

ŘÍZENÍ RIZIK SLOŽITÝCH TECHNOLOGICKÝCH SYSTÉMŮ

Dana PROCHÁZKOVÁ

MANAGEMENT OF RISKS OF COMPLEX TECHNOLOGICAL SYSTEMS

ABSTRAKT

PRÁCE SE ZABÝVÁ ŘÍZENÍM RIZIK KOMPLEXNÍCH TECHNOLOGICKÝCH SYSTÉMŮ, TJ. OBJEKTŮ A INFRASTRUKTUR, KTERÉ JSOU TYPU SYSTÉM SYSTÉMŮ. OBSAHUJE VÝSLEDKY ŠETŘENÍ ÚROVNĚ ŘÍZENÍ JEJICH HAVÁRIÍ A IDENTIFIKUJE JEHO NEDOSTATKY V EU. NA ZÁKLADĚ EXISTUJÍCÍCH ZNALOSTÍ UVÁDÍ KONCEPT PRO ZAJIŠTĚNÍ JEJICH

BEZPEČNOSTI A ZPRACOVÁVÁ PĚTISTUPŇOVÝ MODEL ŘÍZENÍ JEJICH BEZPEČNOSTI. UKAZUJE ZPŮSOB ŘEŠENÍ OČEKÁVANÝCH KONFLIKTŮ V PRAXI PŘI ŘÍZENÍ JEJICH BEZPEČNOSTI A ÚROVEŇ SCHOPNOSTI SOUČASNÝCH POSTUPŮ PŘI ZVLÁDÁVÍ JEJICH RIZIK.

Klíčová slova: systémy systémů, bezpečnost, riziko, řízení rizik, koncept zajištění bezpečnosti, pětistupňový model pro zajištění bezpečnosti, řízení konfliktů, úroveň schopnosti současných postupů při vypořádání rizik

ABSTRACT

THE PAPER DEALS WITH MANAGEMENT OF RISKS OF COMPLEX TECHNOLOGICAL SYSTEMS, I.E. FACILITIES AND INFRASTRUCTURES THAT POSSESSED THE TYPE OF SYSTEM OF SYSTEMS. IT CONTAINS RESULTS OF INVESTIGATION OF LEVEL OF MANAGEMENT OF THEIR ACCIDENTS AND IT IDENTIFIES ITS DEFICIENCIES IN THE EU. ON THE BASIS OF

PRESENT KNOWLEDGE IT GIVES THE CONCEPT FOR ENSURING THEIR SAFETY AND PROCESSES MODEL WITH FIVE STEPS FOR MANAGEMENT OF THEIR SAFETY. IT SHOWS THE WAY OF SOLVING THE EXPECTED CONFLICTS IN A PRACTICE AT MANAGEMENT OF THEIR SAFETY AND THE LEVEL OF CAPABILITY OF PRESENT PROCEDURES AT FIGHT WITH THEIR RISKS.

Key words: system of systems, safety, risk, risk management, concept of ensuring the safety, model with five steps for ensuring the safety; conflict management, level of capability of present procedures at risks defeat

ÚVOD

Technologické systémy tvoří objekty a infrastruktury. Jsou různě složité a hlavně jsou nutné pro životy lidí v dnešním světě, protože jim zajišťují výrobky a služby potřebné pro kvalitní život. Je však pravdou, že na jedné straně usnadňují život lidí, ale na straně druhé ho ohrožují, když dojde k haváriím. Největší rizika jsou spojená s objekty, které jsou složité a obsahují nebezpečné chemické látky. Složitost komplexního technologického systému není dána pouze počtem jeho prvků, nýbrž také jejich rozrůzněností, rozmanitostí a hustotou i významem vztahů mezi prvky. Složitost de facto znamená, že změna jedné proměnné ovlivňuje mnohé další proměnné, a to navíc nelineárním způsobem.

Velké technologické provozy a technické systémy jsou víc než jen množinou technických částí zařízení a součástek. Jsou odrazem organizační struktury, managementu, provozních předpisů a kultury konstrukčních organizací, které je vytvořily a také jsou zpravidla i odrazem společnosti, ve které byly vytvořeny [1-3].

Nehody a havárie v technologických objektech a infrastrukturách jsou často svalované na chyby operátorů nebo zařízení, bez rozlišení průmyslových, organizačních a manažerských faktorů, které způsobily, že se předemné chyby a nedostatky staly nevyhnutelnými. Příčiny havárií mají často, ne-li skoro vždy, kořeny v organizaci - v její kultuře, managementu a struktuře a platí, že všechny faktory jsou kritické pro bezpečnost technických systémů.

Je skutečností, že sice existuje řada přístupů, norem a standardů, jejichž aplikací se zajišťuje bezpečnost objektů, ale havárie se vyskytují stále, a proto se hledají další účinnější přístupy. Na světové konferenci ESREL 2014 [4] bylo prezentováno několik sdělení s výsledky získanými aplikací přístupu obrana do hloubky (defence in depth), který byl na konci 80. let zaveden v jaderné energetice. Prezentované aplikace sice nepoužívají stejné pojmy, jako používá Mezinárodní atomová agentura ve svých návodech [5], ale cíl, koncept a přístupy jsou stejné.

Základní požadavky zmíněných přístupů jsou, aby se v technologických objektech a infrastrukturách:

- používaly systémy inherentní bezpečnosti,
- řídila průřezová rizika v dynamicky proměnném světě,
- a aplikoval proces řízení bezpečnosti, který dominuje nad všemi procesy organizačními i technickými, které probíhají v technologickém objektu či infrastruktuře.

Poslední požadavek je v souladu s dnešním stylem řízení, kterým je projektové a procesní řízení [1].

