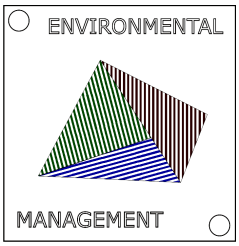
Manažérstvo životného prostredia ▮ 2022 ▮ Management of Environment
Recenzovaný zborník z XXII. medzinárodnej vedeckej konferencie, 5. máj 2022, Bratislava
Proceedings of the 22nd International Conference, Bratislava, May 5, 2022
Slovak Republic
Bratislava: Slovak Society for Environment • Edition ESE-61 • ISBN 978-80-973844-5-6

OPEN ACCESS Article

GENERICKÝ MODEL PRO ŘÍZENÍ BEZPEČNOSTI KRITICKÝCH PRVKŮ DOPRAVNÍ INFRASTRUKTURY

Jan PROCHÁZKA [1] - Dana PROCHÁZKOVÁ [2]

GENERIC MODEL FOR SAFETY MANAGEMENT OF CRITICAL ELEMENTS OF TRANSPORT INFRASTRUCTURE



[1] *Czech Technical university in Prague, Fakulta strojní, Technická 4, 166 07 Praha, Czech Republic*
[2] *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
Competing interests : The author declare no competing interests.

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.

ABSTRAKT
Dopravní infrastruktura je součástí kritické infrastruktury každého státu, což zaručuje jeho základní funkce. Řada jevů představuje nebezpečí pro jeho kritické prvky, a proto je nutné znát velikosti jejich ohrožení a řídit důležitá rizika, která jsou vždy lokálně a časově specifická. V současné době se jedná o řízení rizik ve prospěch bezpečnosti, která je chápána jako bezpečnost celku v systémové koncepci. Na základě současných poznatků dokument ukazuje obecný model řízení rizik kritických prvků dopravní infrastruktury ve prospěch integrální bezpečnosti.

KLÍČOVÁ SLOVA: *Dopravní infrastruktura; kritický prvek; rizika; bezpečnost obecný model řízení bezpečnosti.*

ABSTRACT
A transport infrastructure is part of the critical infrastructure of each State, which guarantees its basic functions. A number of phenomena pose a hazard to its critical elements, and therefore, it is necessary to know their hazards sizes and to manage the important risks, which are always locally and

temporally specific. At present, it is a risk management in favour of safety, which is understood as the safety of the whole in a systemic concept. Based on current knowledge, the paper shows a generic risk management model of critical elements of transport infrastructure in favour of integral safety.

KEYWORDS: *Transport infrastructure; a critical element; risks; safety; generic model for safety management.*

1 ÚVOD

Infrastruktury byly, jsou a budou veřejným aktivem, protože zajišťují dennodenní potřeby občanů, tj. energii, vodu, jídlo, informace apod. a závisí na nich přežití lidí při kritických situacích [1]. Dopravní systém obstarává dopravu osob a nákladů. Zahrnuje souborně všechny způsoby dopravy, které v rámci koordinace jednotlivých dopravních systémů spolupracují a vytváří logistickou síť. Dopravní infrastrukturu zahrnují mezi kritickou infrastrukturu všechny vyspělé země. Z pohledu plnění základních funkcí státu (ústavní zákon č. 1/1993 Sb., ústavní zákon č. 110/1998 Sb.), ochranu kritické infrastruktury upravuje zákon o krizovém řízení č. 240/ 2000 Sb. a průřezová a odvětvová kritéria nařízení vlády č. 432/2010 Sb.

Ve vyspělých zemích a v Evropské unii je cílem nejen ochrana, ale vyšší cíl, tj. bezpečnost základních infrastruktur a jejich propojení, tj. bezpečnost kritické infrastruktury za podmínek normálních, abnormálních i kritických [1,2]. Na základě současného poznání, obsaženého v renomovaných odborných zdrojích uvedených v [1,2]; a ze závazných dokumentů OSN, EU, OECD, IAEA a dalších je vytvořen generický model řízení bezpečnosti pro kritické prvky dopravní infrastruktury, které jsou chápány jako složité otevřené systémy v dynamicky proměnném světě, který je ovlivňován jak procesy, které probíhají nezávisle na člověku, tak procesy, které člověk vytváří vědomě či nevědomě svou činností a chováním [3].

2 RIZIKO A BEZPEČNOST

Riziko je veličina, která je mírou ztrát, škod a újmy na chráněných aktivech (a to ve sledovaném případě veřejných aktivech i aktivech technického díla). Jeho velikost závisí na konkrétní pohromě, která je zdrojem rizika a na zranitelnosti místních sledovaných aktiv. Ve strategickém řízení jsou definovány veličiny: ohrožení (anglicky hazard) jako pravděpodobná velikost pohromy, která se v daném místě vyskytne jedenkrát za definovaný časový interval (tzv. projektová nebo návrhová pohroma) [4]; a riziko jako pravděpodobná velikost ztrát, škod a újmy na sledovaných aktivech při projektové pohromě rozpočtená na jednotku času (nejčastěji 1 rok) a jednotku území [4]. Riziko je tudíž místně a časově specifické, protože závisí na množství a zranitelnosti aktiv v daném území a v daném čase.

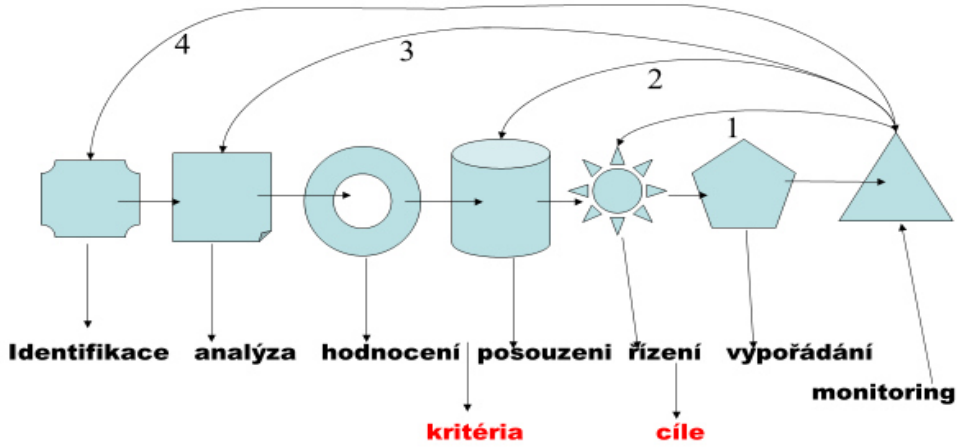
Riziko představuje míru narušení bezpečnosti sledovaného systému, který je předmětem sledování při výskytu možného škodlivého jevu. Jelikož výzkum technických děl ukázal, že nehody, havárie i selhání technických zařízení a technických děl nastávají v cca 80% při kombinaci škodlivých jevů, je třeba sledovat integrální riziko [5]. Proto integrální bezpečnost je spojena s řízením nejen velkých dílčích rizik, které představují nadprojektové živelní pohromy, ale především s řízením integrálního rizika.

