v: vyhnutí se riziku (tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika), když to jde – u přírodních pohrom to nejde; odstranění zdrojů rizik, tj. zabránění vzniku pohrom, když to jde – u přírodních pohrom to nejde; snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom (např. snížením množství nebezpečných chemických látek v podnicích), když to jde – u přírodních pohrom to nejde; snížení závažnosti dopadů rizika, tj. příprava zmírňujících opatření jako jsou varovací systémy, systémy odezvy a obnovy; sdílení rizika, tj. rozdělení rizika mezi zúčastněné a pojišťovny; či retence rizika. Podle Mezinárodní organizace pro standardizaci kvalifikované řízení rizik musí respektovat:

- Řízení rizik musí být nedílnou součástí systému řízení sledované entity.
- Řízení rizik musí být obsaženo v každém procesu rozhodování sledované entity.
- Řízení rizik se musí explicitně zabývat nejistou a neurčitostí v procesech a podmínkách sledované entity a jejího okolí.
- Řízení rizik musí být systematické a strukturované.
- Řízení rizik musí vycházet z nejlepších dostupných informací.
- Řízení rizik musí být dynamické a vhodně reagovat na různé změny.
- Řízení rizik musí být uzpůsobeno každé instituci.
- Řízení rizik musí mít na zřeteli vliv člověka (lidský faktor).
- Řízení rizik musí mít schopnost neustálého zlepšování.

Rizika se ovládají na základě:

- aplikace technických opatření, která se realizují pomocí: výběru vhodných materiálů pro stavby a zařízení; způsobů konstrukce staveb a zařízení; vložení pasivních bariér, které zabrání jevům jako rozlet úlomků nebo rozptylu nebezpečné látky při ztrátě soudržnosti zařízení nebo stavby (např. obálky různých typů); vložení záložních zařízení a systémů, tj. několika zařízení majících stejnou roli a popř. používajících různé fyzikální principy k dosažení plnění úkolu; či vložení ochran důležitých prvků),
- řídicích systémů různých typů, které podle výsledků kontinuálního monitoringu upravují provoz,
- organizačních opatření, jejichž cíle jsou: ochránit zaměstnance, pracovní a popř. i okolní prostředí od škodlivých dopadů; a také stavby a zařízení objektu od velké destrukce, protože technologické celky nejsou levné a pro zachování schopnosti rozvoje území jsou jejich výrobky žádoucí.

Podle výsledků v praxi nejvyšší účinnost (až 80%) mají opatření technická [4,7].

Bezpečnost technických děl není jen záležitost technická, je směsicí aspektů bezpečí a spolehlivosti a vysoce souvisí s provozní spolehlivostí technického systému, která se popisuje zkratkami RAMS (Reliability, Availability, Mantainability, Security) nebo ARSS (Availability, Reliability, Safety, Security), přičemž platí:

- Availability (dostupnost) je schopnost systému poskytovat služby, když se požadují.
- Reliability (spolehlivost) je schopnost systému fungovat tak, je zamýšleno, tj. plnit úkoly tak, jak mu byly předepsány.
- Safety (bezpečnost) je schopnost systému fungovat tak, že nepůsobí škodlivě na sebe a na okolí.
- Security (bezpečí) je schopnost systému ochránit se před nežádoucími vnějšími a vnitřními vlivy.

Zajištění bezpečného technického díla je výsledkem fungování procesu řízení bezpečnosti (uspořádaného souboru opatření a činností), který je souborem procesů, jež mají pod kontrolou všechny faktory, které by mohly vést ke vzniku škody, ztráty či újmy na systému a jeho okolí. Ze systémového hlediska se bezpečnost skládá z následujících komponent:

- Informační činnost pro podporu rozhodování, protože stav bezpečí je výsledkem racionálního rozhodování a dobrých informací. Je však třeba počítat s vlivy na rozhodování o bezpečí jako jsou různá omezení (institucionální, právní, organizační), vlivy medií a veřejného mínění a dimenze politické (zájmové skupiny, ideologie) a technologické.
- Struktura technického systému, což jsou zařízení, technologie a organizační složky.
- Lidé jako subjekty bezpečnosti (experti a manažeři bezpečnosti), lidé jako objekty bezpečnosti (ochrana a prevence).
- Procedury spojující lidi a strukturu.

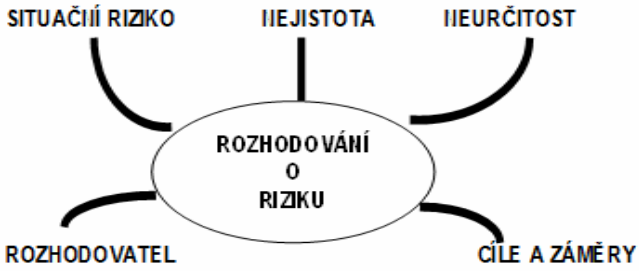
Výběr vhodné strategie na zmírňování rizika je tudíž velmi komplexní a kritický úkol. Nejde jen o snížení pravděpodobnosti výskytu selhání, ale také o zlepšení podmínek provozních aktiv, jejichž selhání může vést k velkým provozním nákladům. Nesprávná strategie snižuje produktivitu a výnosnost technologického systému. Výběr strategie zmírňování rizika je proto typický multikriteriální rozhodovací problém. Nejlepší strategie pro řízení rizika se musí vybrat z možných alternativ. Musí být vzato v úvahu množství kritérií, z nichž některá jsou konfliktní [4,7,8], např. obrázek 7.

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 [18] 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.