Proto se autorka v práci soustředila na vypracování návrhu postupného řízení a zvládání rizik s cílem zajistit bezpečnost komplexních technologických objektů a infrastruktur, které z pohledu systémové teorie představují systémy systémů [6], tj. soubory otevřených vzájemně propojených systémů, které plní společný úkol za určitých podmínek, kterým říkáme podmínky interoperability.

Vzájemné propojení systémů znamená vzájemnou závislost, která za jistých podmínek způsobuje kaskádovitá selhání, jež na kratší či delší dobu ohromují život lidských jedinců i celé lidské společnosti [1,6].

PRINCIP ŘÍZENÍ TECHNOLOGICKÝCH SYSTÉMŮ

Z pohledu exaktních věd se každý dílčí technologický systém (objekt či infrastruktura) skládá z řízeného objektu a z řídicího systému. Řízeným objektem je většinou složitý nelineární systém, který: je tvořen konečným počtem prvků; každý z prvků je jednoznačně popsán konečným počtem měřitelných veličin; vzájemné vazby mezi prvky jsou jednoznačně formulovány.

Dynamické vlastnosti řízeného objektu můžeme popsat pomocí diferenciálních rovnic, jejichž řešením je stavový vektor. Stavový vektor umožňuje pomocí minimálního počtu veličin určit stav systému v libovolném časovém okamžiku. Řídicí systém musí udržovat určené fyzikální veličiny na předem určených hodnotách.

V procesu řízení ve smyslu ovládání (regulace) mění řídicí systém působením na akční veličiny stav technologického systému tak, aby bylo dosaženo žádaného stavu. U řídicího systému se dle recentních pojetí, které kladou nejvyšší důraz na bezpečnost, sledují v prioritním pořadí vlastnosti jako:

- bezpečnost (úroveň dodržování stanovených podmínek provozu a nevytváření škodlivých (nepřijatelných) dopadů na samotný systém a na jeho okolí),
- funkčnost (úroveň plnění požadovaných úkonů),
- provozuschopnost (úroveň plnění požadovaných úkonů v závislosti na podmínkách normálních, abnormálních a kritických); provozní stálost (úroveň dodržování stanovených podmínek provozu v čase),
- a inherentně zabudovaná odolnost vůči možným pohromám [7].

Protože technologický systém (objekt či infrastruktura) i prostředí, ve kterém je systém umístěn, se dynamicky mění, je třeba počítat s výskytem havárií. Z důvodu ochrany lidí a životního prostředí je nutné realizovat odpovídající formu řízení, a to respektovat dynamicky proměnný svět. To znamená připustit jevy, které mohou od určité velikosti poškodit systém, což znamená pracovat s riziky.

VÝSLEDKY ŠETŘENÍ ÚROVNĚ ŘÍZENÍ HAVÁRIÍ SPOJENÝCH S TECHNOLOGICKÝMI CELKY A INFRASTRUKTURAMI V EVROPSKÉ UNII

Šetření úrovně řízení havárií spojených s technologiemi a infrastrukturami v EU bylo provedeno v rámci projektu FOCUS [8] a použita data z odborné oblasti, která jsou citována na příslušných místech a data o legislativě a řídicích mechanismech v EU [9]; např. SEVESO, REACH aj. Ve vlastním výzkumu byly zvaženy pohromy, které se vztahují ke sledované oblasti, a to nehody, havárie, selhání infrastruktur, selhání technologií, ztráty obslužnosti apod. Metoda šetření spočívala v expertním vyhodnocení dotazníku, který byl sestaven pro projekt FOCUS [10] a byl zacílen na zjištění nedostatků v řízení EU a členských zemí s ohledem na řízení pohrom (Disaster Management), které je základem pro budování bezpečné EU s udržitelným rozvojem.

Dotazník byl vyhodnocen 25 experty s vysokoškolským vzděláním a s praktickými zkušenostmi (příslušníci bezpečnostních složek, bezpečnostní manažeři v průmyslu a veřejných organizacích, inženýři z průmyslu, inspektoři BOZP, pracovníci veřejné správy, akademičtí pracovníci, právníci, ekonomové a jeden politolog). Celkové vyhodnocení úrovně řízení pohrom spojených s technologiemi a infrastrukturami v EU provedené 5 experty ČVUT je uvedeno v tabulce 1.

Tab. 1 - Výsledky posouzení úrovně řízení pohrom spojených s technologiemi a infrastrukturami.

Otázka	Odpověď + její průkaz
Obsahuje seznam sledovaných pohrom uvedený výše všechny pohromy možné na území EU?	Je třeba doplnit zneužití technologií (jaderných, nano i IT), zneužití genetického inženýrství a zneužití látek CBRNE.
Které ze sledovaných pohrom jsou pro území EU nejhorší? Udělejte pořadí dle vašich znalostí a zkušeností.	1. Nadprojektová havárie s přítomností radioaktivních látek. 2. Nadprojektová havárie s přítomností nebezpečných látek mutagenních, karcinogenních a nebezpečných pro reprodukci. 3. Dlouhodobý výpadek elektrické infrastruktury. 4. Dlouhodobý výpadek dodávek pitné vody. 5. Dlouhodobý nedostatek základních potravin.
Pro které sledované pohromy není systematicky prováděna prevence? Je úroveň prevence dostatečná? Jaká je situace ve vaší zemi? Co je třeba zlepšit?	Prevenci jaderných havárií i připravenost na jejich zvládnutí je třeba zlepšit na základě poučení z havárie jaderné elektrárny Fukushima [11]. Jistá zlepšení je třeba provést v oblasti řízení bezpečnosti i u dalších technologií v EU i v ČR. Pozornost je třeba věnovat transportu nebezpečných látek, a to především technickým otázkám, Je třeba zavést normy a standardy pro infrastruktury, které zajistí jejich kapacitu, robustnost a posílí jejich odolnost. V EU i v ČR chybí robustní opatření zabraňující zneužití technologií.
Pro které sledované pohromy není v EU systematicky zajišťována připravenost? Je úroveň připravenosti dostatečná? Je připravenost prováděna všemi složkami společnosti (včetně veřejnosti) dostatečná?	Na základě poučení z Fukushima zcela chybí připravenost na nouzové situace, které nastanou, když selžou bezpečnostní systémy [11].

