Manažérstvo životného prostredia ♦ Management of Environment´2018
Recenzovaný zborník z XVIII. medzinárodnej vedeckej konferencie,26.-27.marec 2018,Bratislava
Proceedings of the 18th International Conference, Bratislava, March 26-27, 2018
Žilina: Strix et SSŽP. Edition ESE-41, ISBN 978-80-89753-25-3

VÝBĚR NEJLEPŠÍHO CÍLE ŘÍZENÍ RIZIK PRO TECHNICKÁ DÍLA

Dana PROCHÁZKOVÁ

CHOICE OF BEST AIM OF RISK MANAGEMENT FOR TECHNICAL FACILITIES

ABSTRAKT
RIZIKO JE FENOMÉN SOUČASNÉ DOBY. JE MÍSTNĚ SPECIFICKÉ A URČUJE SE Z VELIKOSTÍ MÍSTNÍCH OHROŽENÍ, KTERÁ VYTVÁŘÍ MOŽNÉ ŠKODLIVÉ JEVY (OBECNĚ POHROMY) V DANÉM MÍSTĚ S OHLEDEM NA MÍRY ZRANITELNOSTI MÍSTA VŮČI KONKRÉTNÍM MOŽNÝM POHROMÁM. PRO POTŘEBY PRAXE JE VYJÁDŘENO SOUHRNEM ZTRÁT, ŠKOD A ÚJMY NA SLEDOVANÝCH CHRÁNĚNÝCH AKTIVECH, KTERÝ SE ROZPOČÍTÁ NA URČITOU ČASOVOU JEDNOTKU (OBVYKLE 1 ROK) A VYBRANÉ ÚZEMÍ, PODNIK, MĚSTO ČI POČET LIDÍ. OBVYKLE PRO VĚTŠÍ NÁZORNOST SE VYJADŘUJE PENĚZI A POČTEM OBĚTÍ. JEHO ŘÍZENÍ U TECHNICKÝCH DĚL JE BUĎ ZACÍLENO NA SPOLEHLIVOST ČI na BEZPEČNOST. ČLÁNEK POROVNÁVÁ CÍLE ŘÍZENÍ RIZIK A UKAZUJE, ŽE PRO LIDSKOU SPOLEČNOST JE PŘÍNOSNĚJŠÍ APLIKOVAT CÍL „BEZPEČNOST“.

Klíčová slova: *pohromy; ohrožení; riziko; technické dílo; spolehlivost; bezpečnost; řízení technických děl.*

ABSTRACT
THE RISK IS THE PHENOMENON OF THE PRESENT TIME. IT IS LOCALLY SPECIFIC AND IT IS DETERMINED FROM THE LOCAL HAZARDS, THAT CREATE THE POTENTIAL HARMFUL PHENOMENA (GENERALLY DISASTERS) AT A GIVEN SITE WITH REGARD TO THE VULNERABILITY DEGREE OF THE SITE TO REAL POTENTIAL DISASTERS. FOR THE PRACTICE NEEDS, IT IS EXPRESSED AS THE SUM OF LOSSES, DAMAGES AND INJURIES TO THE PROTECTED ASSETS, WHICH IS SHARED TO A CERTAIN UNIT OF TIME (TYPICALLY 1 YEAR) AND SELECTED TERRITORIES, BUSINESS, CITY, OR NUMBER OF PEOPLE. TYPICALLY, FOR THE POINT IT IS EXPRESSED IN MONEY, AND THE NUMBER OF VICTIMS. ITS MANAGEMENT IN THE TECHNICAL FACILITIES IS EITHER FOCUS ON RELIABILITY OR SAFETY. THE PAPER COMPARES THE AIMS OF RISK MANAGEMENT AND IT SHOWS THAT FOR HUMAN SOCIETY IT IS MORE BENEFIT TO APPLY THE AIM “SAFETY”.

