Nástroje environmentálnej politiky ♦ Environmental policy tools ´2016

Zborník zo VI. medzinárodnej vedeckej konferencie, 17. jún 2016, Bratislava
Proceedings of the 6th International Conference, Bratislava, June 17, 2016
■ Žilina: Strix. Edícia ESE-29, ISBN 978-80-89753-12-3 ■ Rusko, M. [Ed.] ■

DOPADY NEBEZPEČNÝCH LÁTEK A OCHRANA LIDÍ ZAJIŠTĚNÁ INTEGRÁLNÍ BEZPEČNOSTÍ TECHNOLOGICKÝCH KOMPLEXŮ

Dana PROCHÁZKOVÁ

IMPACTS OF HAZARDOUS SUBSTANCES AND HUMAN PROTECTION PROCURED BY INTEGRAL SAFETY OF TECHNOLOGICAL COMPLEXES

ENVIRONMENTAL POLICY TOOLS ´2016

ABSTRAKT
KOMPLEXNÍ TECHNOLOGICKÉ SYSTÉMY, TJ. OBJEKTY A INFRASTRUKTURY, ZLEPŠUJÍ JEDNAK KVALITU ŽIVOTA LIDÍ A JEDNAK ŽIVOTY LIDÍ OHROŽUJÍ, KDYŽ V NICH DOJDE K NEŽÁDOUCÍM PROCESŮM A JEVŮM, A TO ZVLÁŠTĚ KDYŽ JSOU PŘÍTOMNÉ NEBEZPEČNÉ LÁTKY. PROTO SE VYŽADUJE BEZPEČNÝ PROVOZ TĚCHTO SYSTÉMŮ, A PRO PŘÍPAD JEJICH SELHÁNÍ SPECIFICKÁ OPATŘENÍ PRO OCHRANU LIDÍ PŘED DOPADY NEBEZPEČNÝCH LÁTEK. PRÁCE PRO KOMPLEXNÍ TECHNOLOGICKÉ SYSTÉMY OBSAHUJE VÝSLEDKY VÝZKUMU, A TO: POŽADAVKY PRO JEJICH BEZPEČNOST; KONCEPT PRO ZAJIŠTĚNÍ JEJICH BEZPEČNOSTI ZALOŽENÝ NA PĚTISTUPŇOVÉM MODELU; A PROCESNÍ MODEL PRO ŘÍZENÍ JEJICH BEZPEČNOSTI V ČASE PŘI PROVOZU.

Klíčová slova: *komplexní technologické systémy; systémy systémů; bezpečnost; riziko; řízení rizik; koncept zajištění bezpečnosti; pětistupňový model pro zajištění bezpečnosti; model pro řízení bezpečnosti v čase.*

ABSTRACT
THE COMPLEX TECHNOLOGICAL SYSTEMS, I.E. FACILITIES AND INFRASTRUCTURES, IMPROVE ON THE ONE HAND QUALITY OF HUMAN LIVES AN ON THE OTHER HAND THEY THREATEN THE HUMAN LIVES WHEN INSIDE THE UNACCEPTABLE PROCESSES AND PHENOMENA OCCUR, NAMELY WHEN HAZARDOUS SUBSTANCES ARE PRESENT. THEREFORE, IT IS REQUIRED SAFE OPERATION OF THESE SYSTEMS AND FOR THE CASE OF THEIR FAILURE THE SPECIFIC MEASURES FOR HUMAN PROTECTION AGAINST IMPACTS OF HAZARDOUS SUBSTANCES. THE WORK FOR COMPLEX TECHNOLOGICAL SYSTEMS CONTAINS THE RESULTS OF RESEARCH, NAMELY: DEMANDS FOR THEIR SAFETY; CONCEPT FOR ENSURING THEIR SAFETY BASED ON FIVE STEPS MODEL; AND THE PROCESS MODEL FOR MANAGEMENT OF THEIR SAFETY IN TIME AT OPERATION.

Key words: *complex technological systems; system of systems; safety; risk; risk management; concept of ensuring the safety; five steps model for ensuring the safety; model for management of safety in time.*

1. Úvod

Technologické systémy tvoří objekty a infrastruktury, které jsou v mnoha případech vybavené technologiemi, které pracují s nebezpečnými látkami. Předmětné systémy 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.