Jaká je situace ve vaší zemi? Co je třeba zlepšit?	
Pro které sledované pohromy nemá EU systematicky připravenou kvalifikovanou odezvu? Je úroveň této odezvy dostatečná? Jaká je situace ve vaší zemi? Co je třeba zlepšit?	EU nemá zajištěn systém odezvy. Členské státy mají systémy odezvy různé; jsou určeny národní legislativou. V ČR jsou funkční systémy odezvy zajišťované IZS a hygienickou službou. V ostatních oblastech jako je finanční sektor, sektor správného řízení věcí veřejných apod. úroveň systémů je nízká.
Pro které sledované pohromy nemá EU systematicky připravenou kvalifikovanou obnovu? Je úroveň této obnovy dostatečná? Jaká je situace ve vaší zemi? Co je třeba zlepšit?	EU nemá vlastní systém obnovy. Poskytuje finanční výpomoc v případě vybraných pohrom, jestliže jsou splněny požadavky specifického právního předpisu. ČR má zákon č. 12/2002 Sb., který upravuje obnovu po živelních a jiných pohromách, ale plán obnovy, který specifikuje zásady a postupy obnovy (jako má třeba FEMA [1]) nemá.
Která sledovaná pohroma může způsobit kritické situace v EU? Která sledovaná pohroma může způsobit kritické situace ve vaší zemi?	Nadprojektová jaderná havárie. Dlouhodobý výpadek elektrické energie. Dlouhodobý výpadek dodávek pitné vody. Dlouhodobý výpadek dodávek potravin. Dlouhodobé selhání finanční infrastruktury.
Která sledovaná pohroma může způsobit krizové situace v EU? Která sledovaná pohroma může způsobit krizové situace ve vaší zemi?	Masivní selhání finančního trhu. Nadprojektová jaderná havárie. Dlouhodobý výpadek elektrické energie. Dlouhodobý výpadek dodávek pitné vody. Dlouhodobý výpadek dodávek potravin.
Pro které krizové situace v EU není úroveň krizového řízení dostatečná? Pro které krizové situace ve vaší zemi není úroveň krizového řízení dostatečná?	Nedostatky se projevují ve všech krizových situacích, kdy bude třeba aplikovat strategické, systémové a proaktivní řízení, protože současné krizové řízení uvedené parametry nemá.
Které zranitelnosti lidské společnosti v EU mohou způsobit změnu kritické situace na extrémní situaci? Které zranitelnosti lidské společnosti ve vaší zemi mohou způsobit změnu kritické situace na extrémní situaci?	Nedostatek technických prostředků, nedostatečné znalosti a výcvik řídicích pracovníků, špatné řízení odezvy a nedostatek financí.
Máme spolehlivé metody pro určení scénářů všech sledovaných pohrom očekávaných v EU? Máme spolehlivé metody pro určení scénářů všech sledovaných pohrom očekávaných ve vaší zemi?	Metody používané v EU, členských zemích EU i v ČR jsou založené na deterministických a stochastických přístupech a na předpokladu, že každý systém je stále ve stacionárním stavu nebo blízko něho [6]. Poučení z Fukushima [11] ukazuje, že je třeba vylepšit metody spojené se stanovením zadávacích podmínek pro projekt, výstavbu i provoz technologických objektů a infrastruktur.
Známe pro všechny sledované pohromy v příloze úspěšná opatření a činnosti pro prevenci, zmírnění, odezvu a obnovu? Jaké slabiny jsou ve znalostech o opatřeních a činnostech pro prevenci, zmírnění, odezvu a obnovu?	Teoreticky jsou opatření a činnosti pro prevenci, zmírnění, odezvu a obnovu známy [12]. Konkrétní opatření a činnosti jsou místně specifické. Jejich určení je provedeno jen pro případ důležitých objektů.
Co je nutné vylepšit?	Systém řízení území a objektů.
Jaký výzkum je neefektivnější pro zlepšení řízení bezpečnosti v EU? Jaký výzkum je neefektivnější pro zlepšení řízení bezpečnosti ve vaší zemi?	Řízení integrálního rizika. Dosud aplikované postupy nezvažují průřezová rizika, která jsou příčinou kaskádovitých selhání složených systémů.
Jaké principy, legislativa a pravidla spolupráce v EU jsou nutné pro bezpečí a udržitelný rozvoj lidí?	Respektování zásad pro řízení integrální bezpečnosti [1].
Můžete navrhnout opatření pro odvrácení sociálních krizí v EU?	Respektování veřejného zájmu a zásad pro řízení integrální bezpečnosti [1].

Na základě údajů v tabulce 1 je posouzena úroveň řízení věcí veřejných EU z pohledu řízení havárií spojených s technologiemi a infrastrukturami. Na základě posouzení jsou identifikovány základní nedostatky spojené s řízením sledovaných pohrom a jsou identifikovány oblasti, ve kterých je třeba přijmout opatření (tabulka 2). Z výsledku vyplývá, že nedostatků je mnoho. Je to způsobeno tím, že v současném řízení pohrom všeho druhu chybí zacílení na prioritní problémy.

