GLOBÁLNE ENVIRONMENTÁLNE RIZIKÁ • 2023 • GLOBAL ENVIRONMENTAL RISKS
Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

OPEN ACCESS Article

GENERICKÝ MODEL PRO ŘÍZENÍ BEZPEČNOSTI SLOŽITÉHO OBJEKTU

Dana PROCHÁZKOVÁ [1] - **Miroslav RUSKO** [2]

GENERIC MODEL FOR MANAGEMENT OF SAFETY OF COMPLEX INSTALLATION

GLOBAL ENVIRONMENTAL RISKS ´2023

[1] *Czech Technical university in Prague, Fakulta strojní, Technická 4, 166 07 Praha, Czech Republic*
Email: danuse.prochazkova@fs.cvut.cz
ORCID iD: 0000-0002-4424-3974 ; *https://orcid.org/0000-0002-4424-3974*

[2] *Department of Management, Faculty of Education, Catholic University in Ružomberok, Hrabovská cesta 1, 034 01, Ružomberok, Slovak Republic •• Slovak Society for the Environment, Koceľova 15, 815 94 Bratislava, Slovak Republic*
Email: mirorusko@centrum.sk
ORCID iD: 0000-0002-1428-0141 *https://orcid.org/0000-0002-1428-0141*

Competing interests : The author declare no competing interests.
Publisher's Note: Slovak Society for Environment stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Review text in the conference proceeding: Contributions published in proceedings were reviewed by members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.
Slovak Society for the Environment (Slovenská spoločnosť pre životné prostredie) Bratislava, Slovak Republic

ABSTRAKT
Složitost objektů a infrastruktur roste. Na jedné straně tím roste efektivita předmětných systémů, ale na druhé straně se vytváří nové zdroje rizik, které jsou hůře odhalitelné. Proto mnohá z nových nebezpečí jsou záludnější, hůře eliminovatelná, než v minulosti. Navíc neexistuje žádná předchozí zkušenost, které by mohlo být využito při překonávání nových nebezpečí. Článek shrnuje současné poznatky o rizicích a bezpečnosti složitých objektů a stručně popisuje generický model pro řízení bezpečnosti složitých objektů.

Klíčová slova: *Riziko; bezpečnost; řízení bezpečnosti; složité objekty; generický model.*

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

ABSTRACT
The complexity of objects and infrastructures is increasing. On the one hand, this increases the efficiency of the systems in question, but on the other hand, it creates new sources of risk that are more difficult to detect. Therefore, many of the new dangers are more insidious, harder to eliminate, than in the past. Moreover, there is no previous experience that can be used to overcome new dangers. The article summarizes the current knowledge about the risks and safety of complex objects and briefly describes a generic model for managing the safety of complex objects.

Key words: *Risk; safety; safety management; complex objects; generic model.*

1. ÚVOD

Inženýrství zacílené na bezpečnost představuje soubor znalostí a dovedností, které řeší určitý problém, tj. uspokojují požadavky, kterými jsou užitečnost, disponibilita a bezpečnost, a to na základě principů systémového inženýrství. Předmětné inženýrství je cíleně orientovaný proces, který je založen na propojení řady disciplín a zacílen na tvorbu a provoz bezpečných objektů, které plní určité lidské potřeby, které velmi dobře definoval Maslow [1].

Složitost objektů a infrastruktur roste. Na jedné straně tím roste efektivita předmětných systémů, ale na druhé straně se vytváří nové zdroje rizik, které jsou hůře odhalitelné. Proto mnohá z nových nebezpečí jsou záludnější, hůře eliminovatelná, než v minulosti. Navíc neexistuje žádná předchozí zkušenost, které by mohlo být využito při překonávání nových nebezpečí. Článek shrnuje současné poznatky o rizicích a bezpečnosti složitých objektů a stručně popisuje generický model pro řízení bezpečnosti složitých objektů. Práce uvádí generický model pro řízení bezpečnosti, který ukazuje hierarchické uspořádání plnění opatření pro řízení rizik ve prospěch bezpečnosti.

2. SOUHRN POZNATKŮ O RIZIKU A BEZPEČNOSTI

Na základě současného poznání [2] je každý objekt otevřený systém, který se skládá z řady položek, které jsou vzájemně propojené. Jednotlivé položky i celek na základě procesů probíhajících uvnitř i vně systémuse dynamicky vyvíjí. Propojení mezi položkami jsou fyzická, kybernetická, územní a logická a v řadě případů jsou zranitelnější než položky [3]. ***Bezpečnost objektu či procesu vyjadřuje úroveň kvality souboru antropogenních opatření a činností, která vedou k zajištění bezpečí a rozvoje objektu či procesu***[2,3].