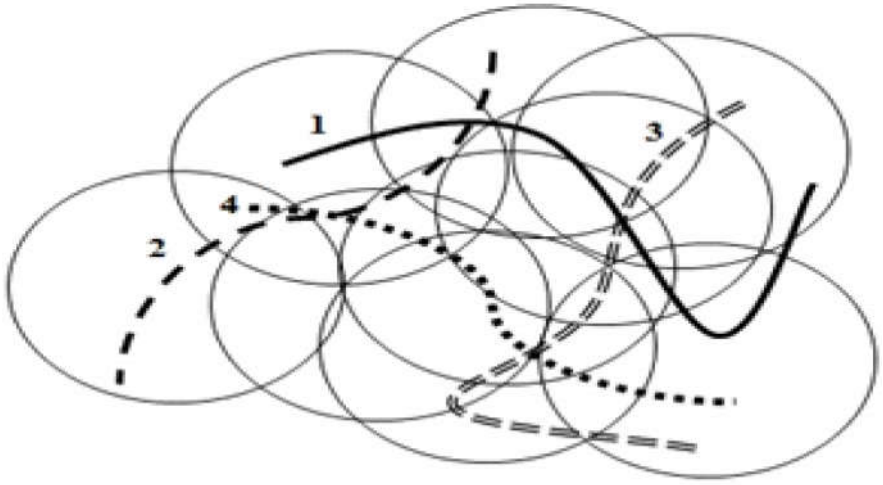
Zborník zo VI. medzinárodnej vedeckej konferencie, 17. jún 2016, Bratislava
Proceedings of the 6th International Conference, Bratislava, June 17, 2016
■ Žilina: Strix. Edícia ESE-29, ISBN 978-80-89753-12-3 ■ Rusko, M. [Ed.] ■

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 vytvořené [1-3]. To znamená, že každý technologický systém zahrnuje technické prostředky, technické postupy, člověka, znalosti a dovednosti vytvářet cíleně nové výrobky, tj. jeho modelem je systém systémů (tj. soubor vzájemně se prolínajících systémů, které mají povahu technickou, sociální, organizační, územní a kybernetickou) [1,4-6], ve kterém probíhají různé procesy, a to výrobní, administrativní, vzdělávací, transportní, dodavatelské, finanční, informační a organizační, obrázek 1. De facto se jedná o sociotechnologické systémy [7].

Cílem řízení systému systémů je zajistit, aby všechny procesy, které v něm probíhají byly žádoucí a vedly k zajištění existence a rozvoje, což znamená, že nežádoucím procesům musí být zabráněno nebo musí být včas zastaveny, aby nezpůsobily poškození až degradaci celku. Vazby v systému jsou jak povahy technické „stroj-stroj“, tak povahy smíšené „člověk-stroj“ a v posledních letech se odlišují vazby „člověk-PC" a „stroj-PC“. Toky v systému jsou energetické, materiálové, informační, finanční a instrukční,

2. Charakteristika technologických systémů

V současné době se pro řešení problémů praxe ve sledované oblasti již nevystačí s jednotlivými systémy, ale se soubory systémů. Podle typu organizovanosti soubory systémů dle [4] rozdělujeme následovně: jednoduše organizované celky (např. stroje); složené systémy vyznačující se složitou organizovaností (např. složené komplexy strojů, které dohromady provádí úkony v daném pořadí a zajišťují určité výrobky, např. propojené výrobní linky s různými technologiemi); složité (komplexní) systémy vyznačující se neorganizovanou složitostí a složených tak, aby plnily jisté funkce (např. automatické systémy pro výrobu, rozdělení a distribuci jistých komodit); a systémy systémů (např. lidské tělo, životní prostředí, systémy pro výrobu, distribuci a spotřebu elektřiny, plynu apod.).



Obr. 1 - Schéma technologického systému pomocí modelu systém systémů a vyznačení procesů, které v něm probíhají.

Pro charakteristiku a řízení jednoduše organizovaných celků se používají výsledky analytických řešení. Pro charakteristiku a řízení složených systémů (v praxi je též používán název soustava), které se chápou jako reprezentace prvků, které jsou určitým způsobem uspořádané a propojené a díky vlastní struktuře plní určité funkce, se používají výsledky statistických řešení založených na analytických funkcích, jejichž parametry jsou proměnné v určitém intervalu, což je odrazem různých možných stavů / variant chování systémů. Pro charakteristiku a řízení komplexních systémů i systémů systémů se používají výsledky simulací, protože dané útvary mají mnoho komponent (často též systémů), které spolu interagují a jsou uspořádané v několika úrovních, což způsobuje, že pozorujeme: náhle vynořené rysy chování, které nelze získat ze znalostí o chování komponent,

jde o tzv. emergenci; hierarchičnost; samo organizovanost; a rozmanité řídící struktury, což vše dohromady připomíná chaos. Při sledování je tudíž nutný mnoho oborový a mezioborový přístup. Pro řízení předmětných systémů je pak nutné používat multikriteriální přístupy [4].