Obr. 7 *Příklad základního konfliktu při řízení kritických objektů – sestaveno s uvážením představy v [18]*

Jak již bylo řečeno, heterogenita a těsná propojení systémů v technologických objektech a infrastrukturách jsou příčinou obtížného popisu a emergentního chování předmětných systémů [4,6]. Klasické analytické metody nemají schopnost poskytnout dostatečný pohled kvůli složitosti systémů. K tomu je třeba hluboké porozumění a holistický přístup [6,11].
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 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
Je také skutečností, že i o riziku se rozhoduje s *rizikem* (technická záležitost − přesnost procesu měření a získávání dat), *nejistotou* (metodologická záležitost − spolehlivost teoretických východisek, identifikace a měření proměnných) a *neurčitosti* (konceptuální záležitost − rozpoznání a identifikace problému), obrázek 8.



Obr. 8 *Rizika spojená s rozhodováním o riziku*

Nejistota obecně je odchylka mezi modelem a realitou. Náhodnou nejistotu lze popsat metodami matematické statistiky, když máme k dispozici dostatečné množství dat. Znalostní nejistoty způsobené nedostatkem kvalitních dat nebo důsledky náhlých změn podmínek v technickém díle či jeho okolí lze postihnout jen specifickými postupy, založenými na metodách operační analýzy nebo expertními odhady [11].
Proto ke zvýšení „nebezpečnosti / kritičnosti“ rozhodnutí o rizicích technických děl obecně přispívají *složitost a rozmanitost cílů* (často jsou konfliktní), *citlivost rozhodnutí na změny, neurčitost klíčových proměnných a rozdílné pohledy na situaci.*

3.2. Norma ČSN ISO 31000

Základní systém pro řízení rizika stanovuje norma ČSN ISO 31000 [19]. Předmětná norma je mezinárodní a stanovuje řadu principů, které je třeba naplnit, aby bylo řízení rizik efektivní. Doporučuje, aby organizace rozvíjely, implementovaly a kontinuálně zlepšovaly rámec, jehož účelem je integrovat proces pro řízení rizik do svého celkového vedení, strategie a plánování, managementu, procesů podávání hlášení, politik, hodnot a kultury. Norma se opírá o projektové a procesní řízení v entitě. Její model je na obrázku 9.

Podle citované normy kvalifikované řízení rizik:

- vytváří hodnoty, protože přispívá k prokazatelnému dosahování cílů jako zlepšení zdraví, bezpečí, kvality životního prostředí, účinnosti procesů a činností atd.,
- je nedílnou součástí procesů, které probíhají v systému, protože za ní odpovídá řídící struktura systému a je nedílnou součástí všech procesů, z nich složených projektů v objektu i řízení změn,
- je součástí rozhodovacích procesů v systému, čímž pomáhá rozhodovat podle důležitosti a rozpoznávat alternativní způsoby řešení problémů,
- je realistické, protože se explicitně zabývá nejistotou i neurčitostí jak v podmínkách, v nichž se systém nachází, tak v procesech, které v objektu i vně probíhají,
- je systematické, uspořádané a včasné, čímž zajišťuje účinnost opatření a činností,
- je založeno na nejlepších dostupných informacích, což zajišťuje aktuální řešení založené na znalostech,
- je přizpůsobené systému, tj. je místně specifické, což zaručuje jak hospodárnost, tak účinnost,
- bere v úvahu lidské a kulturní faktory v systému, což ovlivňuje jeho přijatelnost u zúčastněných,
- je transparentní a komplexní, což zvyšuje jeho spolehlivost,
- je dynamické, opakovatelné a reaguje na změny v systému, což zaručuje jeho aktuálnost a napomáhá neustálému zlepšování a rozvoji systému.

Rámec řízení rizik zahrnuje:

- Pochopení systému a jeho souvislostí. V oblasti vně systému je třeba sledovat především kulturní, politické, právní, finanční, technologické, ekonomické, přírodní a konkurenční aspekty prostředí. V oblasti vnitřní se jedná především o kvalitu zdrojů a znalostí (např. kapitál, čas, lidé, procesy, systémy a technologie), informační systémy, informační toky a rozhodovací procesy (jak oficiální, tak neoficiální), vnitřní zainteresované strany, hodnoty, kultura a řídící struktura systému.
- Politiku řízení rizik. Politika řízení rizik určuje vazby mezi řízením rizik, cíli systému a dalšími politikami (je upřednostněna nebo je na posledním místě při rozhodování; jak se řeší konflikty; jaké metody řízení se používají; jaké nástroje podporují řízení rizik atd.
- Stanovení odpovědnosti za opatření a činnosti spojené s řízením rizik.
- Zdroje nutné pro řízení rizik včetně znalostí, dovedností, zkušeností a kompetencí.
- Stanovení mechanismů pro interní komunikaci a podávání zpráv o rizicích a jejich zvládání.
- Stanovení mechanismů pro externí komunikaci a podávání zpráv o rizicích a jejich zvládání.