Tab. 2 - Návrh oblastí řešení identifikovaných nedostatků. Tučně jsou vyznačeny oblasti, které jsou zvláště důležité pro řešení uvedených nedostatků. Ve sloupci „jiné“ M označuje nutnost monitoringu a K nutnost sestavit plán kontinuity a přežití lidí.

Pohroma	Seznam nedostatků	Typ opatření a činností na odstranění nedostatků				
		legislativa	specifické řízení	výzkum	vzdělání	jiné
Ztráta obslužnosti území (selhání některé z infrastruktury)	Chybí koncept pro vytvoření jak robustní kritické infrastruktury, tak robustních dílčích infrastruktur; zvláště pak kybernetické infrastruktury.	Ano	Ano	Ano	Ano	K
Nadprojektová havárie s přítomností radioaktivních látek	Řízení bezpečnosti vychází z předpokladu, že vícenásobně zálohované bezpečnostní systémy zajistí bezpečnost vždy. Poučení z Fukushima [11] však ukazuje, předpoklad není oprávněný.	Ano	Ano	Ano	Ano	K
Nadprojektová havárie s přítomností nebezpečných látek mutagenních, karcinogenních	Řízení bezpečnosti založené na řízení integrální bezpečnosti je vyžadováno jen ve specifikovaných případech.	Ano	Ano	Ano	Ano	K
Zneužití látek CBRNE	Chybí účinný systém řízení nakládání s látkami CBRNE.	Ano	Ano	Ano	Ano	M
Zneužití nanotechnologií	Neřeší se.	Ano	Ano	Ano	Ano	M
Zneužití genetického inženýrství	Neřeší se.	Ano	Ano	Ano	Ano	M
Zneužití IT technologií	Neřeší se.	Ano	Ano	Ano	Ano	M

Na základě analýzy nástrojů EU pro řízení věcí veřejných je posouzena úroveň řízení pohrom spojených s technologiemi a infrastrukturami. Vysoce byla oceněna tvorba databáze MARS, která vytváří základnu pro tvorbu vysoce kvalifikovaných podkladů pro řízení bezpečnosti. Na základě šetření založeného na specifickém kontrolním seznamu jsou identifikovány základní nedostatky spojené s řízením sledovaných pohrom a jsou identifikovány oblasti, ve kterých je třeba přijmout opatření. Z výsledku vyplývá, že nedostatků je mnoho. Je to způsobeno tím, že v řízení chybí zacílení na prioritní problémy.

Nutné je, aby se řízení rizik a s ním spojené odpovědnosti skutečně zavedly do praxe (tak jak je např. v ČR uloženo zákonem č. 262/2006 Sb.) a byly integrální součástí všech procesů v organizaci, včetně strategického plánování a všech procesů spojených s řízením projektů a změn [13]. Je třeba upravit i požadavky na množství komodit, které skutečně zajistí přežití lidí, např. zabezpečení dodávek ropy a zemního plynu se upravuje na základě výpočtu přidané hodnoty projektu z hlediska krátkodobé a dlouhodobé odolnosti systému a zvýšení zbývající flexibility systému umožňující vyrovnat se s narušením dodávek podle různých scénářů a další kapacity získané v rámci projektu stanovené ve vztahu ke standardu pro infrastrukturu (pravidlo N-1). [14].

K tomu je však nezbytné kvalitní zázemí, které by měl připravit výzkum. Bez kvalitního zázemí budou řešeny jen momentální kritické situace, což obvykle vede k nerovnoměrnému čerpání zdrojů, sil a prostředků.

KONCEPT ŘEŠENÍ BEZPEČNOSTI TECHNOLOGICKÝCH SYSTÉMŮ TYPU SOS

Jak bylo řečeno výše, tak na světové konferenci ESREL 2014 [4] byla prezentována řada sdělení, která obsahovala výsledky aplikace přístupu obrana do hloubky (defence in depth), který byl na konci 80. let zaveden v jaderné energetice.

Na základě bezpečnostních návodů Mezinárodní atomové agentury [5] představuje ochrana do hloubky komplexní přístup, který zajišťuje, že lidé i životní prostředí budou ochráněny i při kritických podmínkách v objektu s jadernou technologií. Jde o komplexní filosofii bezpečnosti, která se začala aplikovat v 80. letech minulého století. Zahnuje všechny činnosti zacílené na bezpečnost při umísťování, navrhování, výrobě, konstrukci, uvedení do provozu, provozu a odstavení z provozu u jaderných elektráren. Pro zajištění bezpečného systému systémů používá systémy bariér a režimová opatření. Jejím cílem je:

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

Rozlišuje opatrení a činnosti usporiadané do päti úrovni. Cílem:

- prvú úroveň ochrany je prevencia abnormálneho provozu a selhání,
- druhú úroveň je řízení / ovládání abnormálního provozu a detekce selhání,
- třetí úroveň je řízení / ovládání havárií pomocí projektových opatření,
- čtvrté úroveň je řízení / ovládání kritických podmínek včetně prevence dalšího rozvoje havárie a zmírnění dopadů havárie,
- páté úroveň je zmírnění dopadů havárie vně objektu s jadernou technologií.

Základní prostředky pro:

- první úroveň jsou konzervativní návrh a vysoká kvalita konstrukce a provozu,
- druhou úroveň ovládací, omezovací a ochranné systémy a další typické znaky dohledu nad provozem,
- třetí úroveň naprojektované (inherentní) vlastnosti podporující bezpečnost,
- čtvrtou úroveň alternativní opatření a řízení havárie,
- a pátou úroveň vnější plány odezvy.