Key words: *disasters; hazard; risk; technical facility; reliability; safety; technical facilities management.*

1. ÚVOD

Předmětem sledování jsou technická díla, která vytváří člověk ke zlepšení kvality života. S rozvojem poznání roste výkon i složitost technických děl. Složitost technických děl je daná několika jejich rysy, jako: velký

rozměr; použití více technologií; složité funkční závislosti; velká interoperabilita; velký výkon; vysoká bezpečnost, tj. funkčnost a spolehlivost; i nízké ohrožení chráněných aktiv při podmínkách normálních, abnormálních i kritických [1]. Z uvedených rysů je zřejmé, že jejich řízení není jednoduché, protože požadavků je mnoho, nejsou souměřitelné a někdy jsou i konfliktní; základní požadavky jsou vyznačeny na obrázku 1 [2].
V současné praxi je pro řízení technických děl používán specifický model, nazývaný systém systému. Jde o ***soubor propojených systémů, které mají otevřenou architekturu***, tj. odlišné prvky se propojují tak dlouho, dokud splňují podmínky interoperability a požadavky uživatele [1-3]. Ačkoliv cíl celého technického díla je jasně dán, tak mezi jednotlivými podsystémy dochází ke konfliktům [4]. Řešení konfliktů znamená optimální vyřešení možných rizik, které jsou jejich příčinou. V oblasti strategického řízení [1,2,4] je riziko ***vyjádřeno souhrnem ztrát, škod a újmy na sledovaných chráněných zájmech, který se rozpočítá na určitou časovou jednotku (obvykle 1 rok) a na jistou jednotku území či jiné reprezentativní míry sledovaného útvaru*** *(podnik, město, počet lidí);* v praxi se často pro větší názornost vyjadřuje penězi.

V praxi se při řízení technického díla používají v současné době způsoby řízení rizik [4], které jsou založené na systémovém pojetí reality a na proaktivním přístupu. Odlišují se cílem řízení; jde o cíle: zajištění spolehlivého systému; zajištění zabezpečeného systému; a zajištění bezpečného systému. Podle souboru zvažovaných rizik a stanovených cílů řízení je řízení rizik u technických děl zacílené na:

- spolehlivé technické dílo, což je technické dílo, které bezchybně plní stanovené úkoly po stanovenou dobu za určitých podmínek,
- zabezpečené technické dílo, což je technické dílo, které bezchybně plní stanovené úkoly po stanovenou dobu za určitých podmínek a přitom je ochráněno proti všem vnitřním a vnějším pohromám, včetně lidského faktoru,
- bezpečné technické dílo, což je technické dílo, které bezchybně plní stanovené úkoly po stanovenou dobu za určitých podmínek, je ochráněno proti všem vnitřním a vnějším pohromám, včetně lidského faktoru, a ani při svých kritických podmínkách neohrozí sebe a své okolí.

Obr. 1 - Položky, které ovlivňují výkon technického díla.

Na základě současných znalostí literatury je zřejmé, že rizika byla, jsou a budou a že neustále se budou objevovat nová. Řízení rizika, 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. Riziko je funkcí pravděpodobnosti výskytu pohromy a velikosti jejích dopadů (závažnosti následků). Proto cílem celého procesu řízení rizik je nejen identifikovat pohromy, tj. zdroje rizika, a početnosti jejich výskytu, ale následně riziko také ohodnotit a použít účinné kroky k jeho eliminaci nebo snížení.

2. RIZIKO

Riziko je místně specifické a určuje se z velikostí místních ohrožení, která vytváří možné škodlivé jevy (obecně pohromy) v daném místě s ohledem na míry zranitelnosti místa vůči konkrétním možným pohromám [1,2,4]. Rozlišují se rizika dílčí, integrovaná a integrální [2].

Integrální (komplexní, systémové, celkové) riziko technického díla je dané vztahem

$$R(H) = \left[\sum_{i=1}^{n} A_i(H) Z_i(H) + \sum_{i=1}^{n} \int_0^T \int_S F(H, A_i, P_i, O, t) \mathrm{d}S\mathrm{d}t \right] \cdot \tau^{-1}$$

ve kterém je ohrožení spojené s danou pohromou v místě objektu; $\boldsymbol{A_i}$ jsou hodnoty sledovaných aktiv pro i = 1,2,…, n; $\boldsymbol{Z_i}$ jsou zranitelnosti aktiv pro i = 1,2,…, n; $\boldsymbol{F}$ je ztrátová funkce; $\boldsymbol{P_i}$ jsou pravděpodobnosti výskytu poškození aktiv pro i = 1,2,…, n – jde o podmíněné pravděpodobnosti; $\boldsymbol{O}$ zranitelnost ochranných opatření; $\boldsymbol{S}$ velikost sledovaného objektu; $\boldsymbol{t}$ je čas měřený od vzniku škodlivého jevu; $\boldsymbol{T}$ je čas, po který vznikají ztráty; a $\boldsymbol{\tau}$ je perioda opakování pohromy.