Systém systémů (SoS – System of Systems nebo v americké angličtině Systems System) je systém, který se skládá z několika systémů různé povahy a různého umístění, které jsou vzájemně provázané k tomu, aby zajistily jisté operace a činnosti. Jedná se o specifické uspořádání několika systémů [4,5]. Je třeba si uvědomit, že při sledování chování SoS pro potřeby řešení jedněch úkolů se musíme zabývat velmi podrobným dělením systémů v několika úrovních a při jiných postačí jen dělení v nejvyšší úrovni (úrovně regionální, obecní, místní atd.). Vzájemná provázanost systémů pochopitelně působí závislost (interdependences). Proto pochopitelně neplatí, že bezpečnost SoS je agregací bezpečnosti dílčích systémů, protože se musí respektovat i průřezová rizika způsobená vazbami a toky napříč SoS a s okolím. Uvedená skutečnost znamená, že integrovaná bezpečnost, která je založená na řízení integrovaného rizika není zcela na místě, a musí být postupně nahrazována integrální bezpečností, při které se spoléhá i na řízení průřezových rizik.

3. Problémy složitých technologických systémů

Technologické systémy jsou otevřené systémy systémů, které plní určité funkce za podmínek interoperability. Za jiných podmínek vznikají konflikty, protože každý systém má svůj vlastní cíl. Propojení mezi provázanými systémy vedou k existenci vzájemných závislostí (interdependences), které musí být zohledněny při všech fázích řízení bezpečnosti technologických systémů. Cílem jejich řízení je zajistit bezpečí a rozvoj lidí v předmětných objektech i v jejich okolí za podmínek normálních, abnormálních i kritických.

Z důvodu existence závislostí dochází při selhání technologických systémů (objektů i infrastruktur) ke kaskádovitým jevům, které jsou z hlediska cílů lidí i vlastníků systémů samotných nežádoucí. Obrana proti vzniku nežádoucích jevů spočívá v tom, že se provádí opatření a činnosti, které zabrání vzniku takových jevů, a když přesto vzniknou, tak zabrání vhodnými opatřeními a činnostmi jejich šíření. *Zabránit kaskádovitým jevům je možné jen aplikací sofistikovaných opatření v řízení, které na základě znalostí nejprve rozpozná možné situace, připustí existenci průřezových rizik a konfliktů mezi zúčastněnými, a připraví vhodná řešení a jejich zázemí.* V předmětné oblasti je při řízení sledována veličina kritičnost.

KRITIČNOST označuje určitou prahovou hodnotu pro sledovaný systém či SoS, která označuje, že jsou-li hodnoty pod tímto prahem, tak je stav žádoucí (podkritický) a opačně. V praxi [4,6] rozlišujeme dva typy kritických položek, a to:

- položky, které pouze způsobují eskalaci dopadů pohrom, buď všech, nebo jen některých, které jsou možné v daném místě,
- položky, které zaručují bezpečnost systému, tj. funkčnost a rozvoj chráněných aktiv. Jejich selhání způsobená nějakou pohromou nebo provozními aspekty vedou k závažným dopadům na chráněná aktiva. Proto se u nich používají principy jako: nemůžeš-li provést úkol v požadované kvalitě, neprováděj ho; a selži bezpečně .

U prvního typu se při obnově provádí zodolnění položky vůči pohromám, které v daném případě vyvolaly nebo mohou vyvolat nepřijatelné dopady. Provádění jejich obnovy nemá žádnou prioritu z pohledu funkčnosti území / objektu / státu apod.

U druhého typu se již v územním plánování, projektování, výstavbě i provozování provádí opatření, která vedou ke zvýšení jejich technické spolehlivosti. Používají se různá opatření i zálohování činností jinými položkami, která vedou k vyšší odolnosti vůči možným pohromám. Proto při obnově je třeba provést opatření jak v oblasti zálohování, tak v oblasti zodolnění. Protože předmětné položky jsou životadárné pro území / objekt / infrastrukturu / stát apod., existují priority v obnově, přičemž je třeba, aby veřejný zájem byl upřednostněn před soukromými zájmy.

Při hodnocení kritičnosti složitých technologických systémů, tj. objektů i infrastruktur se dle [4,6] používají otázky:

- Jak objekt či infrastruktura reaguje na určité typy pohrom?
- Jak je objekt či infrastruktura masivní, odolná a pružná?
- Jak se chování objektu či infrastruktury může zlepšit?
- Jaké jsou vhodné mechanizmy řízení bezpečnosti?
- Jaká pravidla se mohou využít pro samoregulaci nebo pro přípustné odchylky?
- Které části objektu či infrastruktury jsou kritické?

Jelikož kritické objekty jsou často vybaveny drahou technologií, dochází při odezvě na nouzové situace často ke konfliktu mezi provozními inženýry a bezpečnostními složkami zacílenými na ochranu lidí, protože inženýři jsou vzdělávání i cvičení ke zvládání normálních, abnormálních i kritických podmínek a k respektování ochrany technologií, protože provoz technologií jim poskytuje práci, tj. i obživu. Podle současných znalostí se připravují předem plány pro řízení očekávaných rizik, ve kterých se stanovuje postup řešení očekávaných konfliktů [8].