Ze současného poznání i z výše uvedených faktů vyplývá, že bezpečnost komplexních technologických celků typu systém systémů (SoS – soubor otevřených a vzájemně se prolínajících systémů uspořádaných tak, aby plnily určité úkoly v oblasti interoperability) závisí především na řízení integrálního rizika, a to hlavně dílčích rizik spojených s vazbami a toky v systému. Výběr vhodné strategie na zmírňování rizika je velmi komplexní a kritický úkol. Nejde jen o snížení pravděpodobnosti výskytu selhání, ale také o zlepšení podmínek strategie snižuje produktivitu a výnosnost technologického systému. Výběr strategie zmírňování rizika je typický multikriteriální rozhodovací problém. Nejlepší strategie se musí vybrat z možných alternativ. Musí být vzato v úvahu množství kritérií, z nichž některá jsou konfliktní [6].

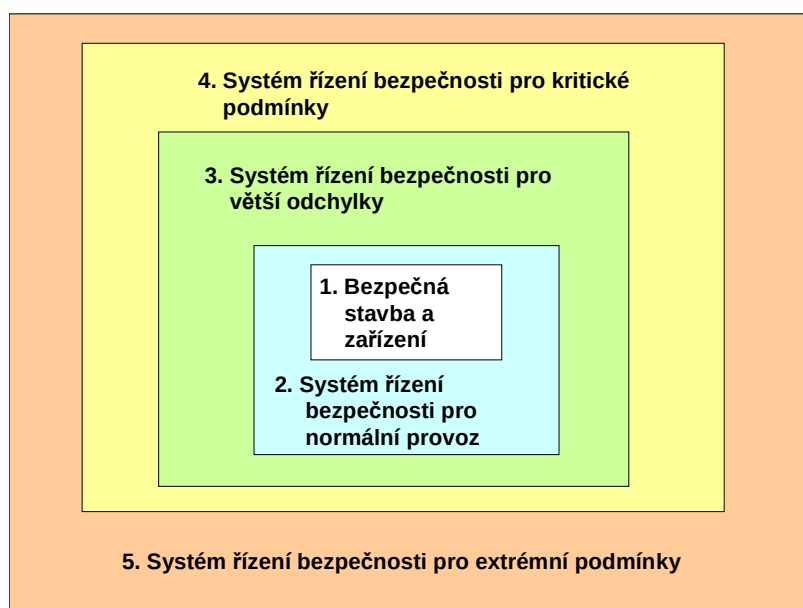
Heterogenita a těsné propojení systémů v technologických objektech a infrastrukturách je příčinou obtížného popisu a emergentního chování předmětných systémů [15, 16]. **Kvůli složitosti systémů systémů nemají klasické analytické metody schopnost poskytnout dostatečné informace o chování systému v prostoru a čase.** K získání dostatečných informací je třeba hluboké porozumění a holistický přístup [16].

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, která jsou největší hrozbou dnešní společnosti [17].

Modely řízení bezpečnosti složitých technologických systémů (objektů a infrastruktur), tj. systémů systémů jsou teprve v počátku. Podle znalostí předmětné modely musí mít inherentní charakteristiky jako dynamické nelineární chování, spleť 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 úrovní vyřešení úkolu.

PĚTISTUPŇOVÝ MODEL ŘÍZENÍ BEZPEČNOSTI KOMPLEXNÍHO TECHNOLOGICKÉHO SYSTÉMU

Na základě znalostí uvedených v pracích [4, 6, 15-19] a zkušeností z praxe, autorka *metodou analogie* odvodila základní principy pro řízení bezpečnosti technologických systémů (objektů a infrastruktur) typu systém systémů (obrázek 1) takto:



Obr. 1 - Pětistupňový systém řízení bezpečnosti technologického objektu.

1. V návrhu, výstavbe a konstrukci inherentne používať princípy bezpečného projektu (prístupy):
 - all hazard approach, proaktívny, systémový aplikujúci integrálny riziko, tj. i dĺžky rizika spojená s vazbami a toky hmotnými, energetickými, finančnými a informačnými v dĺžkach systémoch i naprieč nich,
 - správna práca s rizikami,
 - a monitoring, ve ktorom jsou zabudované korekčné opatrenia a činnosti).
2. Rídici systém objektu musí mať základné rídící funkcie, alarmy a reakcie operátora spracované tak, aby technologický objekt bol udržaný v normálnom (stabilnom) stave za normálnych podmienok.
3. Technologický objekt musí mať špeciálne rídící systémy orientované na bezpečnosť a ochranné bariéry, ktoré ho udržujú v bezpečnom stave i pri väčšej zmene provozních podmienok (tj. pri abnormálnych podmienkach) a zabráňujú vzniku nežiadúcich javov, čo znamená, že má dobrú resilienciu. Predmetné systémy udržujú bezpečný provoz i za zmeny podmienok alebo majú schopnosť zabezpečiť normálny provoz po aplikácii nápravných opatrení (vyčistenie, oprava...).
4. Pro prípad, že sa vyskytnú kritické podmienky, ktoré spôsobí, že dojde ke ztráte ovládání objektu, musí mať technologický objekt systém opatrení pro vnitřní nouzovou odezvu, zmírnění dopadů, a pro návrat do normálního provozu (plán kontinuity a vnitřní nouzový / havarijný plán).
5. Pro prípad, že dopady ztráty ovládání technologického systému postihnou okolí technologického objektu, musí mať technologický systém opatrení i pro vnější odezvu, zmírňující opatrení pro prevenci ztrát v objektu; a kapacitu pro překonání obtíží.

Pri rozlíšení miery bezpečnosti objektu a infraštruktúry sa používa bezpečnostná charakteristika, že objekt má jednoduššiu alebo až päťstupňovú ochranu do hĺbky. Jednotlivé systémy riadenia bezpečnosti zaisťujú aplikáciu technických, provozních a organizačních opatrení a činností, ktoré jsou navrhnené tak, aby buď zabránili iniciácii reťazce škodlivých javov, alebo ho zastavili [5,15,19].