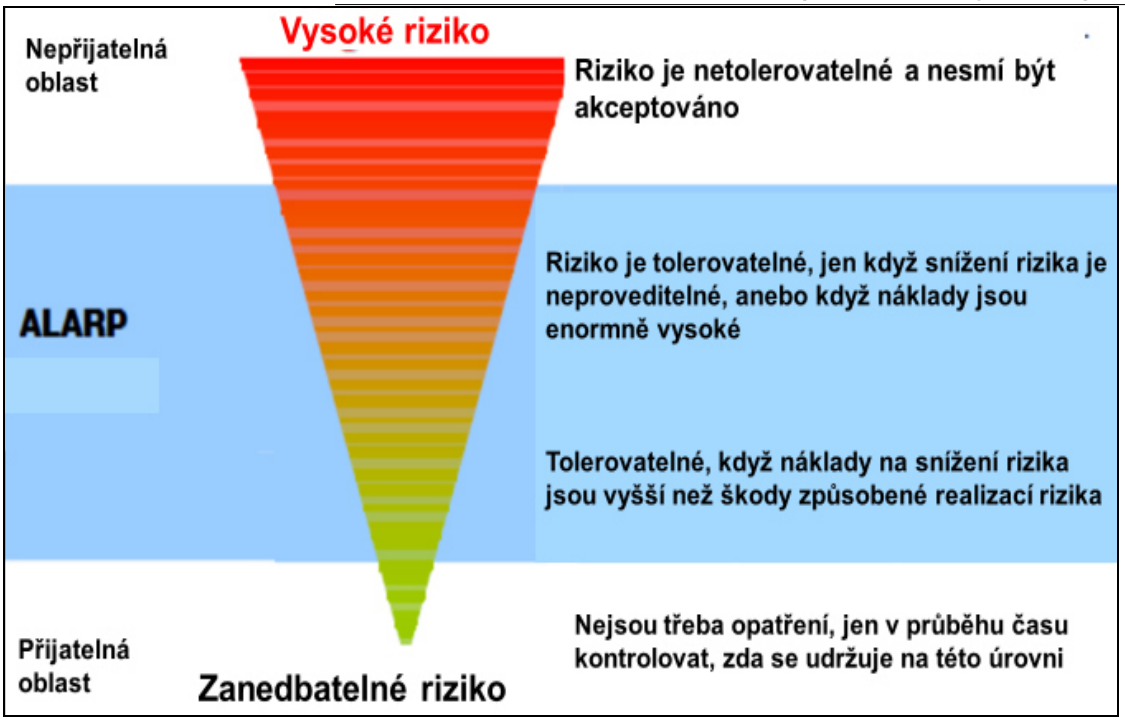
Vývoj objektu v čase je narušován jevy, které jsou světu vrozené / inherentní a mají od určité velikosti nežádoucí, a tudíž nepřijatelné dopady na objekty, které lidská společnost potřebuje pro život [2]. Mírou ztrát a škod objektu a jeho okolí je v inženýrských disciplínách riziko, které je definováno jako pravděpodobná velikost ztrát, škod a újmy na chráněných aktivech objektu a veřejných aktivech v okolí, která je normovaná na zvolené jednotky času a území. Riziko je závislé na velikosti konkrétního škodlivého jevu (pohromy) a na místní zranitelnosti aktiv [2]. Míra narušení bezpečnosti objektu se nazývá „***kritičnost***“ azávisí na velikosti škodlivého jevu a na zranitelnostiobjektu, tj. zranitelnosti jeho aktiv a jejich propojení, tj. na velikosti rizika [2].

Rizika v praxi dělíme na přijatelná, podmíněně přijatelná (ALARP / ALARA) a nepřijatelná (obrázek 1). V případě rizik, která jsou:

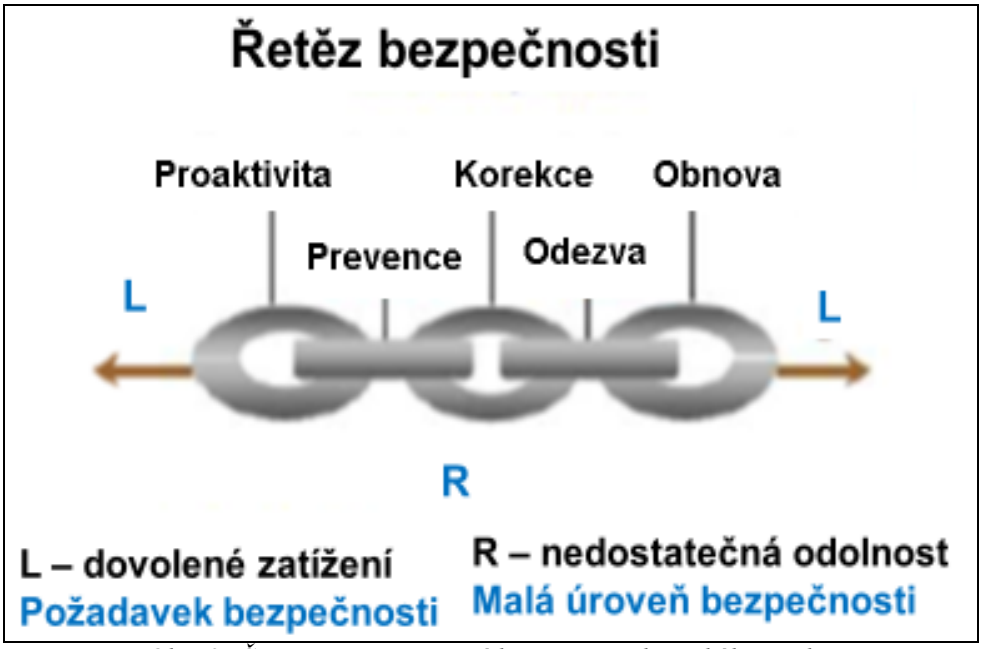
- nepřijatelná je třeba zajistit aplikaci účinných preventivních opatření vůči jejich zdrojům,
- podmíněně přijatelná, je třeba připravit zmírňující, reaktivní a obnovující opatření pro sledovaná aktiva,
- a u přijatelných sledovat, zda v čase nedojde ke zvýšení škodlivého potenciálu jejich příčin.