4. ŘEŠENÍ PROBLÉMŮ TECHNOLOGICKÝCH SYSTÉMŮ

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 [1,5]. Jak již bylo řečeno, tak rozvoj technologií směřuje stále více ke kombinaci jednotlivých zařízení a aplikací do komplexních (složitých) systémů s cílem dosáhnout zvýšení výroby a vysoké ziskovosti. Vytvářené systémy nejsou výsledkem expertů z jedné disciplíny (oboru), nýbrž jsou výsledkem interdisciplinárního týmu. Zvláště pro síťové technologie platí, že jednotlivý expert není schopen kompletně posoudit a ovládat velké technické systémy, a proto je nutná spolupráce expertů z řady disciplín, která vyžaduje vzájemné pochopení cílů a schopnost hledání konsensu [9-12]. Z hlediska potřeby zajistit bezpečí a udržitelný rozvoj lidské společnosti je předpokladem pro konstrukci předmětných komplexů ovládání jejich bezpečnosti [13].

Je logické, že v komplexních systémech bezpečnostní funkce musí být zvažovány v souvislostech s ostatními funkcemi systému a jeho podsystémů. Tj. nestačí řešit jednotlivosti (tj. problémy bezpečnosti uvnitř jednotlivých podsystémů), ale je třeba řešit zároveň bezpečnost celku i bezpečnost jednotlivostí (tj. dílčích podsystémů) [1]. Přitom je třeba počítat s dále uvedenými ohroženími:

- vnější ohrožení (ohrožení od jevů v okolí systému),
- vnitřní ohrožení (ohrožení od vnitřních zařízení jednotlivých podsystémů),
- funkční ohrožení (ohrožení spojená se selháním funkcí celého systému nebo zařízení či komponent systému, tj. selháním podsystémů),
- ohrožení spojená s montáží,
- lidská ohrožení (ohrožení spojená s lidskými činnostmi).

Je skutečností, že bezpečnost jednotlivých technologických sektorů závisí na bezpečnostních tradicích, které se vyvíjely určitou dobu v daném sektoru. Proto v celku složeném z několika sektorů jsou provedená bezpečnostní opatření různorodá a odpovídají znalostem a zkušenostem doby, ve které byly vytvořeny. Dodnes je skutečností, že při sestavování technologických systémů a při vytváření jejich bezpečnosti experti z různých oborů pracují odděleně, což nezaručuje ani optimální bezpečnost, ani optimální náklady. Často se stává, že jednotlivé podsystémy jsou bezpečné, protože pro ně existují standardy a normy (např. jednotlivé technické části určitého provozu), ale bezpečnost celku, který vznikl jejich propojením s kybernetickými a jinými infrastrukturami již sledovaná není, protože se hodnocení a prokázání bezpečnosti nepožaduje relevantní legislativou a navíc k danému účelu není dosud k dispozici relevantní odborný postup. Výsledkem jsou např. tzv. organizační havárie [14]. Jelikož v posledních letech došlo k velkým selhání energetických infrastruktur [1], která tíživě dolehla na lidi ve vyspělých zemích, EU soustředila své úsilí v oblasti výzkumu na pochopení vnitřních závislostí mezi podsystémy s cílem stanovit zásady pro zajištění bezpečnosti systému složeného z historicky vytvořených systémů, jejichž bezpečnost byla zajištěna tradičními přístupy, viz úkoly rámcového programu EU HORIZON2020.

Bezpečnost je závislá na úrovni vyjednávání s riziky. Komplexní / integrální bezpečnost je spojená s vyjednáváním s integrálním rizikem, tj. ne s dílčími riziky (zaměřenými na jednotlivá chráněná aktiva) [1,6]. Je skutečností, že snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí a s nedostatkem technických prostředků, apod. Proto se v praxi hledá hranice, na kterou je únosné riziko snížit tak, aby vynaložené náklady byly ještě rozumné (viz principy ALARP, ALARA aj.). Uvedená míra snížení rizika (určitá optimalizace) je většinou předmětem vrcholového řízení a politického rozhodování, při kterém se využívají současné vědecké a technické poznatky a zohledňují se ekonomické, sociální a další podmínky [6].