Pro implementaci řízení rizik je nutné:

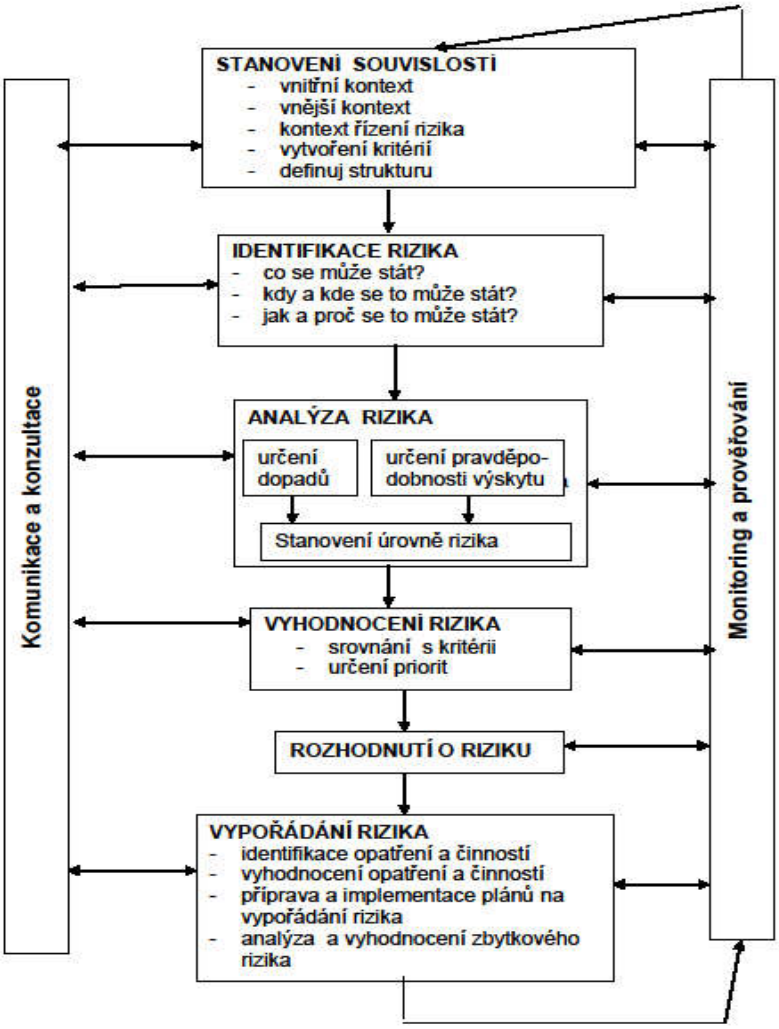
- Stanovit vhodnou strategii a politiku zařadit je do všech procesů v systému.
- Proces řízení rizik začlenit do všech významných úrovní a funkcí systému, tj. musí být součástí všech předpisů a směrnic pro procesy v systému.

Kritéria pro posuzování rizik vychází z:

- charakteru a druhu následků, které se mohou vyskytnout včetně jejich měření,
- způsobu stanovení pravděpodobnosti výskytu rizika,
- časového rámce následků a pravděpodobnosti výskytu rizika,
- způsobu určení úrovně rizika,
- úrovně, pod níž je riziko přijatelné nebo tolerovatelné,
- úrovně rizika, od níž je třeba zajistit cílenou odezvu,
- možnosti kombinace více rizik.

Analýza rizika znamená kritické studium kauzálního vztahu příčiny – dopady. Hodnocení rizik znamená porovnání úrovní rizik získaných analýzou rizik s kritérii pro posuzování rizik. Hodnocení rizika z pohledu prevence, připravenosti, odezvy a obnovymusí obsahovat:

- identifikaci ohrožení; specifikaci jevů (nebo scénářů), které ohrožují; specifikaci četnosti výskytu jevů (nebo scénářů), které ohrožují; odhad důsledků jevů (nebo scénářů), které ohrožují (ve kterých je zahrnuto i působení místní zranitelnosti); odhad rizika z kombinace důsledků jevů (nebo scénářů), které ohrožují a četností výskytu; ocenění kroků pro odhad rizika a provedení odhadu rizika; ocenění výsledků odhadu rizika pro potřeby rozhodnutí,
- standardy a normy pro regulaci projektování a provozování lidských činností; postupy a systémy řízení bezpečnosti; a popř. další,
- jakým způsobem jsou cíle řízení rizika nastaveny, zda: cíle o úrovni rizika jsou kvalitativní nebo kvantitativní; splňují technické standardy; standardy řízení jsou systémové; a další.



Obr. 9

Schéma pro řízení rizika [7]

Zvládání rizik dle podkladů uvedených v [7] znamená v případě, že riziko není přijatelné, provést:

- vyhnutí se riziku (tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika), když to jde – u přírodních pohrom to nejde,
- odstranění zdrojů rizik, tj. zabránění vzniku pohrom, když to jde – u přírodních pohrom to nejde,
- snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom (např. snížením množství nebezpečných chemických látek v podnicích), když to jde – u přírodních pohrom to nejde,
- snížení závažnosti dopadů rizika, tj. příprava zmírňujících opatření jako jsou varovací systémy, systémy odezvy a obnovy,
- sdílení rizika, tj. rozdělení rizika mezi zúčastněné a pojišťovny,
- retenci rizika.

Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika.
Pro posuzování účinnosti řízení rizika se používá index, který hodnotí výkonnost řízení rizika – RMI (Risk Management Index). Jedná se o kvalitativní míru, která je založená na cílech, které si řízení rizik vytyčilo. Někdy se též používají indikátory, u kterých se požaduje, aby byly transparentní, robustní, reprezentativní a snadno pochopitelné pro uživatele (veřejnost, politici, veřejná správa apod.).
Řízení rizik je třeba aplikovat na celé technické dílo, celou organizaci, která technické dílo spravuje, a to v mnoha oblastech a na mnohých úrovních, v kteroukoli dobu a také při řízení projektů a činností.