Uvedeným způsobem provádíme činnost, kterou nazýváme „řízení rizik“. Řetěz pro zajištění bezpečnosti je uveden na obrázku 2.

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic



Obr. 1. Podklady pro dělení rizik podle přijatelnosti.



Obr. 2. Činnosti pro zajištění bezpečnosti kritického prvku.

Bezpečnost objektu (technického zařízení i technických děl) či procesu a jejich okolí lze zajistit jen kvalitním antropogenním řízením [2,3]. Na základě hospodárnosti je třeba především provést snížení rizik v nejkritičtějších místech v rámci prevence, i připravit odezvu a obnovu na rizika, která nejsou vypořádána buď z důvodu opomenutíebo neznalostí v procesu projektování a zhotovení, anebo preventivní opatření jsou velmi nákladná. Jedná se o velmi nákladnou činnost, a proto je nutná vzájemná komunikace mezi vlastníky a provozovateli technických děl, veřejnou správou, veřejností a médii [3].

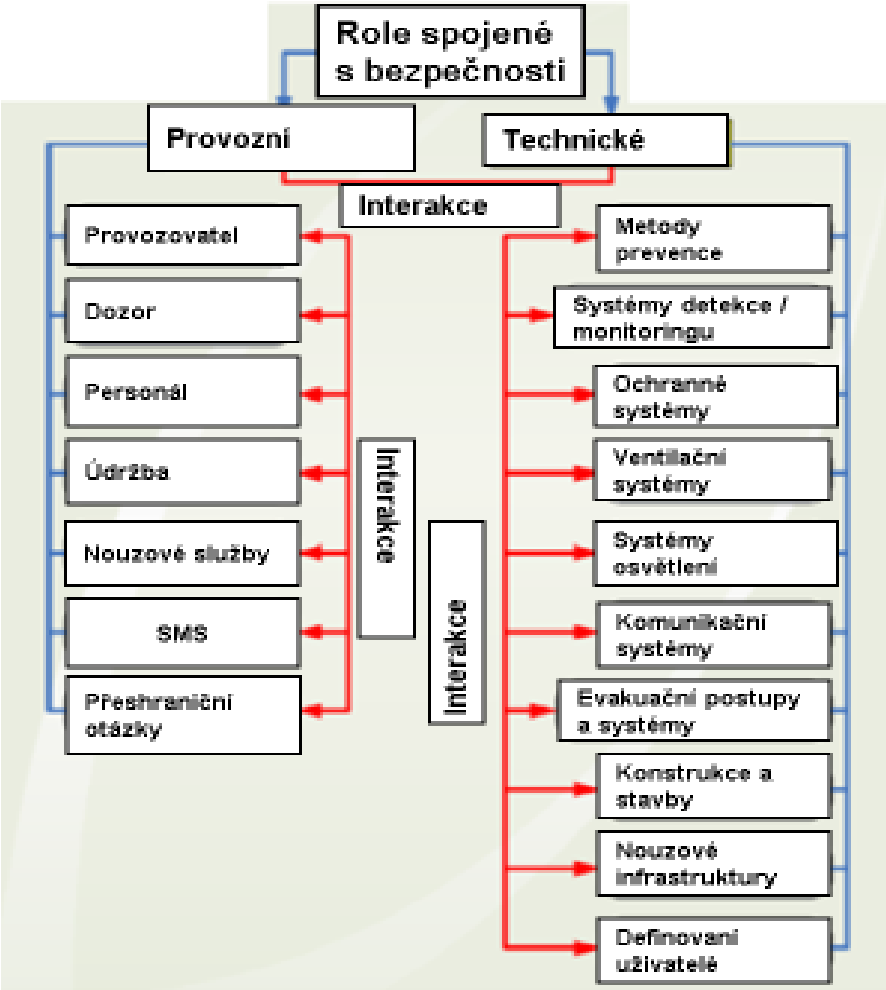
Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá dle [2,3] v rozdělení rizik do kategorií, ve kterých se část rizika: sníží, tj. preventivními opatřeními se odvrátí realizace rizika; zmírní, tj. preventivními opatřeními a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se sníží nebo odvrátí nepřijatelné dopady; pojistí; zajistí opatřeními odezvy a obnovy, pro které se připraví rezervy všeho druhu; a pro část, která je neřiditelná nebo příliš nákladná nebo málo častá se připraví plán pro nepředvídané situace (Contingencyplan).