Pojem bezpečnost se používá v mnoha souvislostech – bezpečnost zařízení, bezpečnost procesu, bezpečnost podniku, bezpečnost území atd. Z pohledu strategického řízení, jehož cílem je bezpečí a rozvoj lidí, jde o integrální bezpečnost, která respektuje systémové chápání světa a jeho součástí i jejich změny v čase a prostoru. Je založená na systémovém, proaktivním a strategicky zacíleném přístupu. Je chápaná jako emergentní vlastnost systému, na které závisí existence systému; tj. jde o hierarchicky nejvíce určující vlastnost systému. Jde o soubor opatření a činností, který při zohlednění povahy (podstaty/naturelu) kritického prvku chápaného jako systém systémů [2]a všech možných rizik i hrozeb směřuje k zajištění fungování prvků, vazeb a toků kritické infrastruktury tak, aby za žádných okolností nedošlo k jejich selhání, při kterém by ohrozily sebe nebo své okolí.

Integrální bezpečnost se neomezuje jen na jednostranná řešení v případě problémů jako je represe, ale zabývá se situacemi ovlivňujícími určitou úroveň bezpečnosti prostřednictvím tzv. řetězce bezpečnosti, jenž se skládá z dále uvedených částí: proaktivita (odstranění strukturálních příčin nejistoty, které narušují bezpečnost, tj. ohrožují bezpečí a udržitelný rozvoj); prevence (odstranění přímých příčin, je-li to možné, nejisté situace porušující stávající bezpečnosti) připravenost (řešit situaci, v níž je bezpečnost narušena); represe (odezva) (zvládnout narušení bezpečnosti a situaci stabilizovat) a obnova (zajistit podmínky pro obnovu a růst bezpečnosti).

Vzhledem k dynamickému vývoji světa, stárnutí a opotřebení částí technických prvků i technických děl a omezeným lidským znalostem, zdrojům a možnostem, management technického díla i veřejnáspráva se musípřipravovatnabudoucírealizacerizik. To znamená mít nástroje, kterými lze snížit realizace známých zdrojů rizik a zmírnit rizik nových. Práce prosazuje řízení rizik ve prospěch bezpečnosti. S ohledem na současné poznání je třeba propojit existující normy a standardy, protože obsahují dřívější poznatky a bez jejich aplikace by docházelo k opakování minulých chyb z minula a výsledky řízení rizik, jak doporučuje nyní i řada norem, např. ISO 31 000, ISO 31010, ISO 9000 atd. Způsob propojování ukazuje práce [6].

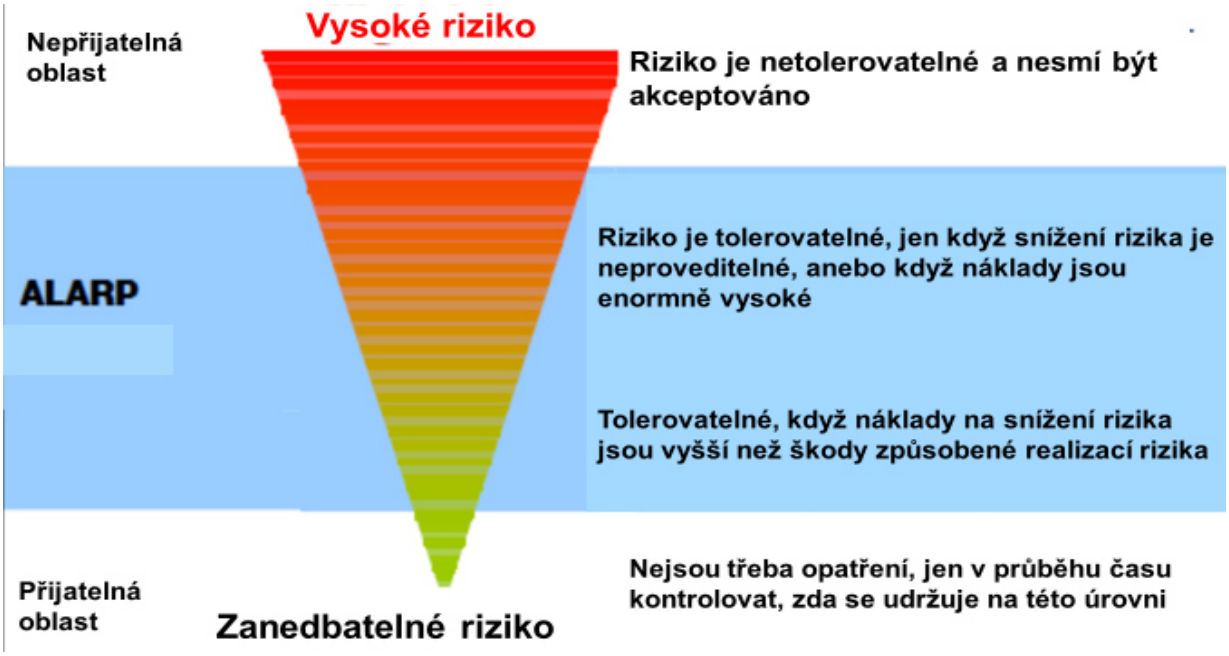
Obrázek 1 ukazuje postup práce s riziky [4]. Cílem je, aby technická zařízení i technická díla byla bezpečná, tj. kvalitně a spolehlivě plnila funkce, ke kterým byla vytvořena a přitom neohrožovala sebe a okolí, tj. lidi a životní prostředí, které je zásadní pro život a rozvoj lidstva. Proto v souladu se současnými znalostmi a zkušenostmi lidé musí nejprve poznat zdroje rizik (tj. pohromy – škodlivé jevy všeho druhu), ocenit jejich škodlivý potenciál (tj. určit ohrožení, která jevy představují a rozložení jejich dopadů) v jednotlivých místech a stanovit velikost možných ztrát a škod v závislosti na rozložení veřejných aktiv (tj. určit riziko). V závislosti na konkrétních možnostech dané lidské společnosti pak rozdělit rizika na přijatelná, podmíněně přijatelná a nepřijatelná [4]; podklad pro rozdělení je uveden na obrázku 2.