3.3. Validita zvládnutí rizika při použití norem a standardů

Další používané normy spojené s rizikem v technické praxi jsou: ČSN IEC 300-3-9; ČSN OHSAS 18001; ČSN EN ISO 12100; ČSN EN ISO 12 100-1; ČSN EN ISO 14121-1; ČSN EN 1050:2001; ČSN EN ISO 12100-1; ČSN EN ISO 12100-2; ČSN EN ISO 9000 atd. Normy a standardy ukládají požadavky, které jsou oprávněné. Nestanovují však často způsob, jak požadavky splnit, tj. jaká data a jaké metody použít a platí jen pro jisté podmínky. Proto při aplikaci norem a standardů si musíme uvědomit, co standardy pokrývají. V daném směru jsou obvykle založené na zásadách teorie pravděpodobnosti. Proto si musíme uvědomovat, že v žádném případě nepokrývají všechny možné varianty. Při použití normálního rozdělení platí, že interval (medián-σ, medián +σ) pokrývá 68.5 % případů; interval (medián -2σ, medián +2σ) pokrývá 95.4 % případů; interval (medián -3σ, medián+3σ) pokrývá 99.8 % případů. To znamená, že neplatí pro celý rozsah možných podmínek. Proto u důležitých technických děl je nutno provádět všechna hodnocení spojená s riziky a bezpečností jako místně specifická, tj. vycházet z logických základů metod a systémového pojetí entity; aplikace různých kódů a software, které nejsou místně specifické, mohou za kritických podmínek vést k selhání technických děl [6,20].
V praxi při práci s riziky spojenými s technickými díly se stále používají jen tradiční metody, jako jsou Kontrolní seznam, HAZOP, FMEA, FMECA, QRA apod. [7,11,16], protože pro ně existuje řada software. Jak bude v dalším odstavci doloženo, předmětné metody při práci s riziky nerespektují systémový charakter technického díla při dopadech vnějších pohrom, úmyslných vnějších aktů (např. korupce na správních úřadech s cílem oslabit konkurenceschopnost technického díla), teroristických činů apod., což potvrzují šetření US EPA [21]. To znamená, že platí, že předmětné metody lze použít s ohledem na bezpečnost technických děl jen při řešení některých úloh, ve kterých nejde o integritu bezpečnosti technického díla; všeobecně použitelné metody jsou správně aplikované metody What, If [7,11] a místně specifické kontrolní seznamy, které jsou sestavené experty.

4. Nástroje pro zajištění koexistence technických děl a okolí

Na základě poznatků uvedených v pracích [4,6,11] by technická díla měla být konstruována a provozována podle následujících zásad:

- každé technické dílo je systém systémů, který se v čase mění,
- v důsledku změn v technickém díle a okolí může dojít ke konfliktu, který nebyl očekáván,

- technické dílo i okolí jsou postihovány pohromami s tím, že velké pohromy se vyskytují zřídka a nepravidelně, a proto jejich možné velikosti nejsou odhalitelné metodami založenými na teorii pravděpodobnosti,
- pohromami pro technické dílo se stávají i vazby a spřažení, a to jak ty, které jsou úmyslně vytvořené z důvodu cíle, který dílo plní, tak i ty, které vzniknou neplánovaně tím, že v důsledku pohromy dojde k neočekávaným propojením, která pak vyvolají selhání díla.
- V důsledku náhodných i znalostních nejistot je pro každé lidské společenství z pohledu veřejného zájmu, konkurenceschopnosti technického díla a udržitelného rozvoje lidského systému důležité, zda:
- bezpečnost (tj. úroveň opatření a činností ve prospěch bezpečí lidí, tj. i technického díla) v čase roste či klesá,
- ve stanovených časových úsecích je dosahováno plánované úrovně bezpečnosti,
- aplikovaná opatření vedou skutečně ke zvýšení bezpečnosti.

Protože jak technické dílo, tak jeho okolí jsou složité systémy, které se vyvíjí a tento vývoj nemusí byt nutně synergický, aplikace přesných matematických metod založených na teoriích, které počítají jen s náhodnými změnami, není schopna určit parametry a jejich proměnnost, jež zajistí bezpečnost technického díla po celou dobu životnosti. Rizikové inženýrství proto zavádí do praxe nástroje, kterými lze zvládnout podmínky, pro něž nebylo technické dílo konstruováno.

Při stanovení rizik je základní aktivitou určení ohrožení, které představuje pohroma / škodlivý jev pro technické dílo. V případě technických děl se často používají k danému cíli techniky HAZOP, FMECA, FTA, ROA (Recursive Operability Analysis, která je méně časově náročná než FTA). V uvedených případech jde o strukturované procedury – organizované přes výrobní proces. Při identifikaci rizik se vyhodnocení škod provádí deterministicky a odhad četnosti výskytu pravděpodobnostně. Právě jejich zaměření na sledování výrobního procesu nedovoluje postihnout selhání na více místech z jedné příčiny [11].

Jelikož většinu rizik nelze odstranit při provozu, leží tíha ochrany technického díla na způsobu řízení bezpečnosti technického díla. Zavádí se pokyny pro provoz při abnormálních situacích: zvážit proměnlivost procesu, tj. odchylky od normálního provozu; příčiny proměnlivosti procesu; důsledky způsobené selháními bezpečnostních funkcí; a ochrana prováděná pomocí: alarmů; zásahu obsluhy; automatickými systémy pro bezpečnost.