3. GENERICKÝ MODEL PRO ŘÍZENÍ BEZPEČNOSTI

Obrázek 3 ukazuje role spojené s bezpečností objektu při provozu v oblasti organizace a v oblasti technického vybavení, nástrojů a personálu. Důležitou roli v oblasti organizace má systém řízení bezpečnosti (SMS – safety management systém). Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika. Systém řízení bezpečnosti SMS (Safety management system) objektu– obrázek 4, proto musí obsahovat provázané položky:

- strategický postup pro zajištění bezpečnosti,
- organizaci řízení bezpečnosti,
- plán pro řízení bezpečnosti,
- opatření pro vypořádání rizik,
- měření úrovně bezpečnosti
- a způsob rozhodování o opatřeních pro udržení či zvýšení úrovně bezpečnosti [3].



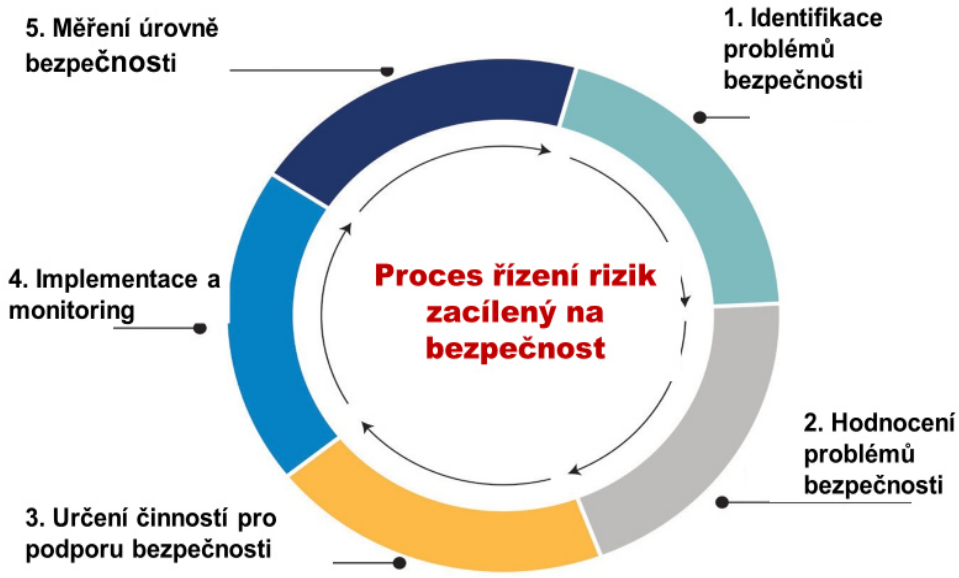
Obr. 3. Role zúčastněných spojené s bezpečností.

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

Obr. 4. Úkoly uvedené v systému řízení bezpečnosti (SMS) objektu.

Podle současných znalostí je nutné při sestavování konceptu bezpečnosti objektu začít od jeho umístění, přes projektování, zhotovení a až k provozu. Je třeba propojit normy a výsledky řízení rizik ve prospěch bezpečnosti, tj. používat nástroje risk-based design, risk-basedoperation; risk-basedinspections, risk-basedmaintenance atd. [3,4], které propojují normy a výsledky řízení rizik. Vlastní metodický proces řízení rizik ve prospěch bezpečnosti (obrázek 5) zahrnuje:

- identifikaci problémů spojených s bezpečností,
- vyhodnocení těchto problémů z hlediska požadované úrovně bezpečnosti,
- určení opatření a činnosti pro udržení či zvýšení úrovně bezpečnosti,
- způsob implementace opatření,
- monitoring jejich účinnosti,
- posouzení úrovně bezpečnosti a v případě, že není dostatečná, způsob identifikace problémů a opakování řetězce akcí.



Obr. 5. Řízení bezpečnosti objektu.

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

Bezpečnost i zabezpečení objektů, hlavně kritických je zásadní pro ochranu a rozvoj lidí i státu, proto každý stát musí mít strategii na udržování a popř. i zvyšování bezpečnosti. Protože svět se dynamicky vyvíjí, tak mohou nastat podmínky, na které nejsou limity objektu připraveny, a proto systémy řízení bezpečnosti (i systémy řízení zabezpečení) musí být vždy vybaveny opatřeními pro minimalizování škod v případech, že bezpečnostní opatření a bezpečnostní systémy selžou, anebo se vyskytne neidentifikované nebezpečí.

Koncept objektu zacílený na bezpečnost [3,5] řeší konflikty proaktivně a v systému řízení bezpečnosti (SMS) kloubí aspekty technické, organizační, právní, finanční, manažerské, sociální, znalostní, vzdělávací, mezinárodní apod.; a v hlavních procesech má proces pro řízení bezpečnosti – PSM (Proces Safety Management) [5]; obrázek 6.

Obr. 6. Procesní model řízení bezpečnosti objektu v čase. Procesy: 1- koncepce a řízení; 2 - administrativní postupy;3 - technické záležitosti; 4 - vnější spolupráce; 5 - nouzová připravenost; 6 - dokumentace a šetření havárií; a zabezpečení objektu – zpracováno dle [3,5].