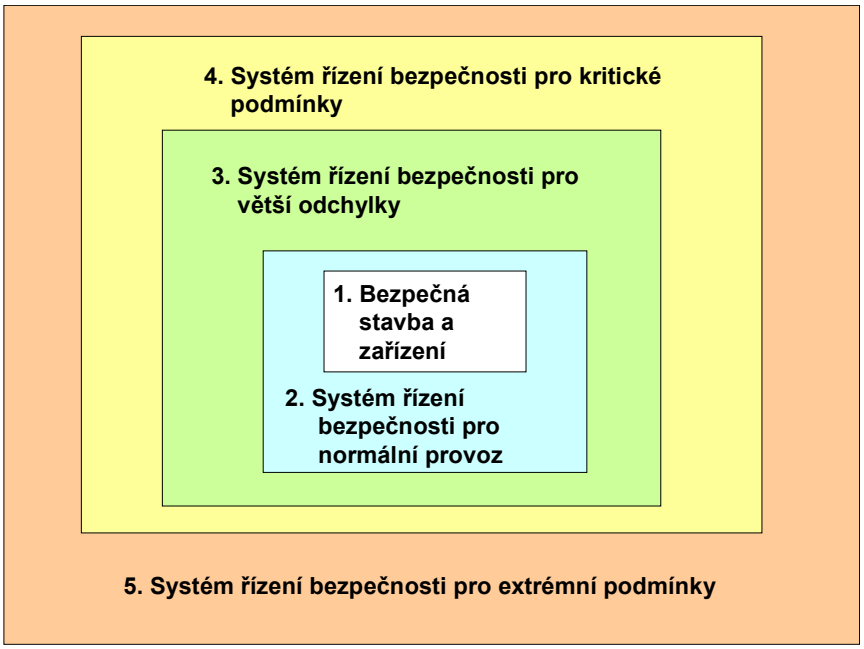
5. Koncept bezpečnosti technologických systémů

Na světové konferenci ESREL 2014 [15] 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 [16], 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].
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 2) takto:



Obr. 2 - Pětistupňový systém řízení bezpečnosti technologického objektu.

1. V návrhu, výstavbě a konstrukci inherentně používat principy bezpečného projektu (přístupy:
   - all hazard approach, proaktivní, systémový aplikující integrální riziko, tj. i dílčí rizika spojená s vazbami a toky hmotnými, energetickými, finančními a informačními v dílčích systémech i napříč nich,
   - správná práce s riziky,
   - a monitoring, ve kterém jsou zabudovány korekční opatření a činnosti).
2. Řídicí systém objektu musí mít základní řídicí funkce, alarmy a reakce operátora zpracované tak, aby technologický objekt byl udržen v normálním (stabilním) stavu za normálních podmínek.
3. Technologický objekt musí mít speciální řídicí systémy orientované na bezpečnost a ochranné bariéry, které ho udržují v bezpečném stavu i při větší změně provozních podmínek (tj. při abnormálních podmínkách) a zabraňují vzniku nežádoucích jevů, což znamená, že má dobrou resilienci. Předmětné systémy udržují bezpečný provoz i za změny podmínek nebo mají schopnost zajistit normální provoz po aplikaci nápravných opatření (vyčištění, oprava…).
4. Pro případ, že se vyskytnou kritické podmínky, které způsobí, že dojde ke ztrátě ovládání objektu, musí mít technologický objekt systém opatření pro vnitřní nouzovou odezvu, zmírnění dopadů, a pro návrat do normálního provozu (plán kontinuity a vnitřní nouzový / havarijní plán).
5. Pro případ, že dopady ztráty ovládání technologického systému postihnou okolí technologického objektu, musí mít technologický systém opatření i pro vnější odezvu, zmírňující opatření pro prevenci ztrát v objektu; a kapacitu pro překonání obtíží.

Při rozlišení míry bezpečnosti objektů a infrastruktur se používá bezpečnostní charakteristika, že objekt má jednostupňovou nebo až pětistupňovou ochranu do hloubky. Jednotlivé systémy řízení bezpečnosti zajišťují aplikaci technických, provozních a organizačních opatření a činnosti, které jsou navrženy tak, aby buď zabránily iniciaci řetězce škodlivých jevů, anebo ho zastavily [16,17,19].

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

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

6. Způsob řízení technologických systémů zacílený na bezpečnost

Ohranu lidí před nebezpečnými látkami spojenými s technologickými systémy zajistí pouze aplikace kvalitního řízení jejich provozu. založené na ***řízení bezpečnosti*** [5]. Účelem a cílem řízení rizik je jejich snížení na přijatelnou úroveň. Jakmile na základě stanovení ohrožení je nebezpečí jednou identifikováno, musí být nejvyšší prioritou jeho eliminace, anebo jeho spolehlivé řízení.

Systém řízení bezpečnosti (SMS – Safety Management System - někdy též systémové řízení bezpečnosti nebo jen krátce systémová bezpečnost) má cíl zvyšovat bezpečnost a provádí to také na základě snižování rizik na úroveň přijatelného rizika. Má široko akceptované priority jak zvládnout nebezpečí, kterými jsou:

- Eliminovat zdroje nebezpečí.
- Redukovat (omezit) možné dopady, tj. možná nebezpečí pro chráněná aktiva.
- Zvládnout rizika.
- Lokalizovat a zmírňovat škody.