Pro úspěšné zvládnutí rizik u technologických systémech je dle [19] třeba:

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

METODA ŘEŠENÍ KONFLIKTŮ PŘI ŘÍZENÍ BEZPEČNOSTI TECHNOLOGICKÝCH SYSTÉMŮ

Jak již bylo řečeno výše, technologické objekty a infrastruktury jsou otevřené systémy systémů, které jsou soubory vzájemně se prolínajících dílčích systémů, které hrají v naplňování uvedeného cíle důležitou roli, a zároveň při svých kritických stavech mohou základní cíl lidí vážně ohrožovat. Zkušenosti z praxe ukazují, že při jejich řízení vznikají konflikty zájmů. Nejčastěji se vyskytují konflikty při:

- rozhodování o alokaci zdrojů, sil a prostředků, a to buď na rozvoj aktiv a nebo na redukci existujících rizik; tj. konflikt asset management vs. risk management [20],
- řešení jejich kritických stavů, kdy se rozhoduje mezi šetrným zacházením s technologií a razantními opatřeními ve prospěch ochrany obyvatelstva [21].

Jelikož se nejedná o nic neobvyklého v lidské společnosti, vznikly celé teorie, jak řešit konflikty při řízení technologických systémů, např. [22-25]. Dle citovaných prací je třeba konflikty řešit konstruktivně tak, aby byly co nejvíce uspokojeny a dosaženy strategické cíle lidské společnosti (existence, bezpečí a rozvoj lidí). Proto je řízení konfliktů chápáno jako proces plánování, jak dosáhnout vzájemně výhodné řešení závažných problémů. Nástroj vyžaduje, aby se obě strany konfliktu předem dohodly na řešení očekávaných sporných problémů s ohledem na stanovené zájmy a cíle [26], kterými je v našem případě veřejný zájem, tj. zajištění bezpečí a rozvoje lidí, a to dnes i v budoucnosti [1].

Na základě pro-aktivního přístupu, který je vlastní projektovému a procesnímu řízení [1], se lze na řešení konfliktů předem připravit vypracováním plánu pro řízení rizik, který je odsouhlasen předpokládanými zúčastněnými stranami [21].

OCENĚNÍ SCHOPNOSTI ZVLÁDAT RIZIKA TECHNOLOGICKÝCH OBJEKTŮ

Úkolem řízení a vypořádání rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Snížování rizika je vždy spojeno se zvyšováním nákladů. Proto řízení rizika je vedeno snahou najít hranici, na kterou je únosné riziko ještě snížit, aby vynaložené náklady byly společensky přijatelné. Z pohledu praxe je třeba se dohodnout na tom, jaké požadavky bude výstup z hodnocení rizika splňovat. Při hodnocení rizik je nutné se snažit stanovené požadavky dodržovat a případné nedodržení odůvodnit. Jedná se především o splnění požadavků: provedení hodnocení v požadované šíři a kvalitě

v súlade s prijatou metodikou hodnotení; úplnosť hodnotení; zahrnutie najnovších poznatkov vedy; odhad nejistoty i neurčitosti v prípade použitia extrapolácie; jednotné vyjadrenie charakteristik rizika; a prístupnosť procesu hodnotenia rizika.

Dosaženie cieľa znamená dobre riadiť a správne rozhodovať, pričom dobré riadenie a správne rozhodovanie je možné len tehdy, keď máme dobré údaje a vieme využiť nástroje, ktoré máme k dispozícii [6]. *Poznámka:* najčastejšia chyba v českých pomeroch je podľa skúseností autorky fakt, že sa neprověřuje kvalita dátových súborů, vzájomný vzťah medzi presnosťou dát a citlivosťou metódy, a hodnotenie nerešpektujú systémovú podstatu objektů, tj. nezvažujú vliv vzťahů a toků.

Z vyššie uvedených faktů vyplývajú základné princípy pre prácu a riziká, a to:

- byť proaktívny,
- domýšľať možné dôsledky,
- správne určovať priority z pohľadu verejného zájmu,
- myslieť na zvládnutie neprijateľných dopadů,
- zvažovať synergie,
- a byť ostražitý,

čo zodpovedá filozofii prosazovanej v práci [28].

Proto pri stanovení rizika pre strategické rozhodovanie je nutno používať hierarchický multikritériálny postup. Recentné odborné práce používajú pojem hierarchické holografické modelovanie (HHM) [28]. Výsledky však sú vysoko kvalitné, pretože zohľadňujú radu faktorů, ktoré sú pôvodcami neurčitostí. Pretože ide o postup náročný na údaje a spracovateľské metódy, tak sa autorka domníva, že by Rada vlády pre bezpečnostný výskum mala dať prostriedky na predmetnú problematiku odborníkum, ktorí majú znalosti a schopnosti predmetné postupy do českej praxe zaviesť.

Snižovanie akéhokoľvek rizika je spojené so zvyšovaním nákladů, s nedostatkom znalostí, technických prostriedků, apod., a preto sa v praxi hľadajú hranice, na ktorých je únosné riziko znížiť tak, aby vynaložené náklady boli ešte rozumné. Táto miera rizika (určitá optimalizáciou) je väčšinou predmetom vrcholového riadenia a výsledkom politického rozhodovania, pri ktorom je z hľadiska zajišenia rozvoja nutné, aby sa využili súčasné vedecké a technické poznatky a zohľadnili ekonomické, sociálne a ďalšie podmienky.