Integrální čili systémové riziko respektuje i vazby a toky mezi aktivy. Problém je, že neznáme tvar ztrátové funkce a že závislosti mezi aktivy jsou proměnné v čase a prostoru. Proto pro jeho určení nelze použít analytické funkce, ale specifické heuristické postupy, které se osvědčily v inženýrských disciplínách soustavně pracujících s riziky [2,4].

Obrázek 2 [2] ukazuje položky, které je nutno zvážit při určení věrohodné velikosti rizika.

Situaci v praxi ukazuje příklad uvedený v [2,5], ze kterého vyplývá, že doposud nejsou v praxi použity poznatky, které již o riziku byly shromážděny. V návaznosti na tento fakt, výsledky výzkumu v EU, uvedené v pracích [1,2], ukazují velmi mnoho nedostatků spojených s prací s riziky. Příčiny uvedených nedostatků v oblasti vrcholového řízení států byly identifikovány takto:

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

Obr. 2 - Položky, které ovlivňují výsledek práce s riziky technického díla.

Dle práce [4] na úrovni států chybí konkrétní požadavky na práci s riziky a spolupráce při zvládání rizik mezi veřejnou správou a vlastníky a provozovateli technických děl. Jasná specifikace požadavků na práci s riziky i spolupráce všech zúčastněných je nutná, protože:

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

Každé řízení rizik směřuje k jeho ovládání. Představuje kulturu, procesy a struktury zaměřené na efektivní řízení potenciálních příležitostí a možných nežádoucích důsledků. Je to interaktivní proces, který se skládá z kroků, které při zachování plánované postupnosti umožňují trvalé zkvalitnění rozhodnutí a tím i následné zlepšování výsledků uskutečňovaných procesů. Proto řízení rizik musí být integrální činností každé řídící praxe, bez ohledu na úroveň řízení.

Rámec řízení rizik technického díla jako systému dle [2] zahrnuje:

- Pochopení systému a jeho souvislostí. V oblasti vně systému je třeba sledovat především kulturní, politické, právní, finanční, technologické, ekonomické, přírodní a konkurenční aspekty prostředí. V oblasti vnitřní se jedná především o kvalitu zdrojů a znalostí (např. kapitál, čas, lidé, procesy, systémy a

technologie), informační systémy, informační toky a rozhodovací procesy (jak oficiální, tak neoficiální), vnitřní zainteresované strany, hodnoty, kultura a řídící struktura systému.

- Politiku řízení rizik. Politika řízení rizik určuje vazby mezi řízením rizik, cíli systému a dalšími politikami (je upřednostněna nebo je na posledním místě při rozhodování; jak se řeší konflikty; jaké metody řízení se používají; jaké nástroje podporují řízení rizik atd.).
- Integraci výsledků řízení rizik do řídících procesů. Aby řízení rizik bylo efektivní a účinné, musí být obsaženo ve všech směrnicích a realizačních procesech, které v systému probíhají. Patří do strategického plánování a do politiky rozvoje.
- Stanovení odpovědnosti za opatření a činnosti spojené s řízením rizik.
- Zdroje nutné pro řízení rizik včetně znalostí, dovedností, zkušeností a kompetencí.
- Stanovení mechanismů pro interní komunikaci a podávání zpráv o rizicích a jejich zvládání.
- Stanovení mechanismů pro externí komunikaci a podávání zpráv o rizicích a jejich zvládání.

Pro implementaci řízení rizik je dle současného poznání, shrnutého v pracích [1,2,4], nutné:

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

Kritéria pro posuzování rizik dle současného poznání, shrnutého v pracích [1,2,4], vychází z:

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

Snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, apod. 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 trvalého rozvoje nutné, aby se využily současné vědecké a technické poznatky a zohlednily ekonomické, sociální a další podmínky [2].