Uvedené priority neznamenají, že stačí, aby byla jen jedna z nich aplikovaná při projektu zaměřeném na zvyšování bezpečnosti, nebo že jen nejvyšší priorita je nejžádanější. Pokud není možné kompletně eliminovat zdroj rizika, je dalším nejlepším výběrem ochrana před dopady spojenými s realizací rizika (tj. zmírňování dopadů pomocí specifických opatření), a to minimalizováním vzniku realizace rizika tak, že se příslušná bezpečnostní ochranná opatření (bezpečnostní systémy – Safety Systems) přímo zabudují jak do projektu zařízení, tak i do podmínek provozu projektovaného zařízení, tj. zajišťují bezpečnost. Dalšími v akceptovatelném pořádku priorit jsou zařízení na zvládnutí nebezpečí a na zmírnění jejich dopadů (systémy spojené s bezpečností – Safety Related Systems), které mají jen ochranné funkce. Jsou to např. pojistné ventily, které chrání před nedovoleným přetlakem v případech, ve kterých se nedovolenému zvýšenému tlaku v zařízení nedá úplně zabránit.

Bezpečnostní systémy jsou konstruované jako pasivní anebo aktivní. Nejefektivnějšími bezpečnostními zařízeními jsou zařízení pasivní, která fungují na bázi fyzikálních principů (např. gravitace) a pro uvedení do činnosti nepotřebují žádný přidaný impuls. Příkladem pasivního bezpečnostního systému je železniční semafor, jehož rameno automaticky spadne do polohy „stop“ vždy, když se přeruší ovládací proud v přívodním kabelu.

Aktivní bezpečnostní zařízení / systémy jsou méně vhodné, protože pro jejich aktivaci pro zabránění havárie anebo zmírnění jejich dopadů jsou potřebné zvláštní iniciační impulsy. Jejich vytvoření zahrnuje detekci nebezpečí a rozpoznání odpovídající bezpečnostní procedury. Příkladem aktivního bezpečnostního systému může být detektor kouře propojený se sprchovým systémem. Současné technické poznání dovoluje používat hybridní bezpečnostní systémy, které se samostatně vypínají, když podmínky nejsou v rozsahu podmínek stanovených pro provoz aktivních systémů.

Systém řízení bezpečnosti musí být vždy vybaven opatřeními pro minimalizování škod v případech, že bezpečnostní opatření a bezpečnostní systémy selžou, anebo se vyskytne neidentifikované nebezpečí. Minimalizování škod může mít podobu varovné a výstražné signalizace, výcviku, pokynů a procedur pro chování v nebezpečných situacích, anebo izolace nebezpečných zařízení od osídlených center. Opatření před nehodami včetně nouzového plánování musí být vypracováno ještě před tím, než bude zařízení spuštěno do provozu. Při vzniku havárie by už na to nemuselo být dosti

času.

Správné porozumění určité problémové oblasti vyžaduje pochopení její historie, vědeckého základu, kulturního a sociálního prostředí, ve kterém byla vyvinutá a ve kterém se využívá. Systém řízení bezpečnosti má svoje kořeny v inženýrství průmyslové bezpečnosti, která se datuje už od 19. století. Relativně nová disciplína zabývající se systémem řízení bezpečnosti (v inženýrském slangu systémovou bezpečností) je odpovědí na podmínky, které vznikly po 2. světové válce, když se vyvinuly její "rodičovské" disciplíny, a to systémové inženýrství a systémová analýza, které se vyvinuly pro řešení nových a komplexních inženýrských problémů. Vědecká báze všech těchto nových proudů inženýrství spočívá v teorii systémů, jejíž vývoj začal v třicátých letech minulého století.

7. Koncept řízení bezpečnosti v čase

Na základě současného poznání, shrnutého v pracích [1,2,4-6,20], systém řízení bezpečnosti (tzv. SMS – Safety Management System) komplexního objektu je postaven na zásadách procesního řízení a zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v území. Zpravidla se týká řady otázek, kromě jiného i organizace, pracovníků, identifikace a hodnocení ohrožení a z nich plynoucích rizik, řízení chodu organizace, řízení změn v organizaci, nouzového a krizového plánování, monitorování bezpečnosti, auditů a přezkoumávání [1,20]. Skládá se z šesti procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií. Uvedené procesy se dále dělí na podprocesy.