S vnímaním rizika súvisí prijateľnosť rizika, ktorá musí mať sociálny rozměr. Je treba zvažovať:

- pre koho má byť riziko prijateľné?; pre pôvodcu rizika, pre politiky alebo pre verejnú správu?
- kto stanoví prijateľnosť?; politici rozhodujú o tom, čo je zákonné, a taktiež by nemali rozhodovať o tom, čo je prijateľné,
- či pri stanovení prijateľnosti riziká by sa diskutovala aktuálne tolerovateľná riziká, netolerovateľné prahové hodnoty a postoje verejnosti k rizikům.

Pri hodnotení prijateľnosti rizika sa jedná o porovnanie hodnoty / miery rizika zistených analýzou rizika sledovaného systému s meznou hodnotou prijateľnosti alebo stanovenou meznou funkciou prijateľnosti. Postoj jednotlivca k riziku závisí na vnímaní rizika a stresu, ktorý dané riziko spôsobí danému jednotlivcovi (úmrtie, zranenie, strata zamestnania aj.). Postoj spoločnosti k riziku závisí taktiež na celkovom vnímaní rizika, ďalej na averzii voči riziku, napr. jedna havária s vyšším počtom obeť v jednom prípade je menej prijateľná než vyšší počet havárií s jednotlivými obeťmi, a to preto, že celková suma obeť za určité obdobie je rovnaká. Spoločnosť akceptuje, keď určitá skupina ľudí je vystavená riziku, aby sa získali výhody pre iné skupiny ľudí. Roli hrá pomer medzi nákladmi na zvyšovanie bezpečnosti a počty zachránených životů, pozornosť médií apod. Prijateľnosť rizika závisí na sociálnych, ekonomických a politických faktorech a na vnímanom prospechu z činností, u ktorých prínosy sú podstatne vyššie než náklady na záchranné a likvidačné práce pri realizácii rizika.

Riziká by mali byť, ale neustále sa budú objavovať nové. Riadenie a vypořádanie rizika, ktoré spôsobujú pohromy, vyžaduje rozměr a meranie rizika, ktoré berú v úvahu nejen fyzické škody, obeť a ekvivalent ekonomických strát, ale i sociálne, organizačné a inštitucionálne faktory. Väčšina technik na určovanie rizika nereprezentuje holistický prístup a nerešpektuje, že riziko je rozdelené na lokálne, regionálne i štátne úrovne.

Je zjavné, že nejsme-li schopni riziko identifikovať a analyzovať, nejsme schopni sa proti nemu účinne brániť. Chyba, ktorú sa dopustíme pri identifikácii, analýze a hodnotení rizika, sa prenáša do nouzových a krízových plánů, do plánů kontinuity a snižuje jej hodnotu vo vzťahu k plánovaným opatreniam smerujúcim predovšetkým k ochrane ľudských životů a zdravia, ale i v oblasti akceschopnosti záchranných súložek podieľajúcich sa na realizácii záchranných operácií.

Z výsledků výskumu [28], ktorý sa zaoberal hodnotením miery kritičnosti konceptů súčasného riadenia a vypořádania rizik objektů, chápaných ako určité typy systémů vyplýva, že žiadny z dnes používaných konceptů pre riadenie a vypořádanie rizik nemá zanedbateľnú mieru kritičnosti, obrázok 2; tj. miera kritičnosti pri aplikácii:

- klasického konceptu riadenia a inžinierskeho vypořádania rizik je extrémne vysoká,
- konceptu riadenia a inžinierskeho vypořádania rizik zvažujúciho ľudský faktor, je veľmi vysoká,
- konceptu riadenia a inžinierskeho vypořádania rizik zameraného na zabezpečený systém je vysoká,
- konceptu riadenia a inžinierskeho vypořádania rizik zameraného na bezpečný systém je stredná,
- konceptu riadenia a inžinierskeho vypořádania rizik zameraného na bezpečný systém systémů je nízka.

KONCEPT	MÍRA KRITIČNOSTI				
1	■	■	■	■	■
2	■	■	■	■	■
3	■	■	■	■	■
4	■	■	■	■	■
5	■	■	■	■	■
STUPNICE	1	2	3	4	5

Obr. 2 - Míry kritičnosti konceptů pro řízení a vypořádání rizik:
 1 – klasický koncept řízení a inženýrského vypořádání rizik;
 2 - koncept řízení a inženýrského vypořádání rizik zvažující lidský faktor;
 3 – koncept řízení a inženýrského vypořádání rizik zaměřený na zabezpečený systém;
 4 - koncept řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém;
 a koncept řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém systémů [28].

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

ZÁVĚR

Z výše uvedeného vyplývá, že pro život lidí v současném světě potřebujeme technologické celky i infrastruktury. Z důvodu ochrany lidí však musíme řádně řídit a vypořádávat rizika, která jsou s nimi spojená. Nezbyvá nic jiného, než vyslovit souhlas s panem Fawcettem, který v práci [29] uvedl velkou moudrost „Vědět znamená přežít, ignorovat znamená říkat si o zničení“. Z ní vyplývá, že ignorování či podceňování řízení a vypořádání rizik, je důvodem většiny problémů, nezdarů, katastrof. Pro bezpečí a rozvoj lidí je proto důležité mít vždy předem připravené nástroje: jak zvládnout očekávaná rizika, k čemuž slouží plán řízení rizik; a co udělat v případě neočekávaných rizik, k čemuž slouží plány pro zvládnutí nečekaných situací (contingency plans).