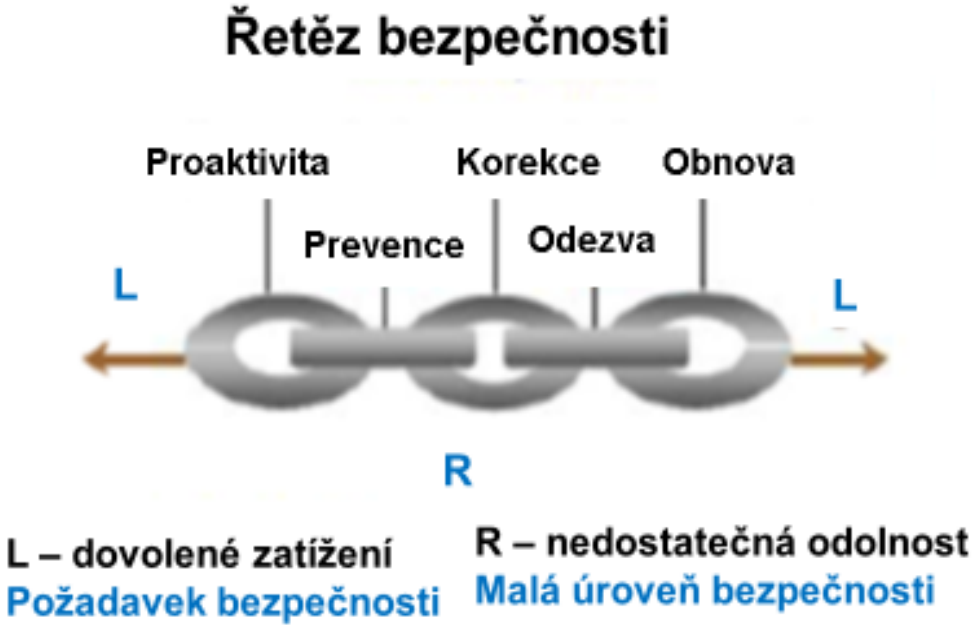
Obr. 1. Procesní model práce s riziky. Kritéria = podmínky, které stanovují, kdy je riziko přijatelné, podmíněně přijatelné nebo nepřijatelné. Cíle označují žádoucí stavy. Čísla 1,2,3,4 označují zpětné vazby, které se používají, když monitoring ukáže, že nejsou splněny stanovené požadavky na bezpečnost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

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 3.

Bezpečnost je chápaná jako vlastnost na úrovni systému, kterou formuje člověk svými opatřeními a činnostmi [4]. Veličiny riziko a bezpečnost nejsou komplementární veličiny, protože bezpečnost prostředí i každého technického díla lze zvýšit pomocí organizačních opatření, např. zavedením varovacích systémů, vzdělání osob a záložních řešení, aniž bychom snížili velikost rizika; doplňkovým pojmem k bezpečnosti je kritičnost [4].



Obr. 2. Podklady pro dělení rizik podle přijatelnosti.



Obr. 3. Činnosti pro zajištění bezpečnosti kritického prvku.

Bezpečnost technického zařízení i technických děl a jejich okolí lze zajistit jen kvalitním antropogenním řízením [4,7]. 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 opomenutí nebo 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 [7].

3 ZDROJE RIZIK U KRITICKÝCH PRVKŮ DOPRAVNÍ INFRASTRUKTURY

Na základě výsledků výzkumu popsaného v pracích [4,5,8-13] se v současné praxi v souvislosti s kritickými prvky dopravní infrastruktury díly používají dále uvedené výběry zdrojů rizik ve spojení s určenou entitou (technické zařízení, komponenta, propojení komponent apod.):

- Zdroje rizik určené buď legislativou, anebo zkušenostmi pracovníka, který předmětný úkol řeší.
- Jen technické zdroje rizik v daném kritickém prvku dopravní infrastruktury. Většinou jde o zdroje rizik spojené s: materiálem (splnění potřebných parametrů, dodavatelské vztahy – náhradní materiál apod.); konstrukcí a propojováním komponent a zařízení (nejsou stanovené postupy, jsou přítomné labilní nebezpečné látky apod.); výrobními postupy, např. při výrobě slitin, svařování, specifickém obrábění atd.; a podmínkami, které jsou nutné pro kvalitní výrobek, např. jistý tlak, jistá teplota či jistá vlhkost okolního prostředí atd.
- Technické zdroje rizik a lidský faktor. Jde o zdroje uvedené v bodě 2 a špatné provedení technických úkonů při provozu kritického prvku dopravní infrastruktury.
- Technické zdroje rizik a lidský faktor v nejširším pojetí. Jde o zdroje uvedené v bodech 2 a 3 a zdroje organizačních havárií v kritickém prvku dopravní infrastruktury (tj. špatná rozhodnutí, použití nesprávných postupů atd.).
- Zdroje rizik uvedené v bodech 2 až 4 doplněné o zdroje rizik související s BOZP a s pracovním prostředím.
- Zdroje rizik uvedené v bodech 2 až 5 doplněné o zdroje rizik z okolí kritického prvku dopravní infrastruktury, tj. vnější zdroje rizik.
- Zdroje rizik uvedené v bodech 2 až 6 doplněné o zdroje rizik spojené s propojeními mezi dílčími zařízeními, komponentami a systémy (jde o zdroje rizik, které jsou spojené s technickou integritou, automatizací, vzděláváním a dobrými dovednostmi, ochranou majetku, ochranou dat a informací, ochranou specifických znalostí, ochranou know-how, ochranou good will, financemi, konkurenceschopností, kontinuitou provozu za podmínek kritických a extrémních apod.).