Dle [22] existuje více než 60 metodik pro analýzu rizik, které umožňují řízení aspektů bezpečnosti průmyslových objektů. Jsou však místně specifické, a proto vždy před jejich použitím je třeba ověřit, zda jsou pro daný případ vhodné. Analýzy havárií [4,6] ukazují, že při výskytu vnější pohromy nebo chyby lidského činitele může dojít k poškozením na několika místech objektu současně, což stromy událostí založené na výrobním procesu neodhalí.

V práci [21] byly porovnány výše sledované nástroje a byla stanovena vhodnost postupů při práci s riziky v závislosti na cíli, který je v technickém díle požadován. Výsledek je v tabulce 1. Z tabulky vyplývá, že vždy jsou použitelné metody kontrolní seznam, What, If a jejich kombinace. Ostatní metody lze použít jen v určitých fázích řízení rizik zacíleného na bezpečnost technických děl.

Tab. 1 *Použitelnost nástrojů při práci s riziky technického díla; X – označuje použitelnost*

Fáze navrhování a provozu	**Kontrolní seznam**	**What If**	**Kombinace What If a kontrolního seznamu**	**HAZOP**	**FMEA**	**FTA**
Výzkum		X				
Projekt	X	X	X			
Zkušební provoz technického díla	X	X	X	X	X	X
Detailní	X	X	X	X	X	X

inženýrské práce						
Konstrukce + zahájení provozu	X	X	X			
Rutinní provoz	X	X	X	X	X	X
Modifikace	X	X	X	X	X	X
Vyšetřování nehod a havárií		X		X	X	X
Odstavení z provozu	X	X	X			

O problémech, které jsou spojené s aplikací stromových modelů, pojednává také práce [23], která ukazuje, že velkým nedostatkem aplikace stromových modelů v bezpečnostních a spolehlivostních studiích technických děl je, že technická díla pokládáme za hierarchicky uspořádaná a neuvědomujeme si předpoklady, které používáme při vytváření struktury modelů (tj. to, co zanedbáváme). Jde o předpoklady:

- Všechny komponenty jsou vzájemně nezávislé. Zanedbávají se vzájemná propojení trvalá i občasná.
- Systém má strukturu složenou z několika vrstev, které jsou znázorněny jako strom. Zanedbává se, že každý subsystém či komponenta může mít více stavů.
- Každá úroveň provozu odpovídá jedné konstelaci podmínek. Zanedbává se, že každá úroveň provozu (od perfektního výkonu po totální selhání) je výsledkem složité kombinace konstelací komponent při reakci na momentální podmínky.
- Oprava poruchy komponenty je okamžitá. Zanedbává se čas potřebný k identifikaci poruchy a k provedení nápravy.

Z důvodu tohoto zanedbání se pak musí v praxi u technického díla používat zálohy.

Když chceme řídit a vypořádat rizika u inženýrských systémů, musíme pochopit jejich složitost. Jde o spřažené / propojené komponenty (systémy), ve kterých jsou zpětné vazby, smyčky a mnoho činitelů. Jejich chování závisí na podmínkách, které jsou rozmanité, a proto nepředvídatelné. Proto jednoduché modely chování těchto systémů, pro které jsou software, nemají schopnost identifikovat všechna rizika, a to hlavně ta, která jsou málo pravděpodobná.

Práce [24] ukazuje, že míra získaného poznání na základě zpracování dat výsledek hodnocení významně závisí na kvalitě dat a zvolené metodě zpracování dat, což potvrzuje výsledky z naší praxe [25].

Problém výběru metod nastává u SoS. Z metodického pohledu řízení rizik SoS představuje koordinaci řady nesourodých procesů, které probíhají současně v různých oblastech a některé jejich výsledky se vzájemně podmiňují, tj. procesy jsou jistým způsobem na sobě závislé, tj. zvládnutí úkolů spojených se zajištěním bezpečnosti je určováno usměrněním opatření a činností v různých částech SoS. Z pohledu daného cíle je nutné, aby každý řídící orgán SoS chápal každý problém v existujících souvislostech a hledal jeho efektivní řešení v daných podmínkách s ohledem na další systémy, přitom postupoval racionálně a s ohledem na náklady a dostupné zdroje v příslušných oblastech. Uvedené požadavky jsou základním principem SMS pro SoS.

Na základě recentních poznatků a dlouholetých zkušeností s řešením složitých praktických úkolů, při kterých bylo nutno použít praktiky dobré inženýrské praxe, autorka sestavila návrh nástroje na identifikaci a řízení rizik SoS a pro podporu jeho aplikace v praxi jsou uvedeny výsledky testů na reálných datech. Proto na základě znalostí a zkušeností s navrhováním systémů pro podporu rozhodování [7,11] byl logickou syntézou údajů a zkušeností navržen komplexní nástroj pro identifikaci, analýzu, hodnocení a řízení rizik, včetně průřezových, který zaručuje přežití či kontinuitu aktiv při kritických pohromách.

Na základě zkušeností z praxe při práci s rizikem a zranitelností, a to především při hodnocení u technických děl [11], existují omezení při jejich užívání:

- pochopení konceptu metod je obtížné, protože vyžaduje kombinaci několika hledisek,
- nejsou jednotné pojmy a pletou se koncepty zacílené na spolehlivost, zabezpečení a bezpečnost,
- podpory informačních technologií jsou špatně strukturované, protože neodráží systémovou podstatu technického díla,
- uživatelé mají omezené znalosti a schopnosti pracovat např. s informačními technologiemi,
- provedení hodnocení je časově náročné a je i náročné na data,
- procesy hodnocení na sebe nenavazují,
- vedení technických děl se neřídí výsledky hodnocení rizik.