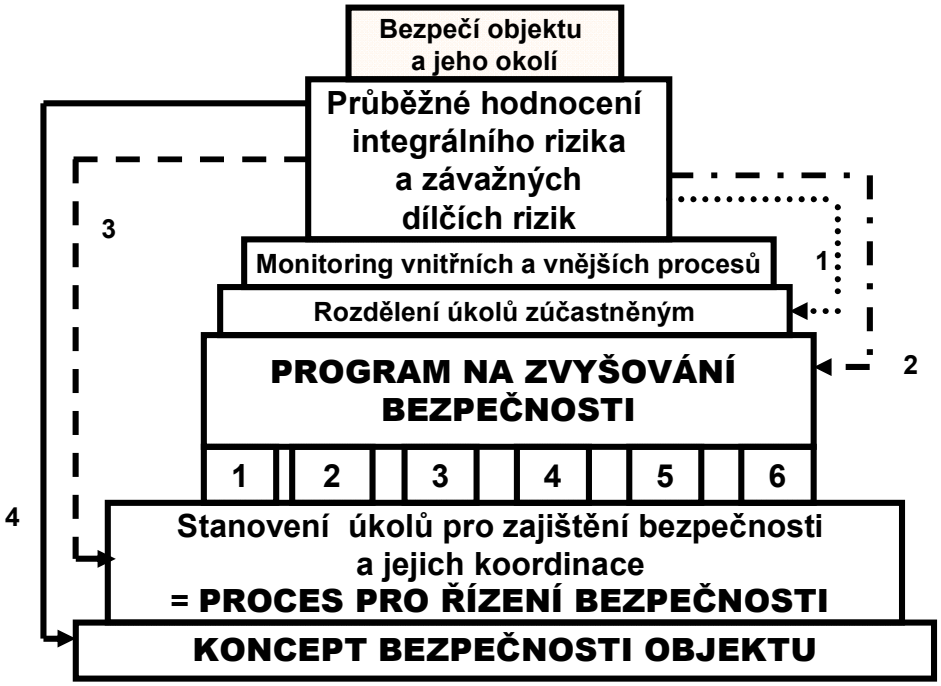
První proces se skládá z podprocesů pro: celkovou koncepci; dosahování dílčích cílů bezpečnosti; vedení / správu bezpečnosti; systém řízení bezpečnosti; personál a zahrnuje úseky pro: řízení lidských zdrojů, výcvik a vzdělání, vnitřní komunikaci / informovanost a pracovní prostředí; revize a hodnocení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

Na základě analýz existujících systémů řízení bezpečnosti, popsaných v odborné literatuře, o nichž jsou údaje shrnuté v pracích [1-4,15,18], a především poznatků shromážděných OECD [2,21-23] autorka sestavila metodou analogie k existujícím modelům řízení bezpečnosti obecný procesní model systému řízení bezpečnosti entity, ověřila ho na datech shromážděných v archivu [24] a metodou analogie převedla pro kritické složité objekty, obrázek 3. Z obrázku 3 je zřejmá zásadní role konceptu bezpečnosti objektu průběžného hodnocení integrálního rizika a závažných dílčích rizik. V případě, že se při hodnocení zjistí, že riziko je nepřijatelné, je třeba provést změny, jak naznačují zpětné vazby na obrázku 3. Protože změny vyžadují zdroje, síly a prostředky, tak na základě zajištění hospodárnosti se nejprve realizuje zpětná vazba 1, a teprve, když nepřinese žádoucí stav, tak se realizuje zpětná vazba 2; poté zpětná vazba 3, a když ani po ní není žádoucí výsledek, tak zpětná vazba 4. V případě výskytu extrémních jevů s katastrofickými dopady se přikračuje okamžitě k realizaci zpětné vazby 4.

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

- Role a odpovědnosti osob podílejících se na řízení závažných nebezpečí, která jsou spojená s možnými pohromami na všech organizačních úrovních kritického objektu a opatření na zajištění výcviku, která jsou sladěna s identifikovanými potřebami výcviku.
- Plány pro systematické identifikování závažných nebezpečí spojených s možnými pohromami a z nich plynoucích rizik, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti).

- Plány a postupy pro zajištění bezpečnosti všech komponent, systémů a funkcí v kritickém objektu a v jeho okolí, a to včetně údržby objektů, zařízení.
- Plány na implementaci změn v kritickém objektu a v objektech i zařízeních, které jsou v okolí.
- Plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na možné nouzové situace.
- Plány pro průběžné hodnocení souladu s cíli vyjasněnými v koncepci bezpečnosti a zabudovanými v SMS, a účinné mechanismy pro vyšetřování a provádění korekčních činností v případě selhání s cílem dosáhnout stanovené cíle.
- Plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků kritického objektu.



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

8. Závěr

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

- interval (-σ,+σ) pokrývá 68.5 % případů,
- interval (-2σ, +2σ) pokrývá 95.4 % případů,
- interval (-3σ, +3σ) pokrývá 99.8 % případů.

Proto nyní připouštíme, že složité kritické objekty jsou z různých důvodů čas od času v nestabilním stavu a vznikají organizační havárie, kaskády selhání bez zjevné příčiny, tj. připouštíme nejistoty náhodné i epistemické (znalostní) v jejich chování. Z důvodu zajištění bezpečnosti kritických objektů a ochrany lidí hledáme řešení odezvy pro možné

případy, které nelze odhalit pravděpodobnostními přístupy a budujeme pro ně náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik záchranářů.