Systém řízení bezpečnosti (tzv. SMS – Safety Management System) složitého 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. Skládá se ze sedmi procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií; zabezpečení objektu i systému řízení, tj. informačního a kontrolního (ovládacího) systém.

Uvedené procesy se dále dělí na podprocesy:

- Proces pro koncepce a řízení se skládá z podprocesů pro: celkovou koncepci; dosahování dílčích cílů bezpečnosti; vedení / správu bezpečnosti; systém řízení bezpečnosti; personál a

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

zahrnuje úseky pro: řízení lidských zdrojů, výcvik a vzdělání, vnitřní komunikaci / informovanost a pracovní prostředí; revize a hodnocení plnění cílů v bezpečnosti.

- Proces pro administrativní postupy 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.
- Proces pro technické záležitosti 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.
- Proces pro vnější spolupráci obsahuje podprocesy pro: spolupráci se správními úřady; spolupráci s veřejností a dalšími zúčastněnými (včetně akademických pracovišť); a spolupráci s dalšími podniky.
- Proces pro nouzovou připravenost 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.
- Proces pro dokumentaci a šetření havárií 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).
- Proces pro zabezpečení má podporocesy pro: kybernetickou ochranu; fyzickou ochranu; a ochranu know-how.

Rizika objektů 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 [3]. Přijatelné riziko závisí na sociálních, ekonomických a politických faktorech, a platí, že přijatelná úroveň rizika neznamená nulové škody, ztráty a újmy na chráněných aktivech, tj. že pravděpodobnost vzniku ztrát, škod a újmy na chráněných zájmech je malá až zanedbatelná.

Systém řízení bezpečnosti objektu (safety management systém – SMS) je mechanismus, který řídí (reguluje/ kontroluje) sledovaný objekt. Určuje dynamické chování objektu tím, že popisuje mechanismy, které ho určují. Mechanismy jsou vytvářeny systémy zpětných vazeb. Zpětné vazby jsou pozitivní, když mají synergickou zesilující funkci, a negativní, když mají regulační funkci. Lze na ně pohlížet jako na systémové mechanismy, které zajišťují dynamickou rovnováhu systému (každý systém se vyvíjí a může existovat jen tehdy, když je v dynamické‘ rovnováze). To znamená, že v případě menšího narušení provádí předmětné mechanismy kompenzaci narušení menšími vnitřními změnami, v případě větších narušení změnami většími, které mohou narušit stabilitu systému, a tím i jeho bezpečnost.

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

Realita je složitější, máme poznatky o různých působeních kumulace menších narušení, a to ve smyslu positivním i negativním, které osvětlují až recentní teorie, a to teorie chaosu, teorie možností či teorie komplexity. Je pochopitelné, že schopnost dynamických mechanismů systému není neomezená a při velkých zásazích nemusí být zmíněné mechanismy schopny kompenzovat narušení v dostatečné míře tak, aby odvrátily selhání objektu. Při regulaci (tj. při tvorbě regulačních mechanismů u technologických systémů) se vychází z kybernetického pojetí, že každý systém má určité podmínky existence a že existují bariéry v prostoru a čase, které v zájmu jeho existence nesmí být narušeny. Úkolem lidí odpovědných za řídicí systém je předmětné bariéry rozpoznat a regulovat dostupnými prostředky (pasivními i aktivními) a antropogenními činnostmi chování předmětných systémů tak, aby nedošlo k překročení bariér.

Řízení bezpečnosti vychází z řízení procesů, které je založeno na důsledném využití znalostí o problému v systému a jeho okolí, a proto se mu také říká „knowledge management“. Řízení procesů založené na řízení znalostí se nezaměřuje na výsledky, ale na příčiny. Je založené na rozpracování koncepce a metodologie. Strategická úroveň tohoto řízení určuje základní směry vývoje, ze kterých vyplývá, které procesy je nezbytné upravit nebo vytvořit, jaké organizační změny bude nezbytné provést, kde získat know-how, finanční zdroje atd. Taktická úroveň řízení procesů pomáhá utřídit činnosti nutné pro realizaci dlouhodobých záměrů. Hledají se odpovědi na otázky jak procesy nastavit, v jakém stavu je udržovat a jak musejí tyto procesy navzájem spolupracovat. Operativní úroveň řízení rozhoduje o konkrétním rozmístění zdrojů v procesu (lidských, technologických, finančních) a také o výkonu jednotlivých činností v rámci nastavených procesů (jak provést konkrétní operaci). Snahou je zajistit transfer znalostí a dovedností mezi pracovníky. Na technické úrovni řízení se řeší konkrétní problémy. Je si třeba uvědomit, že nejnáročnější je vyjednávání s riziky, které se odehrává právě na této posledně jmenované úrovni řízení; zde se zvyšuje odolnost prvků, zařízení, komponent i celých systémů a dle údajů z praxe úspěšnost technických opatření se pohybuje mezi 40 a 80%.