Pro zlepšení práce s riziky sdělení obsahuje:

- výsledky posouzení úrovně řízení havárií spojených s technologiemi a infrastrukturami,
- návrh oblastí řešení identifikovaných nedostatků, které byly zjištěny při posuzování úrovně řízení havárií,
- koncept řešení bezpečnosti technologických systémů typu SoS,
- metodu řešení konfliktů při řízení bezpečnosti technologických systémů,
- výsledky ocenění schopnosti zvládat rizika technologických objektů.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] PROCHÁZKOVÁ, D., 2011: Strategické řízení bezpečnosti území a organizace. Praha: ČVUT, ISBN 978-80-01-04844-3, 483p.
- [2] OECD, 2002: Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response. Paris: OECD, 191p.
- [3] PROCHÁZKOVÁ, D., BUMBA, J., SLUKA, V., ŠESTÁK, B. (2008): Nebezpečné chemické látky a chemické přípravky a průmyslové nehody. Praha: PA ČR, ISBN 978-80-7251-275-1, 420p.
- [4] T. NOWAKOWSKI ET AL. (eds), 2015: Safety and Reliability: Methodology and Application. London: Taylor & Francis Group, ISBN 978-1-138-02681-0, 2453p.
- [5] IAEA, 2005: Assessment of defence in depth for nuclear power plants. Safety report series No. 46. Vienna: IAEA, ISBN: 92-0-114004-5, 119p.
- [6] PROCHÁZKOVÁ, D., 2011: Analýza a řízení rizik. Praha: ČVUT, ISBN 978-80-01-04841-2, 405p.
- [7] ELLUL, J., 1980: The Technological System. New York: The Continuum Publishing Corpor., ISBN 0-8264-9007-4.
- [8] PROCHÁZKOVÁ, D., 2014: Challenges to future disasters management. Saarbruecken: Lambert Academic Publishing, ISBN

- 978-3-659-53926-8, 170p.
- [9] EU: <http://eur-lex.europa.eu>
- [10] PROCHÁZKOVÁ, D., 2011: Questionnaire for special investigation. Brussels: EU. www.focus.eu
- [11] PROCHÁZKOVÁ, D., 2012: TopSafe 2012. Zpravodaj ČNS. Praha, www.csvts.cz/cns
- [12] PROCHÁZKOVÁ, D., 2007: Metodika pro odhad nákladů na obnovu majetku v územích postižených živelní nebo jinou pohromou. Ostrava: SPBI SPEKTRUM XI, ISBN 978-80-86634-98-2, 251p.
- [13] ISO, 2009: Management rizik – Principy a směrnice. ISO 31000.
- [14] EU, 2006: Návrh nařízení Evropského parlamentu a Rady o hlavních směrech transevropské energetické infrastruktury a o zrušení rozhodnutí č. 1364/2006/ES. COM/2011/0658.
- [15] SEVCIK, A., GUDMESTADO, T., 2015: Solutions and safety barriers: The holistic approach to risk-reducing measures. In: Safety and Reliability: Methodology and Application. London: Taylor & Francis Group, ISBN 978-1-138-02681-0.
- [16] PROCHÁZKOVÁ, D., 2012: Bezpečnost kritické infrastruktury. Praha: ČVUT, ISBN: 978-80-01-05103-0, 318p.
- [17] PROCHÁZKOVÁ, D., 2013: Základy řízení bezpečnosti kritické infrastruktury. Praha: ČVUT, ISBN 978-80-01-05245-7, 223p.
- [18] PROCHÁZKOVÁ, D., 2014: Challenges connected with critical infrastructure safety. Saarbrücken: Lambert Academic Publishing, ISBN 978-3-659-54930-4, 218p.
- [19] VATN, J., 2015: Structuring contributors to successful operation. In: Safety and Reliability: Methodology and Application. London: Taylor & Francis Group, ISBN 978-1-138-02681-0.
- [20] US National Bank, 2012: Asset management. Conflicts of interest. controller's handbook. AM-CInt, 95p.
- [21] PROCHÁZKOVÁ, D., 2014: Plány pro řízení rizik jsou též nástroje podporující optimální řešení konfliktů u kritických objektů. In: Fire Safety 2014. Ostrava: SPBI, ISBN: 978-80-7385-149-1.
- [22] BRIEF, A. P. AT ALL, 2005: Community Matters: Realistic Group Conflict Theory and the Impact of Diversity. Academy of Management Journal, 48(2005), 5 830-844.
- [23] LULOFS, R. S., CAHN, D. D., 2000: Conflict: From Theory to Action. Needham Heights, MA: Allyn & Bacon.
- [24] PUTNAM, L. L., POOLE, M.S., 1987: Conflict and Negotiation. In F. M. Jablin, L. L. Putnam, K. H. Roberts & L. W. Porter (Eds.), Handbook of Organizational Communication (pp. 549-599). Newbury Park: Sage.
- [25] MORTON DEUTSCH, A., 1987: A Theoretical Perspective on Conflict and Conflict Resolution, 48. In: Dennis J.D. Sandole & Ingrid Sandole-Staroste, eds., Conflict Management and Problem Solving (New York University Press).
- [26] ČAKRT, M., 2000: Konflikty v řízení a řízení konfliktů. Praha: Management press, ISBN 80-85943-81-6, 182 p.
- [27] HAIMES, Y.Y., 2009: Risk Modeling, Assessment, and Management. John Wiley & Sons, ISBN 978-0-470-28237-3. 1040p.
- [28] PROCHÁZKOVÁ, D., 2014: Optimum Concept of Management and Trade-off with Risks. In: Safety and Reliability: Methodology and Application. CD ROM. London: CRC Press 2014 (kniha - London: Taylor & Francis Group 2015), ISBN 978-1-138-02681-0. pp 1463-1471.
- [29] FAWCETT, H. H., 1984: Hazardous and Toxic Materials. Safe Handling and Disposal. New York: Willey .

ADRESA AUTORA:

Dana PROCHÁZKOVÁ, doc., RNDr., PhD., DrSc., Department of Security Technologies and Engineering, Czech Technical University in Prague, Konviktska 20, 110 00 Praha 1, CZECH REPUBLIC, 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.