Dosažení požadované úrovně bezpečnosti znamená dobře řídit a správně rozhodovat. Dobré / správné řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici. Data musí být: správná, tj. zná se jejich velikost a přesnost; a musí mít vypovídací schopnost pro řešený problém, tj. musí být validovaná. Datové soubory musí být reprezentativní, tj.: úplné; obsahovat správná data; mít dostatečný počet dat; data musí být rozprostřena homogenně v celém sledovaném intervalu a musí být validovaná. Při aplikaci modelů musí být správně zváženy nejistoty a neurčitosti v datech.
Je si nutno uvědomit, že v reálném světe při zajišťování bezpečnosti kritických objektů řešíme netriviální problémy, tj.: je více chráněných aktiv, jejichž cíle jsou konfliktní; aktiva se mění v čase a prostoru; a prostředí, ve kterém jsou aktiva, tj. lidský systém se dynamický vyvíjí.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN:978-80-01-04844-3. Praha: ČVUT, 483p,
[2] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191p.
[3] PROCHÁZKOVÁ, D., BUMBA, J., SLUKA, V., ŠESTÁK, B. *Nebezpečné chemické látky a chemické přípravky a průmyslové nehody*. ISBN 978-80-7251-275-1. Praha: PA ČR 2008, 420p.
[4] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. Praha: ČVUT 2013, ISBN:978-80-01-05245-7, 223p.
[5] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. ISBN:978-80-01-04841-2. Praha: ČVUT 2011, 405p.
[6] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. Praha: ČVUT 2012, ISBN:978-80-01-05103-0, 318p.
[7] ROPOHL, G. *Philosophy of Socio-Technical Systems*. In: Society for Philosophy and Technology, 4 (1999), No 3.
[8] PROCHÁZKOVÁ, D. *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.
[9] STEIN, W., HAMMERLI, B., POHL, H., POSCH, R.(eds). *Critical Infrastructure Protection – Status and Perspectives*. Workshop on CIP, Frankfurt am Main, www.informatik2003.de
[10] MOTEFF, J., COPELAND, D., FISCHER, J. *Critical Infrastructures: What Makes an Infrastrucuture Critical?* Report for Congress, 2003, CRS Web, Order Code RL31556.
[11] RINALDI, S. M. *Modeling and Simulating Critical Infrastructures and Their Interdependencies.* In: Proceedings of the 37th Hawaii International Conference on System Sciences – 2004. Sandia National Laboratories. Sandia. Web: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1265180
[12] RINALDI, S. M., PEERENBOOM, J. P., KELLY, T. K. *Critical Infrastructure Interdependencies. (Identifying, Understanding, and Analyzing).* In: IEEE Control Systems Magazine, Vol. 21, December 2001, pp.12-25, www.ce.cmu. edu/~hsm/im2004/readings/CII-Rinaldi.pdf
[13] KUHLMANN, A. *Does Safety Science Fulfill the Requirements of Modern Technical Systems?* In: Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN:3-8249-0659-7, pp. 9-17.
[14] REASON, J. *Human error*. Cambridge University Press 1990.
[15] NOWAKOWSKI T. ET AL. (eds). *Safety and Reliability: Methodology and Application*. London: Taylor & Francis Group 2014, ISBN:978-1-138-02681-0, 2453p.
[16] IAEA. *Assessment of Defence in Depth for Nuclear Power Plants*. Safety report series No. 46. Vienna: IAEA 2005, ISBN: 92–0–114004–5, 119p.
[17] SEVCIK, A., GUDMESTADO, T. *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.
[18] PROCHÁZKOVÁ, D. *Challenges Connected with Critical Infrastructure Safety*. Saarbruecken: Lambert Academic Publishing 2014, ISBN:978-3-659-54930-4, 218p.
[19] VATN, J. *Structuring Contributors to Successful Operation*. In: Safety and Reliability: Methodology and Application. London: Taylor & Francis Group 2014, ISBN:978-1-138-02681-0.
[20] PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. Praha: ČVUT 2011, 301p. ISBN: 978-80-01-04843-

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

[22] OECD. *Environmental Indicators: Overview of Work Programme and Publications.Group on the State of the Environment*. Paris: OECD1993.

[23] OECD. *Indicators to Measure Decoupling of Environmental Pressure from Economic Growth*. OECD SG/SD(2002)1/FINAL, 16. 5. 2002.

[24] PROCHÁZKOVÁ, D. *Výsledky identifikace rizik kritických objektů* Archiv ČVUT v Praze, fakulta dopravní, ústav bezpečnostních technologií a inženýrství.

ADRESA AUTORA

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

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

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