Z uvedeného vyplývá, že v případech 1 až 6 jsou zanedbány mnohé zdroje rizik pro kritické prvky dopravní infrastruktury. Je to způsobeno skutečností, že v uvedených případech:

- při stanovení rizik nejsou zvažována všechna veřejná aktiva a všechna aktiva kritického prvku dopravní infrastruktury (tj. není respektován přístup All-Hazard-Approach [3-5], který je velmi náročný na data, metody, znalosti, zkušenosti a dobu provedení),
- je zanedbána systémová podstata kritického prvku dopravní infrastruktury,
- nezvažují se dynamické dopady vnějšího prostředí na kritický prvek dopravní infrastruktury, které následně ovlivní konkurenceschopnost kritického prvku dopravní infrastruktury a zajištění obslužnosti území v delším časovém intervalu (např. špatné postupy veřejné správy jsou zdrojem rizik pro kritické prvky dopravní infrastruktury).

Z hlediska potřeb a ekonomického využití zdrojů je však pravdou, že v řadě praktických úloh postačuje zvažovat jen některé zdroje rizik, protože cílem je bezpečné dílčí technické zařízení, a ne celý kritický prvek dopravní infrastruktury a jeho okolí. Proto je třeba u každé úlohy spojené s prací s riziky důležité určení cíle (obrázek 1).

Jelikož některá technická zařízení (pojišťovací ventily, odpouštěcí ventily apod.) či některé komponenty kritického prvku dopravní infrastruktury (tlaková zařízení, klimatizace, řídící systémy apod.) mají zásadní důležitost pro bezpečnost kritického prvku dopravní infrastruktury, tak u nich nestačí pracovat s riziky jen z hlediska samotné entity, ale je třeba pracovat s riziky, která jsou důležitá i z hlediska bezpečnosti celého kritického prvku dopravní infrastruktury). Jde o kritická zařízení, kritická spojení, kritické komponenty a kritické systémy kritického prvku dopravní infrastruktury [1,7,14], které vyžadují speciální práci s riziky při umísťování, výstavbě, konstrukci a provozu [7,14].

4 METODIKA PRÁCE S RIZIKY KRITICKÝCH PRVKŮ DOPRAVNÍ INFRASTRUKTURY

Na základě komplexní analýzy a kritického posouzení několika tisíc odborných prací a výsledků z praxe, jejichž výsledky jsou v pracích [1-5,7], je nutné při řešení problémů bezpečnosti kritických objektů použít systémový přístup (tj. zaměřit se na integrální riziko) a nejprve vybrat správný koncept práce s riziky (tj. kontext, v němž rizika sledujeme) a poté respektovat logický model práce s riziky. Klíčové koncepty inženýrství zaměřených na bezpečnost jsou:

- Přístupy jsou založené na riziku - intenzita prací a dokumentace je přiměřená úrovni rizika.
- Odborný přístup je založen na tom, že se zvažují jen kritické atributy kvality a kritické parametry procesu.
- Řešení problémů se orientuje na kritické položky – sledují a řídí se kritické aspekty technických systémů zajišťujících konzistenci operací systémů.
- Prověřené parametry kvality se objevují již v návrhu projektu.
- Důraz na kvalitní inženýrské postupy – musí se prokazovat správnost zvolených postupů v daných podmínkách.
- Zacílení na zvyšování bezpečnosti - neustále zlepšování procesů s využitím analýzy kořenových příčin poruch a selhání.

Snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, apod., a proto se v praxi hledá hranice, na kterou je únosné riziko snížit tak, aby vynaložené náklady byly ještě rozumné. Tato míra rizika (určitá optimalizace) je většinou předmětem vrcholového řízení a výsledkem politického rozhodování, při kterém je z hlediska zajištění rozvoje nutné, aby se využily současné vědecké a technické poznatky a zohlednily ekonomické, sociální a další podmínky.

Rizika byla, jsou a budou a neustále se budou objevovat nová. Řízení a vypořádání rizik, které způsobují pohromy, vyžaduje rozměr a měření rizika, které berou v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Většina technik na určování rizika nereprezentuje holistický přístup a nerespektuje, že riziko je rozdělené na lokální, regionální i státní úroveň [4].

Při práci s riziky si je třeba uvědomit, že úkolem řízení rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Základní principy při práci s riziky jsou: být proaktivní; domýšlet možné důsledky; správně určovat priority veřejného zájmu; myslet na zvládnutí problémů; zvažovat synergie; a být ostražitý.

Podle Mezinárodní organizace pro standardizaci (ISO) kvalifikované řízení rizik technického díla musí: být součástí systému řízení sledovaného technického díla; být součástí každého procesu rozhodování sledovaného technického díla; explicitně zvažovat nejistoty a neurčitosti v procesech a podmínkách sledovaného technického díla a jeho okolí; být systematické a strukturované; vycházet z nejlepších dostupných informací; být dynamické a vhodně reagovat na různé změny; být uzpůsobeno místním podmínkám a legislativním požadavkům; respektovat vliv člověka (lidský faktor) na technické dílo; a mít schopnost neustálého zlepšování.

Při výběru nástrojů pro práci s riziky kritických prvků dopravní infrastruktury zacílené na bezpečnost jsou dle argumentů shrnutých v práci [4] rozhodující dva faktory:

- Prvním faktorem je poznání, že riziko je veličina, která je místně specifická, tj. závisí jak na příčině poškození aktiva nebo souboru aktiv (tj. na charakteru a velikosti škodlivého jevu / pohromy), tak na vlastnostech aktiva či souboru aktiv (zranitelnosti) v momentě výskytu pohromy. Protože v čase jsou proměnné, jak stavy aktiv či souboru aktiv, tak i velikosti škodlivých jevů či pohrom, tak z pohledu zvládnutí dopadů realizovaného rizika existují tři kategorie situací, a to situace: normální; nouzová; a kritická. S rostoucí kategorií rostou odborné, finanční, organizační i personální nároky na řízení a vypořádání rizik spojených s těmito situacemi. Proto zde hraje velkou roli legislativa, která ukládá vlastníkům i provozovatelům kritických prvků dopravní infrastruktury požadavky na práci s riziky a veřejné správě požadavky na dozor nad bezpečností ve veřejném zájmu [4]. Na základě

analýz legislativy [4] je současná legislativa příliš obecná; neuvádí požadavky na data a na metody zpracování dat, které zásadně určují kvalitu výsledku [15]. Z hlediska úplnosti je třeba uvést, že v České republice je na dobré úrovni odezva na nouzové a krizové situace na základě zřízení a stálého zvyšování úrovně IZS (integrovaný záchranný systém - zákon č. 239/2000 Sb.) a jaderná bezpečnost, která je pod trvalým dohledem Mezinárodní agentury pro atomovou energii.