Pro zajištění bezpečnosti zahrnující funkčnost, provozní spolehlivost a stabilitu objektu jsou důležité limity a podmínky nastavené v projektu [3,5]. Úkolem SMS je udržovat určené fyzikální veličiny (parametry dílčích systémů) na předem určených hodnotách a při použití automatizace upozornit na významné odchylky vyvolané chováním senzorů. V procesu regulace mění řídicí systém působením na akční veličiny stavy jednotlivých řízených systémů tak, aby bylo dosaženo žádaného stavu celého systému.

U řídicího systému se sledují v prioritním pořadí vlastnosti jako:

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

Z výše uvedeného vyplývá, že řídicí systémy určují kvalitu a výkon (výkonnost) systémů. Mají rozhodující vliv na bezpečnost, a proto se u řídicích systémů sledují faktory: odpovědná autonomie; adaptabilita; celistvost; a smysluplnost úkolů. Celistvost vyjadřuje vnitřní jednotu, tj. autonomnost, nezávislost a odlišnost od okolí. Protože lidské chování není deterministické, jsou hlavními charakteristikami předmětných systémů vynořující se vlastnosti, nedeterministické chování a složité vztahy mezi organizačními cíli. O každém sledovaném systému vždy rozhoduje člověk a údržba, renovace, změny. Z inženýrského pohledu se sledované systémy charakterizují strukturou, hardwarem, procedurami, prostředím, toky informací, organizací (problém organizačních havárií) a rozhraním mezi uvedenými položkami [3,5].

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

Účinná kultura bezpečnosti je základním prvkem bezpečnosti [3,5]. Odráží koncepci bezpečnosti a vychází z hodnot, stanovisek a jednání vrcholových řídících pracovníků a z jejich komunikace se všemi zúčastněnými. Ukládá managementu objektu, aby praktikoval takový systém řízení bezpečnosti objektu, který udrží procesy v objektu v určitých mezích. Je zřetelným závazkem aktivně se podílet na řešení otázek bezpečnosti a prosazuje, aby všichni zúčastnění konali bezpečně a aby dodržovali příslušné právní předpisy, standardy a normy. Pravidla kultury bezpečnosti musí být zapracována do všech činností v území / objektu. Jejich základem není koncentrace na potrestání viníků / původců chyb, ale poučení z chyb a zavedení takových nápravných opatření, aby se chyby nemohly opakovat nebo aby se alespoň výrazně snížila četnost jejich výskytu.

4. PLÁN ŘÍZENÍ RIZIK

Pro účinné a kvalitní zvládnutí dílčích rizik je vhodné zpracovat plán řízení rizik dle ISO 31 000. Plán řízení rizik je nástroj pro proaktivní řízení rizik, které zvažuje možná vzájemná propojení v čase [2]. Je klíčovým výstupem každého řízení rizik. Svět se dynamicky mění, a proto pro zajištění bezpečnosti během času je vždy důležité stanovení toho, co je třeba v dané situaci provést, určení toho, kdo opatření provede a stanovení osoby, která odpovídá za provedení, tj. plán řízení rizik; a to na úrovni top managementu, senior managementu, liniového managementua konkrétních pracovníků.

Plán řízení rizik se opírá o způsob řízení TQM [6]. Zvažuje prioritní rizika, která nebylo možno vypořádat jistými preventivními opatřeními, a která při realizaci mají potenciál významně poškodit technické dílo. Samotný plán se zpracovává ve formě tabulky, která zvažuje rizika z oblastí:řízení technického díla; vnitřní zdroje rizik technického díla spojené s jeho stavbou, konstrukcí, zařízeními a provozem; personál technického díla; vnější zdroje rizik technického díla spojené s živelními pohromami; vnější zdroje rizik technického díla spojené s chováním veřejné správy, konkurencí, trhem apod.; útoky na technické dílo; kybernetické zdroje rizik spojené se sítěmi; válka; a dozor veřejné správy.

Pro každou oblast rizika se v tabulce uvádí:příčiny rizika; dopadyselhání kritického prvku dopravní infrastruktury rizika na veřejná aktiva v okolí a na službu, kterou poskytuje státu dopravní infrastruktura; pravděpodobnost / četnost výskytu realizace rizika a velikostdopadů rizika; opatření na zvládnutí nebo alespoň zmírnění rizika, které jsou jasně stanoveny, a u každého z nich je uvedena organizace (či její odpovědný zástupce), která provede odezvu a osoba odpovědná za správné a včasné provedení odezvy je uvedena odpovědnost za jejich provedení.***Plán pro řízení rizik se připravuje předem a při jeho přípravě se řeší i očekávané konflikty při odezvě na dopady rizik.***

Podle principů platných v řízení [7-11] odpovědnost za bezpečnost technických zařízení má vlastník i veřejná správa. Důležitou roli při řízení hraje organizační struktura správy kritického prvku [7-10], tj. mechanismus, který slouží ke koordinaci a řízení provozu kritického prvku. Představuje hierarchické uspořádání vztahů nadřízenosti a podřízenosti a řeší vzájemné pravomoci (kompetence), vazby a odpovědnost. Uvolnění velkých finančních a dalších prostředků na řízení a vypořádání rizik pochopitelně je jen na nejvyšší hierarchické úrovni. Na základě analogie s materiály [10,11] je zvážena struktura: vrcholový management; střední management; technický management; a personál (kritický a podpůrný), a také role veřejné správy, která vykonává dohled nad bezpečností ve veřejném zájmu. Generické modely plánů řízení rizik pro různé fáze životnosti kritických objektů jsou v pracích[12-15].