Práce [11] shrnuje výsledky testů nástrojů pro práci s riziky složitých technických děl a doporučuje používat metody: What, If; kontrolní seznamy; Decision Support System; Fischbone Diagram; a Risk Management Plan; jejich popisy jsou v [16].

5. Shrnutí poznatků pro praxi

Jelikož je skutečností, že mnoho zdrojů rizik nelze odstranit, tak pro bezpečí a rozvoj lidí je třeba, aby riziko bylo přijatelné, tak je třeba ho správně řídit. Pro zajištění bezpečí a rozvoj společenství lidí musí správy celků, na které je organizačně roztříděn lidský systém (tj. správci technických děl i správci území, tj. obce, kraje, státy a společenství států) dobře pracovat s riziky. Pro práci s riziky v každé entitě je třeba vymezit:

- koncept entity a jejich částí v systémovém pojetí,
- základní / prioritní či kritická aktiva entit,
- pojmy důležité pro chápání a řízení bezpečnosti entit,
- zdroje rizik, jejich dopady na chráněná aktiva entity,
- metody pro identifikaci, analýzu, hodnocení a posuzování rizik,
- způsoby řízení rizik,
- způsoby inženýrského vypořádání rizik,
- způsoby práce s riziky v čase.

Výzkum musí pro jednotlivé aktéry připravit datové soubory a nástroje, které budou jak pochopitelné, tak použitelné pro širší odbornou veřejnost. Možná bude třeba vybudovat i poradenskou síť takovou, jakou mají západní země v organizacích TSO (Technical Support Organization).

Na základě současného poznání [11] normativ určující úroveň práce s riziky má sedm položek (obrázek 10), které ovlivňují výsledek práce s riziky technického díla, tj. jeho bezpečnost, a to:

Obr. 10 *Položky, které ovlivňují výsledek práce s riziky technického díla*

- Kontext, do kterého jsou zasazena rizika spojená inherentně s technickými díly.
- Seznam zvlažovaných zdrojů rizik.
- Typ rizika.
- Způsoby vypořádání rizik.
- Procesní model práce s riziky, aplikaci TQM [17] a Coaseho teorému [26].
- Techniku řízení a vypořádání rizik technického díla.
- Způsob řízení rizik v čase.

Představa o řízení rizik procesů spojených s technickými díly a jejich okolím je zobrazena na obrázku 10. Technické dílo i okolí na sebe neustále působí, přičemž konfliktní situace nastávají zejména ve čtyřech fázích:

- výběr typu technického díla a jeho umístění do území,
- výstavba technického díla,
- provoz technického díla,
- vyřazení technického díla z provozu a umožnění dalšího využití území zabraného technickým dílem.

Protože jak technické dílo, tak jeho okolí jsou složité systémy, které se vyvíjí a tento vývoj nemusí byt nutně synergický, tak aplikace přesných matematických metod založených na teoriích, které počítají jen s náhodnými změnami, není schopna určit parametry a jejich proměnnost, jež zajistí bezpečnost technického díla po celou dobu životnosti. Inženýrské disciplíny pracující s riziky proto zavádí do praxe nástroje založené na heuristickém přístupu pro práci s riziky, kterými lze zvládnout i podmínky, pro něž nebylo technické dílo konstruováno.

Nashromážděná fakta ukazují, že pro zajištění bezpečnosti složitých technických děl je nutno z důvodu složitosti pracovat s riziky specifickým způsobem. Nestačí aplikace norem a standardů, které mají omezenou platnost, je třeba poznat dopady stabilních i možných dočasných propojení mezi prvky, komponentami a systémy technického díla i při abnormálních a kritických podmínkách a podle toho sestavit systém řízení bezpečnosti a způsob jeho fungování v čase. Jelikož během času vznikají rizika nová, je třeba mít pravidelný monitoring rizik, jehož součástí budou i připravená nápravná opatření pro případ výskytu nepřijatelných rizik.

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání technických děl, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie (často označované jako ***černé labutě, dračí králové*** atd.). Proto nyní připouštíme, že složité objekty, jakými jsou technická díla, jsou z různých důvodů čas od času v nestabilním stavu a vznikají extrémní havárie, kaskády selhání bez zjevné příčiny, neobvyklé jevy apod., tj. připouštíme nejistoty náhodné i znalostní v jejich chování. Z důvodu zajištění jejich bezpečnosti a ochrany lidí:

- zavádíme specifická technická opatření (např. po havárii jaderné elektrárny Fukushima čtvrtý nezávislý zdroj energie a čtvrtý nezávislý zdroj chladiva pro případ odezvy na extrémní pohromu),
- připravujeme řešení odezvy pro možné případy, kdy se realizují rizika z příčin, které nelze odhalit pravděpodobnostními přístupy, a budujeme pro ně náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik inženýrů a záchranářů.

V návaznosti na tento fakt, výsledky výzkumu v EU, uvedené v práci [4], ukazují velmi mnoho nedostatků spojených s prací s riziky. Příčiny uvedených nedostatků v oblasti vrcholového řízení státůbyly identifikoványtakto:

- řízení je předurčené politickými a vojenskými aspekty; postrádá lidský rozměr a dává malou podporu obyvatelům EU,
- řízení není prováděno na základě kvalifikovaných dat zpracovaných kvalifikovanými metodami,
- řízení je často určeno fixními ideami bez reálného ohodnocení jejich realizovatelnosti,
- řízení je založeno na představě, že všechno je stacionární, tj. nerespektuje se dynamický vývoj světa, který vyžaduje přípravu na možné extrémní scénáře situací a opatření pro přežití lidí,
- řízení není realizované na základě principu systém řízení bezpečnosti systému systémů v dynamicky proměnném světě.