- Druhým faktorem je výběr typu rizika, který je třeba v řešené úloze sledovat, který závisí na určení: počtu aktiv a jejich vyjmenování, tj. jde o zvážení, která veřejná aktiva a která specifická aktiva kritického prvku dopravní infrastruktury v dané úloze jsou důležitá; např., zda jsou jimi i výkon, konkurenceschopnost, zisk aj.; a zda v dané úloze hrají roli vazby a toky mezi vyjmenovanými aktivy, tj. nestačí mechanický koncept, ale je třeba zvažovat systémový koncept.

Pro krátkodobé zajištění bezpečnosti kritického prvku dopravní infrastruktury (např. bezpečný stav jednoduchého technického zařízení), stačí sledovat stav aktiva, tj. dílčí riziko spojené s kritickým prvkem dopravní infrastruktury. S ohledem na bezpečí lidí legislativa ve vyspělých zemích požaduje sledovat také bezpečí osob na pracovišti (BOZP), tj. jde již o sledování dvou aktiv (životy a zdraví osob na pracovišti, kvalita pracovního prostředí), a to pomocí integrovaného rizika (tj. je zanedbána vazba stroj – člověk). Protože technická zařízení, osoby na pracovišti a pracovní prostředí jsou provázané, je třeba pro střednědobé a dlouhodobé zajištění bezpečnosti sledovat vazby a toky mezi uvedenými dílčími systémy, tj. integrální riziko.

Proto při výběru nástrojů pro práci s riziky (identifikace, analýza, hodnocení, posouzení, řízení a vypořádání) zacílenou na bezpečnost vybrané entity je třeba v technické oblasti v případě kritických prvků dopravní infrastruktury rozlišit následující úlohy výběr nástrojů pro práci s rizikem spojeným se stavem technického zařízení (cíl – bezpečné technické zařízení); výběr nástrojů pro práci s rizikem spojeným:

- se stavem technické komponenty (cíl – bezpečná technická komponenta),
- s výrobním procesem či provozem (cíl – bezpečný výrobní proces nebo provoz),
- se stavem souboru procesů v entitě (cíl – bezpečný soubor procesů v entitě),
- s celým technickým dílem, tj. v našem případě s kritickým prvkem dopravní infrastruktury (cíl – bezpečné technické dílo, tj. bezpečný kritický prvek dopravní infrastruktury),
- s kritickým prvkem dopravní infrastruktury a jeho okolím (cíl – bezpečný kritický prvek dopravní infrastruktury a jeho bezpečné okolí).

Na základě výsledků dosažených a shrnutých v pracích [1-14,16] nestačí při zajišťování bezpečnosti lidského systému v souvislosti s technickými díly a technologiemi (tj. koexistence technického díla s okolím během jeho provozu) jen orientace na technická díla a jejich zařízení, protože výběr nástrojů pro práci s riziky závisí na: charakteru sledované entity (tj. vybraného technického zařízení či vyšších systémů technického díla, tj. kritického prvku dopravní infrastruktury); charakteru prostředí, ve kterém sledovaná entita (tj. vybrané technické zařízení či vyšší systém technického díla) pracuje; režimu, v jakém sledovaná entita (tj. vybrané technické zařízení či vyšší systém technického díla, tj. kritického prvku dopravní infrastruktury) pracuje; požadavcích na provoz entity (tj. vybraného technického zařízení či vyšších systémů technického díla); také na tom, zda se požaduje řešení krátkodobé, střednědobé nebo strategické, tj. dlouhodobé.

Pokyny pro výběr vhodného nástroje pro jednotlivé úkoly jsou uvedeny v pracích [5,17]. Je faktem, že čím vyšší typ nástroje je použit, tak tím vyšší jsou náklady (znalosti, finance, čas) na jeho použití. Z výše uvedeného vyplývá, že pro zajištění bezpečnosti sledovaných kritických prvků dopravní infrastruktury je pro rozhodování o rizicích nutno použít systémy pro podporu rozhodování.

Pro rozhodování o řízení integrálního rizika složitých systémů, kterými prvky dopravní infrastruktury jsou, ve prospěch bezpečnosti se v praxi osvědčil systém pro podporu rozhodování (DSS) [4,5]. Výsledky, tj. DSS a stupnice pro hodnocení rizik jsou pro: mosty v práci [9]; tunely

v práci [10]; letiště v práci [11]; nádraží v práci [12]; řídící systémy dopravy v práci [13]; a pozemní komunikace v práci [8].

Hodnocení konkrétního případu, tj. hodnocení souboru očekávaných variant provozu kritického prvku dopravní infrastruktury dle příslušného DSS musí dělat tým specialistů z různých odborů nezávisle; v praxi se osvědčil tým [18,19], který je složený z pracovníka: veřejné správy odpovědného za bezpečnost území; veřejné správy odpovědného za dozor nad provozem kritického prvku dopravní infrastruktury; managementu kritického prvku dopravní infrastruktury, odpovědného za řízení rizik; odborné instituce pro posuzování bezpečnosti kritického prvku dopravní infrastruktury – např. z technické inspekce; a Integrovaného záchranného systému odpovědného za odezvu na havárie a selhání kritických prvků dopravní infrastruktury.

Principy roztřídění integrálního rizika do kategorií přijatelné, ALARP a nepřijatelné jsou detailně popsány v článku [16].