5. ZÁVĚR

Ačkoliv koncept integrální bezpečnosti se rozšiřuje v praxi pomalu z důvodů uvedených v práci [12], je třeba ho prosazovat, protože do pojetí integrální bezpečnosti patří i život podporující funkce, jejichž rizika s ohledem na zdraví člověka, ekosystémy a bezpečnost systému se minimalizují.

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

Generický model pro řízení bezpečnosti objektů (a to hlavně kritických) ukazuje způsob řízení rizik, aby se předešlo, anebo alespoň zmírnilo možným nežádoucím a nepřijatelným dopadům. Jeho respektování zajišťuje, že všichni zúčastnění chápou řízení rizik ve prospěch bezpečnosti stejně. Jednotné chápání rizik, způsobů a cílů jejich řízení dovoluje odstranit příčiny havárií, které vznikly různým chápáním rizik specialisty různých oborů [16,17].

Proto jeho respektováním lze zajistit zvládnutí (odstranění, zmírnění či připravenost na včasnou odezvu): slabin v zabezpečení vůči vnějším vlivům; vnitřních náhodných poruch systému; vnitřních systémových poruch zařízení; poruch v procesech; lidských chyb; nedostatku zdrojů; konfliktů mezi požadavky na bezpečnost a zabezpečení; chybné nebo nedostatečné identifikace ovlivňujících činitelů; chybné práce s riziky (volba metody, definice stupnice, ohodnocení rizika); neodpovědnosti manažerů či personálu; nekompetence manažerů či kritického personálu; a závislosti a nedůvěryhodnosti řešitelských subjektů.

V oblastech, kde jsou nadřazené systémy propojeny toky či vazbami s podřízenými či vedlejšími systémy jde především o zabránění: přenosu chybných a matoucích informací, tj. chyby na vstupu nebo na výstupu systémů; přerušení informačních a materiálových toků; vykonávání navzájem se ovlivňujících funkcí; a poruchám okolních systémů a realizaci relevantních pohrom.V oblastech propojení mezi jednotlivými vrstvami systému řízení bezpečnosti jde především o zabránění: aplikaci chybných metodik pro identifikace ohrožení a analýzy rizik z vyšších úrovní systému řízení bezpečnosti (SMS); neporozumění požadavkům a informacím z jiné vrstvy SMS; přenosu poruchových stavů v případě jejich výskytů z jedné vrstvy do druhé; a nedodání vstupní informace. Na rozhraní objektů s okolním prostředím jde o zabránění nepředvídatelným událostem a útokům: změna podmínek pro provoz ze strany státu; úmyslná poškození; a cílené útoky.

Složitost objektů a infrastruktur roste. Na jedné straně tím roste efektivita předmětných systémů, ale na druhé straně se vytváří nové zdroje rizik, které jsou hůře odhalitelné. Některé způsoby zajištění jejich bezpečnosti (např. redundance, znásobení součástkových komponent pro ochranu před selháním obvodů měřící nebo regulační funkce - zálohování) poskytuje ochranu před haváriemi zapříčiněnými selháním individuálních částí, není však stejně efektivní vůči škodlivým jevům, které vygenerují interakce mezi komponentami ve stále komplexnějších a vzájemně interagujících inženýrských systémech dneška. Redundance mohou ve skutečnosti zvýšit složitost až do takové míry, při které už ony samotné jsou přispívajícími faktory k haváriím.

Proto mnohá z nových nebezpečí jsou záludnější, hůře odhalitelná a eliminovatelná, než v minulosti. Navíc neexistuje žádná předchozí zkušenost, které by mohlo být využito při překonávání nových nebezpečí. Mnoho zkušeností a poučení z předcházejících havárií je uloženo v zákonech, normách a v postupech dobré praxe. Ale odpovídající zákony a normy pro mnohé z nových inženýrských odvětví a technologií ještě nejsou vypracované. Mnohokrát se poučení získané za celá staletí ztratí, když se starší technologie nahradí novějšími; například, když se mechanické zařízení nahradí digitálními počítači.

Dalšími novými nebezpečími jsou již jen heslovitě např.:vzrůstající expozice nebezpečí; zvyšování kumulace energií a dosahů nebezpečí; zvyšování automatizace; narůstající centralizace a výrobní kapacita; a nárůst tempa technologických změn. Proto je třeba kontinuálně monitorovat účinnost opatření a činností zacílených na bezpečnost a při zjištění odchylek aplikovat korekční opatření, anebo změnit koncept práce s riziky, jak ukazuje obrázek 6.

V rámci strategie pro zajištění bezpečnosti a udržitelného rozvoje se musí v kritických objektech nastavit: program pro neustálé zvýšení bezpečnosti kritických objektů; míry pro posuzování úrovně bezpečnosti z hlediska účinnosti bezpečnostního systému (ukazatele); program, který zajišťuje bezpečnost, který je sestaven z provázaných projektů; a projekty, které jsou naplněné provázanými procesy.