Ve všech úvahách si je třeba uvědomit známé pravdy, a to:

- riziko je mírou inherentní vlastnosti lidského systému (světa) i každého technického díla, tj. není možné se mu zcela vyhnout,
- zdroje rizik jsou uvnitř i vně technického díla a v procesech, které v technickém díle probíhají a mění se v čase,
- větší riziko znamená zároveň možnost většího zisku i ztrát, a proto riziko vyžaduje duální pohled – pokud chceme získat vyšší zisk nebo jiné přínosy, zvyšujeme i riziko nezdaru a ztrát, a proto úkolem managementu rizik je tyto dvě stránky vyvážit,
- čím přesněji definujeme předmět a cíle technického díla, tím je riziko nižší, protože nejvíce rizik vzniká z nejednoznačných definic předmětu a cílů technického díla,
- dříve identifikované riziko má vyšší šanci na úspěšné vyřešení a naopak, pozdější identifikací rizika nebo jeho ignorováním a následným řešením nečekaných problémů je technické dílo výrazně poškozováno,
- vše, co není řízeno, dopadá náhodně, většinou však hůře než při aktivním řízení (aktivní řízení rizik znamená trvalé sledování rizika, přípravu a provádění plánů ošetření rizik; zanedbání tohoto principu vede ke zbytečným ztrátám),
- rizika je třeba řídit efektivně. Z pohledu hospodárnosti se zdroji, silami a prostředky nemá smysl se zabývat všemi riziky, ale jen těmi, kde vynaložené úsilí přinese výsledky, jež toto úsilí přesvědčivě převyšují.

Na základě zkušeností autorky, která se v roli recenzenta odborných prací a projektů setkala s výsledky specialistů z oblasti informačních technologií, kteří na křídovém papíře prezentovali barevné obrázky modelů zpestřené blikajícími efekty, jež odporovaly fyzikálním zákonitostem (např. zákonu o zemské přitažlivosti, zákonu útlumu energie se vzdáleností apod.) uvádíme pravidla publikovaná Golombem v r. 1970 [27]:

1. Nevěřte důsledkům 33. řádu u modelů 1. řádu.
2. Neextrapolujte výsledky modelu za hranice jeho platnosti.
3. Nepoužívejte žádný model, dokud neporozumíte zjednodušujícím předpokladům, na kterých je založen.
4. Nevěřte tomu, že model je realita.
5. Nepokoušejte se realitu přizpůsobit modelu.
6. Neomezujte se pouze na jediný model sledovaného jevu nebo procesu. Použití více modelů pro sledovaný jev umožňuje lépe porozumět jeho různým aspektům.
7. Nepoužívejte modely, o kterých se ví, že nejsou správné.
8. Nebuďte zamilovaní do svého modelu.
9. Neaplikujte terminologii oblasti A na problémy oblasti B. Neprospěje to žádné z nich.
10. Nečekejte, že pokud jste problém pojmenovali, tak jste ho také vyřešili.

Zejména je třeba se vyvarovat přístupu, který je možno shrnout do následujících bodů:

- Pokud máte kladivo, hledáte hřebík.
- Pokud máte dobré kladivo, vše vypadá jako hřebík.

Dynamické vlastnosti systémů jsou dány dynamickými charakteristikami, které mohou být algebraické nebo experimentální. Každý řídicí systém má pět vzájemně souvisejících struktur: rozhodovací; funkční; organizační; informační; a technické zabezpečení. A každá struktura řeší specifický okruh problémů, tj. jde též o systém systémů. Cílem praktických úloh je pochopitelně najít optimální řešení pro všechny uvedené systémy, jak ukazuje [6].

Poznatky pro kvalitní práci s riziky, zacílenou na bezpečné technické dílo a jeho bezpečné okolí, uvedené výše lze shrnout následovně:

- určit kritické procesy, kritická místa a kritická aktiva technického díla,
- zvážit všechny možné pohromy, které mohou ovlivnit technické dílo (All-Hazard-Approach) [14] a vypořádat se s nimi pomocí aplikace přístupu Defence-In-Depth [28],
- monitorovat a posuzovat rizika v čase a posuzovat úroveň bezpečnosti technického díla a v případě, že není žádoucí reagovat kvalifikovaně na prioritní rizika.

Důležité je si uvědomit, že riziko je nejen proměnné v čase, ale i místně specifické, a tudíž není určitelné nástroji, které byly odvozené jinde pro konkrétní situace a mají softwarové podoby. Zde je nutné respektovat podmínky transferu technologií a nástroj přizpůsobit místním podmínkám. Přizpůsobení místním podmínkám vyžaduje:

- rekognoskaci technického díla a jeho okolí doprovázenou určením kritických procesů, kritických míst a kritických aktiv technického díla,
- stanovení variantních scénářů pro prioritní pohromy (příčiny prioritních rizik), jejichž zdroje jsou uvnitř i vně technického díla a také lidský faktor. Z důvodu výše zmíněného poznání, že použití jednoho software, které respektuje jen výrobní proces, vede k nezvážení dopadů pohromy na několik míst technického díla najednou (v technickém slangu mluvíme o příčinách selhání technického díla z jedné příčiny), je nutné vytvořit scénáře pro technické dílo jako celek s mnoha aktivy, i scénáře pro dobře definované části kolem kritických míst. Na základě všech scénářů stanovit dopady na aktiva technického díla metodou What, If,
- logicky vyhodnotit variantní scénáře a jejich dopady, a přitom vyznačit a posoudit možná propojení.