5 GENERICKÝ MODEL ŘÍZENÍ BEZPEČNOSTI KRITICKÝCH PRVKŮ DOPRAVNÍ INFASTRUKTURY

Kritické prvky dopravní infrastruktury jsou složité systémy typu systémy systémů, tj. jsou to otevřené vzájemně propojené systémy, jejichž povaha je socio-kyber-fyzická (technická) [7]. V Evropě k jejich řízení používáme způsob Total Quality Management (TQM) [3,20,21], který je základem ISO norem třídy 9000, 14000 a dalších. Přístup TQM spočívá v tom, že na procesu zlepšování kvality se musí podílet všichni zaměstnanci, od řadových zaměstnanců až po nejvyšší řídící pracovníky. Proces zlepšování jakosti vychází z impulsu podle potřeb od zákazníka / občana. TQM vychází z toho, že trvalá kvalita výrobků a služeb se nedá zajistit příkazy, kontrolou, dílčími programy, organizačními nebo ekonomickými opatřeními, ale cíleným hledáním, měřením a hodnocením příčin toho, proč se produktivita a kvalita nezvyšuje [21]. Je to způsob, při kterém se pozornost zaměřuje na procesy probíhající v instituci. Při implementaci TQM se přihlíží na specifika instituce, protože z důvodu účinnosti musí odpovídat struktuře instituce. TQM se využívá v řízení podniků (technických děl), obcí a regionů.

Z pohledu zajištění bezpečnosti sledovaných kritických prvků a jejich koexistence s okolím po celou dobu životnosti jde o určení velikosti příslušných rizik a jejich roztřídění do kategorií: přijatelné riziko; podmíněně přijatelné riziko, u kterého se navrhnou nutná opatření preventivní, zmírňující, reaktivní a obnovovací; a nepřijatelné riziko, u kterého se navrhne buď vyhnutí dané činnosti, je-li to možné, anebo další opatření v rámci krizového řízení, která vyžadují vyšší znalosti, vyšší technické vybavení, vyšší náklady, vyšší připravenost lidských zdrojů [4]. Proto musíme riziko selhání kritického prvku dopravní infrastruktury nejprve určit správnými nástroji.

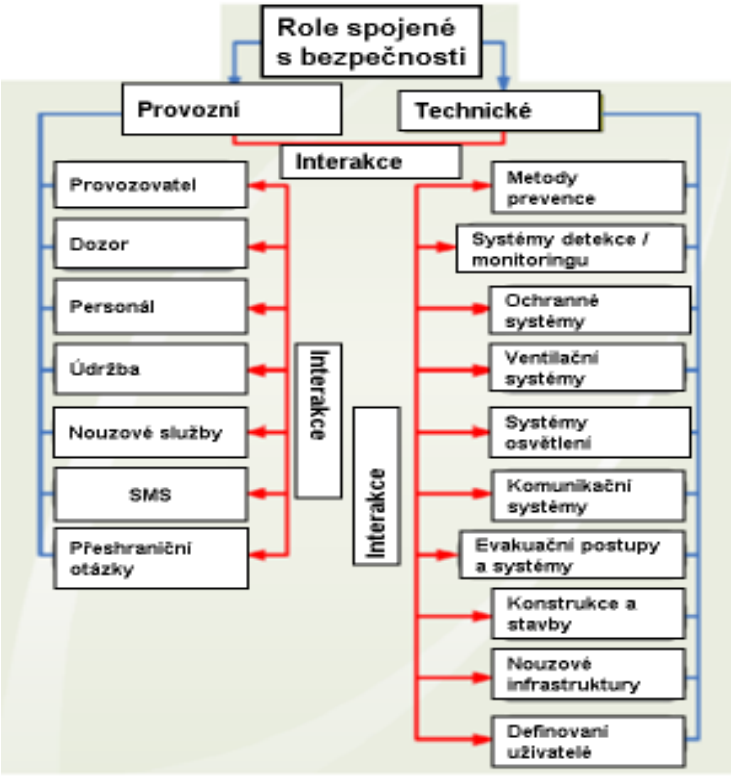
Abychom zajistili bezpečnost technických zařízení i technických děl, řešíme problém bezpečnosti systému systémů [5,7], protože soubor propojených bezpečných systémů není ještě nutně bezpečný systém, protože bezpečnost systému systémů závisí také na charakteru vzájemných propojení mezi systémy. Důsledkem vzájemných závislostí je to, že defekt v jedné části technického díla způsobí selhání dalších částí technického díla a kaskádu dalších dopadů. To znamená, že když chceme zajistit bezpečnost systému systémů, tak kromě bezpečnosti dílčích částí technického díla musíme ještě zvlášť sledovat soubor systémů jako celek. Musíme zjišťovat: typy selhání systému systémů; provozní podmínky systému systémů; vnitřní vazby a jejich projevy; a charakteristiky kritických stavů systému systémů.

Zvládání rizik v případě, že riziko není přijatelné, spočívá dle [1-7] ve výběru některé z dále uvedených alternativ: vyhnutí se riziku, tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika, když to jde (lidská společnost se může bez technického díla obejít); odstranění zdrojů rizik, tj. zabránění vzniku pohrom, když to jde (zvolit alternativu technického díla, která bude mít méně zdrojů rizik, anebo menší rizika); snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom, když to jde (aplikace zásad kultury bezpečnosti); snížení závažnosti dopadů rizika, tj. příprava zmírňujících opatření jako jsou varovací systémy, systémy odezvy a obnovy; sdílení rizika, tj. rozdělení rizika mezi zúčastněné a pojišťovny; a retence rizika.

Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá dle [1,3,4,7] v rozdělení rizik do kategorií, ve kterých se část rizika: sníží, tj. preventivními opatřeními se

Bratislava: Slovak Society for Environment • Edition ESE-61 • ISBN 978-80-973844-5-6

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 (Contingency plan).
K tomu se rovněž připojuje rozdělení zvládání rizik mezi všechny zúčastněné. Rozdělení ve správném řízení [3] se provádí tak, že se vychází z toho, že za zvládání rizik odpovídají všichni zúčastnění (od politiků přes pracovníky správy, vedení technických děl až po techniky a občany) a že zvládání konkrétního rizika se přiděluje tomu subjektu, který je na to nejlépe připraven; obrázek 4.