Nástroje pro ovládání kritických komplexních objektů a infrastruktur, zajišťující bezpečnost a rozvoj, tedy jinými slovy, zachování, ochranu a rozvoj chráněných aktiv jsou:umístění a výstavba objektů; promyšlený několika úrovňový řídicí systém zahrnující řízení strategické, taktické a operativní, který je založen na kvalifikovaných datech, odborných znalostech, expertních hodnoceních a dobrých metodách rozhodování; vzdělávání a výcvik zaměstnanců; věda, výzkum a TSO (profesní

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

organizace zajišťující profesionální podporu provozovatele kritického objektu a veřejné správy); specifické vzdělávání technických a řídících pracovníků; technické, zdravotní, ekologické, sociální, cyber a dalších standardy, normy a předpisy, tedy nástroje pro řízení procesů, které mohou nebo by mohly vést k výskytu (vzniku) pohromy nebo k zvětšení jejich dopadů; inspekce; systém spolupráce vedení komplexního objektu s veřejnou správou, s organizacemi na území a s organizacemi, které používají podobné technologie; personál pro zvládání nouzových situací; komponenty a systémy pro zvládání kritických situací (tj. všemi způsoby zajistit řízení kontinuity a krizové řízení); a bezpečnostní, nouzové (a to včetně plánování kontinuity kritických objektů) a krizové plánování.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] MASLOW, A. H. *Motivation and Personality*. New York: Haper 1954, 236 p.
[2] PROCHÁZKOVÁ D. *Analýza, řízení a vypořádání rizik spojených s technickými díly*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p., doi.org/10.14311%2FBK.978 8001064801
[3] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN: 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364p., doi.org/10.14 311%2FBK.9788001061824
[4] PROCHÁZKOVÁ D. Propojení norem a výsledků řízení rizik ve prospěch bezpečnosti. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 7-19. DSPACE. http://hdl.handle.net/10467/98461.
[5] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. Praha: DSPACE ČVUT 2022, 129 p. ISBN 978-80-01-06995-0, doi:10.14311/BK.9788001069950 .
[6] ZAIRI, M. *Total Quality Management forEngineers*. Cambridge: WoodheadPublishing Ltd, 1991.
[7] VEBER, J. a kol., 2001. *Management*. - ISBN 807261-029-5. Praha: Management Press. 700 p.
[8] BĚLOHLÁVEK, F, KOŠŤAN, P., ŠULEŘ, O. *Management.* ISBN 80-251-0396-X. Brno: ComputerPress 2006. 724 p.
[9] DĚDINA, J. *Management a organizační chování*. Praha: Grada 2005.
[10] DELONGU, B. *Risk Analysis and Governance in EU PolicyMaking and Regulation.* ISBN 978-3-319-30822-1. Springer 2016, 288 p.
[11] NENADÁL, J. TQM. *Role ekonomiky jakosti v koncepci TQM*. 1999, www: http://fmmi10.vsb.cz/639/ qmag/mj03-cz.htm .
[12] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L.*Řízení rizik procesů spojených s provozem technického díla během jeho životnosti.* ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. http://hdl.handle.net/10467/100254, doi.org/10.14311 %2FBK.9788001066751
[13] PROCHÁZKOVÁ, D., PROCHÁZKA, J., ŘÍHA, J., BERAN, V., PROCHÁZKA, Z.: *Řízení rizik procesů spojených se specifikací a umístěním technického díla do území.* ISBN: 978-80-01-06467-2. Praha: ČVUT 2018, 134p., http://hdl.handle.net/10467/100037 , doi.org/10.14311%2FBK.9788001064672
[14] PROCHÁZKOVÁ, D. PROCHÁZKA, J., ŘÍHA, J., BERAN, V., PROCHÁZKA, Z. *Řízení rizik spojených s ukončením provozu technického díla a s předáním území do dalšího užívání.*ISBN 978-80-01-06527-3. Praha: ČVUT 2018, 114 p., http://hdl.handle.net/10467/100036 , doi.org/10.14311%2FBK. 9788001065273
[15] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu.* ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. http://hdl.handle.net/10467/84466 , doi.org/10.14311%2FBK.9788001066096

Recenzovaný zborník vedeckých prác • Proceedings of scientific works
Edition ESE-63 • ISBN 978-80-570-5441-2
Bratislava: Slovak Society for Environment, Slovak Republic

[16] CEPIN, M., BRIS, R. *Safety and Reliability – Theory and Applications.* ISBN: 978-1-138-62937-0. London: Taylor& Francis Group 2017, 3627 p.

[17] HAUGEN, S., VINNEM, J., E., BARROS, A., KONGSVIK, T., VAN GULIJK, C. (eds). *SafeSocieties in a ChangingWorld.* ISBN: 978-0-8153-8682-7 (Handbook). London: Taylor& Francis Group 2018, 3234 p.; ISBN: 978-1-351-17466-4 (eBook); https://www.ntnu.edu/esrel2018