Pak už lze použít logické rutinní postupy, které jsou shodné u obecných metod, popsané v [7,16], a které jsou obsaženy v modelu na obrázku 9 obsaženém v normě ISO 31 000 [19], a mají softwarové podpory. Z uvedeného je zřejmé, že know how práce s riziky je právě v prvních bodech, které jsou určeny specifikami technického díla. Ze zkušeností z praxe vyplývá, že právě tato část je často podceněná zpracovateli, kteří věří v sílu software. Kvalitní provedení první specifické části práce s riziky vyžaduje spolupráci odborníka, který má zkušenosti s popsanými úkoly a odborníků z technického díla, kteří mají místní znalosti a zkušenosti. Pro podporu praxe, jsou proto v publikaci uvedeny konkrétní příklady jak vzorů úspěšných aplikací nástrojů používaných inženýrskými disciplínami při práci riziky, tak obecné nástroje, které lze použít u každého technického díla, protože je v nich inherentně zabudována proměnnost sledovaných položek v prostoru i čase.

LITERATURA

[1] ASCE. Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters“, Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards“, Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters“. Washington: ASCE 2001.

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

[3] KIRCHSTEIGER, Ch. (ed.). Risk Assessment and Management in the Context of theSEVESO II Directive. Amsterdam: Elsevier, 1998.

[4] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů.* ISBN: 978-80-01-05771-1. Praha: ČVUT 2015, 208p.

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

[6] PROCHÁZKOVÁ, D.*Zásady řízení rizik složitých technologických zařízení.* ISBN: 978-80-01-06180-0. Praha: ČVUT 2017, 364p. http://hdl.handle.net/10467/72582

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

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

[9] UNDP. *Human Development Report*. ISBN: 978-92-1-126413-5. New York: UN 2016, 272p., http://hdr.undp.org

[10] ČR. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

[11] PROCHÁZKOVÁ, D.*Analýza, řízení a vypořádání rizik spojených s technickými díly*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222p.

[12] EU. http://ec.europa.eu

[13] PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládání*. ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234p.

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

[15] PROCHÁZKOVÁ, D. Metodika pro odhad nákladů na obnovu majetku v územích postižených živelní nebo jinou pohromou. ISBN 978-80-86634-98-2. Ostrava: SPBI SPEKTRUM XI 2007, 251p.
[16] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369p.
[17] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991
[18] BORGES, HICKEY, C. Balancing Safety and Performance through QRA and RAM Analyses. In: *Safety and Reliability: Methodology and Applications*. ISBN:978-1-138-02681-0. London: Taylor & Francis Group 2015, pp. 445-452.
[19] ISO. Risk Management – Principles and Guidelines, ISO 31000:2009.
[20] FEMA. *Promoting Critical Infrastructure Protection by Emergency Managers and First Responders.* Nationwide. 2005. www.usfa.fema.gov
[21] US EPA. PHA Techniques in Chemical Emergency Prevention & Planning. *Newsletter* 2008, No. 8, pp. 3-6.
[22] CONTINI, P. M., CONTINI, S., COPELLI, S., ROTA, R., DEMICHELA, M. From HazOp Study to Automatic Construction of Cause Consequence Diagrams for Frequency Calculation of Hazardous Plant States. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-315-64841-5. London: Taylor &Francis Group 2015, pp. 347-355.
[23] GUANGHAO ZHU, YUFENG SUN & GUANGYAN ZHAO. A Dynamic Fault Tree Method for Availability Assessment of the Repairable Gas Transmission System. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-315-64841-5. London: Taylor &Francis Group 2015, pp. 1897-1903
[24] SHORTRIDGE, J. E., AVEN, A., GUIKEMA, S. D. Risk Assessment under Deep Uncertainty: A Methodological Comparison. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1. www.tayloeandfrancis.com, London: Taylor &Francis Group 2015. pp. 847-855.
[25] ČVUT. *Archiv řešených úloh z oblasti řízení bezpečnosti a krizového řízení.* Praha: ČVUT, fakulta dopravní, ústav bezpečnostníchtechnologií
[26] COASE, R. H. The Problem of Social Cost. *Journal of Law and Economics,* 3 (1960), pp. 1-44.
[27] GOLOMB, S. W. Mathematical Models - Uses and Limitations of Simulation. *Mathematical Journal*, 14 (1970), 4, pp 197 - 198.
[28] INSAG. *Defence in Depth in Nuclear Safety. INSAG-10.* ISBN 92-0-103295-1. Vienna:IAEA, 1996.
[29] *Sbírka zákonů ČR*

NÁVAZNOST NA VÝZKUMNÉ PROJEKTY:

EU „FOCUS - Foresight Security Scenarios – Mapping Research to a Comprehensive Approach to Exogenous EU Roles";
grant ČVUT „OHK2-003/15, Řízení bezpečnosti a ochrana kritických objektů a kritických infrastruktur";
a projekt MŠMT „RIRIZIBE CZ.02.2.69/0.0/0.0/16 _018/000".
Autorka děkuje všem zadavatelům uvedených projektů za vytvoření podmínek, které jí umožnily odbornou práci.

ADRESA AUTORA

Doc. RNDr. Dana Procházková, PhD., DrSc.
ČVUT v Praze, Česká republika
e-mail: prochdana7@seznam.cz
t.: +420 608147773

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.