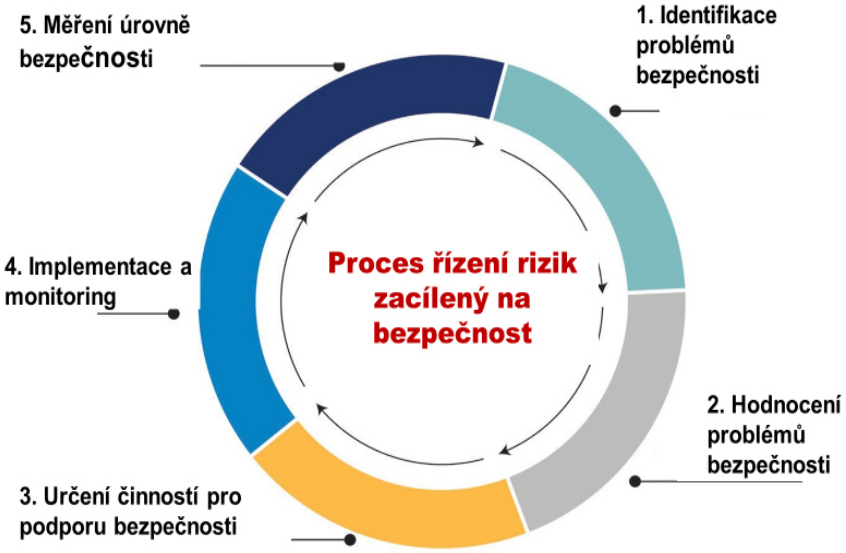


Obr. 4. Role zúčastněných spojené s bezpečností; SMS je systém řízení bezpečnosti celku (safety management systém).

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) kritického prvku musí obsahovat úkoly uvedené na obrázku 5.

Obr. 5. Úkoly uvedené v systému řízení bezpečnosti (SMS) kritického prvku.

Podle současných znalostí v souvislosti s bezpečností technického zařízení či technického díla, tj. i kritického prvku dopravní infrastruktury, je nutné při sestavování jeho konceptu, jeho umístění, projektování, zhotovení a provozu respektovat dále uvedený postup, který propojuje normy a výsledky řízení rizik ve prospěch bezpečnosti, tj. používat nástroje risk-based design, risk-based operation; risk-based inspections, risk-based maintenance atd. [6], které propojují normy a výsledky řízení rizik. Vlastní metodický proces řízení rizik ve prospěch bezpečnosti (řízení bezpečnosti) je zobrazen na obrázku 6.



Obr. 6. Řízení bezpečnosti kritické entity.

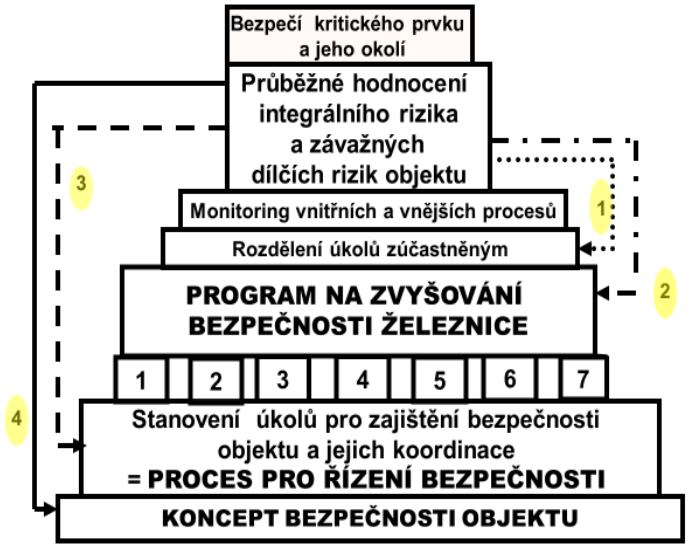
Bezpečnost i zabezpečení kritických prvky dopravní infrastruktury je zásadní pro ochranu a rozvoj lidí i státu, proto každý stát musí mít strategii na udržování a popř. i zvyšování bezpečnosti. Protože svět se dynamicky vyvíjí, tak mohou nastat podmínky, na které nejsou limity kritického prvku dopravní infrastruktury 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.

Minimalizování škod může mít podobu varovné a výstražné signalizace, výcviku, pokynů a procedur pro chování v nebezpečných situacích, nebo izolace nebezpečných zařízení od osídlených center. Opatření před nehodami včetně nouzového plánování musí být vypracováno ještě před tím, než je zařízení spuštěno do provozu. Při vzniku havárie by už na to nemuselo být dosti času [5].

Kritické prvky dopravní infrastruktury jsou složité socio-kyber-fyzické systémy s vysokým počtem mnoha různých propojení. Podle projektu všechny komponenty a propojení mají své limity, které jsou nastaveny na určité podmínky tak, aby společně plnily zadaný cíl (interoperabilita) [1,2]. Jelikož v důsledku dynamického vývoje světa se podmínky mění, tak se mění i podmínky pro interoperabilitu. Proto bezpečnost kritických prvků dopravní infrastruktury se mění v závislosti na podmínkách.

V souladu s požadavky OECD [22] a s výsledky pro technická díla [5,8-13,23,24], každý správce kritického prvku dopravní infrastruktury musí mít program pro řízení bezpečnosti kritického prvku dopravní infrastruktury, který je založen na řízení rizik, a to od projektování, přes výstavbu až po provoz [5,23]. Proto z důvodu důležitosti role kybernetické infrastruktury spojené s automatizovaným systémem řízení musí SMS také sledovat kybernetické zabezpečení; obrázek 7 [13].

Hlavním cílem zabezpečení kritického prvku dopravní infrastruktury při automatickém řízení je, aby instrukce pro systémy ovládací provoz kritického prvku dopravní infrastruktury byly jasné a přesné, tj. aby nebyly ovlivněny jevy, které je zkreslí.



Obr. 7. Model řízení bezpečnosti kritického prvku dopravní infrastruktury s automatizovaným řízením v čase [13]. Procesy: 1- koncepce a řízení; 2 - administrativní postupy; 3 - technické záležitosti; 4 - vnější spolupráce; 5 - nouzová připravenost; 6 - dokumentace a šetření havárií; 7- kybernetické zabezpečení. Zpětné vazby: 1-4.

6 DOKUMENTACE A ODPOVĚDNOST

Ze studia havárií a selhání technických zařízení a technických děl [5,23-25], tj. i kritických prvků dopravní infrastruktury [9-13] (*obecně entit*) vyplývá, že k těmto nežádaným jevům došlo v řadě případů kvůli nedostatečné dokumentaci procesů zobrazeným na obrázku 7 a nedostatečně určeným odpovědnostem. Proto řada nadnárodních institucí (EU, IAEA, IATA, ICAO, OECD atd.) i řada českých zákonů (263/2016 Sb., 224/2015 Sb., 181/2014 Sb. atd.) požaduje zpracování dokumentace ve formě bezpečnostní zprávy (safety report), což znamená, že jde o dokument podporující bezpečnost sledované entity. Předmětný dokument je určen pro řídící činnost provozovatele entity a pro potřebu příslušných orgánů veřejné správy (státní dozor) i pro informování veřejnosti. Jeho detailní popis je v práci [16].

V každé entitě rozlišujeme základní úrovně řízení, které je nutné sladit, a to: politická, strategická, taktická, operativní / funkční a technická [3]; detailní popis je v pracích [3,16].Podle vědecké teorie řízení TQM [20,21] a dle dosavadních zkušeností autorů je třeba v souvislosti s řešením problémů při stanovení rozdělení úkolů a odpovědností při zajišťování bezpečnosti brát v úvahu možnosti, které existují na jednotlivých úrovních řízení. Možnosti jsou totiž dané jak pravomocemi, tak dostupností a množstvím disponibilních zdrojů, sil a prostředků které jsou potřebné k řešení:

- na operativní úrovni managementu technického díla lze úspěšně řešit dobře strukturované problémy,
- na střední úrovni managementu technického díla lze úspěšně řešit strukturované i špatně strukturované problémy, které nejsou spojeny s velkými riziky pro technické dílo,
- na vrcholové úrovni řízení technického díla lze úspěšně řešit složité i nestrukturované problémy, která mají rizika, která lze ovládat za použití nástrojů, které má jen vrcholové řízení technického díla k dispozici,
- jen vzájemnou spoluprací veřejné správy a vrcholového managementu technického díla lze řešit složité i nestrukturované problémy velkého rozsahu s velkými riziky.

U technických děl nadnárodního dosahu je pak ještě nutná mezinárodní spolupráce.

7 ZÁVĚR

Ačkoliv koncept integrální bezpečnosti se rozšiřuje v praxi pomalu z důvodů uvedených v práci [26], 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. Generický model pro řízení bezpečnosti kritických prvků dopravní infrastruktury ukazuje způsob řízení rizik, aby se předešlo, anebo alespoň zmírnilo možným nežádoucím a nepřijatelným dopadům. Jde především o zajištění zvládnutí: slabin v zabezpečení vůči vnějším vlivům; výskytu vnitřních náhodných poruch systému; výskytu 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 stupnic, ohodnocení rizika neodpovědnosti, nekompetence, 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 infrastruktury s okolním prostředím jde o zabránění nepředvídatelným událostem a útokům: změna podmínek pro provoz ze strany státu; úmyslná poškození; a cílené útoky.

Acknowledgments - Poděkování:
Článek byl vypracován v rámci projektu TAČR CK01000095 Plán řízení rizik pro vybrané kritické objekty dopravní infrastruktury.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.
[2] PROCHÁZKOVÁ, D.*Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.
[3] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN 978-80-01-04844-3. Praha: ČVUT 2011, 483 p.
[4] PROCHÁZKOVÁ D. *Analýza, řízení a vypořádání rizik spojených s technickými díly.* ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. https://doi.org/10.14311%2FBK.9788001064801
[5] PROCHÁZKOVÁ, D., PROCHÁZKA, 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. https://doi.org/10.14311%2FBK.9788001066751
[6] 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. doi.org/10.14311/ BK.9788001069066.
[7] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364 p. https://doi.org/10.14311%2FBK.9788001061824
[8] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Rizika spojená s pozemními komunikacemi.* ISBN 978-80-01-06843-4. Praha: ČVUT 2021, 296 p., http://hdl.handle.net/10467/9 4283

[9] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Rizika a bezpečnost mostů. In: *Řízení rizik procesů a bezpečnost složitých technických děl*. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 107-179. http://hdl.handle.net/10467/91988; https://doi.org/10.14311/BK. 9788001067864

[10] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Rizika a bezpečnost tunelů na pozemních komunikacích. In: *Řízení rizik procesů a bezpečnost složitých technických děl*. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 268-318. http://hdl.handle.net/10467/91988; https://doi.org/10.14311/BK.9788001067864

[11] PROCHÁZKOVÁ D., PROCHÁZKA, J. Rizika spojená s leteckou dopravou. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 70-136. DSPACE. http://hdl.handle.net/10467/98461.doi.org/10.14311/ BK.97880 01069066.

[12] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Rizika spojená s kritickými vlakovými a autobusovými nádražími. *Soudní inženýrství.* ISSN 1211-443X. 32 (2021), 3, pp. 33-46.

[13] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. *Připraveno do tisku*.

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

[15] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Data a metodika jejich zpracování pro potřeby inženýrských disciplín*. ISBN: 978-80-01-05792-6. Praha: ČVUT 2015, 186 p.

[16] PROCHÁZKOVÁ D., PROCHÁZKA, J., MARTINCOVÁ, J. V., KERTIS, T. Návrhy opatření pro zvýšení bezpečnosti vybraných prvků dopravní kritické infrastruktury. In: *ExFoS 2000.* ISBN 978-80-214-6033-1. Brno: VUT 2022, pp. 343-386.

[17] PROCHAZKOVA, D., PROCHAZKA, J. Optimum Risk Engineering Tools Depend on Technical Facility Complexity. *International Journal of Computers,* ISSN 1998-4308.14 (2020), pp. 26-33. DOI: 10.46300/9108.2020.14.4

[18] OTA. *Public Law 92-484.*www.princeton.edu

[19] PROCHÁZKOVÁ, D. Nástroj pro sestavení podkladů pro řízení bezpečnosti. In: *Bezpečnost a ochrana zdraví při práci 2011*. ISBN 978-80-248-2424-6. Ostrava: VŠB 2011, pp. 157-169.

[20] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991.

[21] NENADÁL, J. TQM. *Role ekonomiky jakosti v koncepci TQM*. 1999, www: http://fmmi10.vsb.cz/639/ qmag/mj03-cz.htm.

[22] 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, 191 p.

[23] 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. https://doi.org/10.14311%2FBK.9788001066096

[24] 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, 114p. https://doi.org/10.14311%2FBK.9788001065273

[25] ČVUT. Archiv pohrom, havárií, selhání a práce s riziky. Praha: ČVUT 2022.

[26] PROCHÁZKOVÁ, D. Integral Safety. In: *Motivation – Education – Trust – Environment – Safety.* ISBN 978-80-973460-7-2. Bratislava: SSŽP et STRIX 2021, pp. 69-73.