Vždy, když pracujeme s rizikem, ať ho řídíme nebo s ním vyjednáváme, a to v klasickém pojetí nebo v moderním pojetí zaměřeném na bezpečí a udržitelný rozvoj chráněných aktiv (u technických děl jak veřejných, tak vlastních), tak musíme respektovat, že hlavními znaky každého rizika jsou nejistota a neurčitost. Jejich příčiny dělíme dle údajů shrnutých v [2] na odchylky vznikající při průběhu děje, který je:

- obvyklý za normálních podmínek systému, kdy vznikají jen malé variace (zdroj nejistot),
- skutečný, kdy vznikají příležitostné změny procesu v systému, které vedou k výskytu příležitostných extrémních hodnot (zdroj nejistot a příležitostných neurčitosti),
- proměnný, kdy vznikají velké změny procesu v systému, např. způsobené vnějšími příčinami a různými typy útoků zdroj neurčitostí).

Náhodná nejistota souvisí s rozptylem pozorování a měření. Lze ji do hodnocení a predikce zapracovat pomocí aparátu matematické statistiky. Neurčitost souvisí jak s nedostatkem znalostí a informací o procesu, tak s přirozenou variabilitou procesů a dějů, které vyvolávají pohromy nebo dokonce hrubými chybami. Pro zapracování a zvážení neurčitostí je aparát matematické statistiky nedostatečný, a je třeba používat jiný, modernější matematický aparát, který poskytují např. teorie extrémních hodnot, teorie mlhavých množin, teorie fraktálů, teorie dynamického chaosu, vybrané expertní metody a vhodné heuristiky [6].

Neurčitost dat vyplývá ze skutečnosti, že data jsou neúplná, nehomogenní (tj. jejich přesnost závisí na jejich velikosti nebo na čase výskytu) a nestacionární, tj. data mají značný rozptyl a jsou zatížená náhodnými a někdy i systematickými chybami, jejichž funkce rozdělení obvykle není možno stanovit. Protože není nic absolutně přesného, tak obecně u každé veličiny, kterou zkoumáme, musíme zvažovat nejistoty a neurčitosti dat. Proto inženýrství zacílené na řízení rizik, anebo řízení bezpečnosti vyžadují, aby se při řešení úkolů ověřovala kvalita datových souborů z hlediska jejich věrohodnosti s ohledem na daný úkol.

Rizika vstupují do veřejné oblasti, naplňují-li některý z dále uvedených atributů:
- Jde o externality, které nemohou řešit tržní mechanizmy.
- V souvislosti s individuálními právy jsou občanům vnucovány škodlivé dopady.
- Je ohrožena značná část veřejnosti.
- Politické rozhodnutí vyvolá událost, při které dojde k realizaci rizika.
- Nežádoucí události (pohromy), tj. jevy, při kterých se realizují nepřijatelná rizika, jsou rozloženy tak, že neberou ohled na politickou spravedlivost.

Pro zajištění základních funkcí státu, veřejná správa musí zajistit, že rizika jsou analyzována nejen z hlediska společenských dopadů, nýbrž také z hlediska dopadů na systém řízení veřejné správy [4]. Může se totiž stát, že rozhodování veřejné správy může dopady nouzové situace ještě zhoršit. Kroky postupu řízení rizik veřejné správy se liší od běžného postupu řízení organizačního celku jen tím, že se musí věnovat značná pozornost formulaci kontextu a musí se řídit rizika ze strategických a procesních hledisek [2,4].

Nicméně je třeba vzít v úvahu, že v současné době existují 3 vyhraněné koncepty, které pracují s riziky:
- řízení a inženýrství spolehlivosti (reliability management and engineering), kde řízení rizik u technických děl je zacílené na spolehlivost technických děl, např. [7],
- řízení a inženýrství zabezpečení / bezpečnostní (security management and engineering), kde řízení rizik technických děl je zacílené na zabezpečené technické dílo, např. [8],
- řízení a inženýrství bezpečnosti (safety management and engineering), kde řízení rizik je zacílené na bezpečné technické dílo, např. [9].
- Všechny tři uvedené koncepty používají stejné postupy, metody, nástroje i techniky [4]. Praxe ukazuje, že mezi nimi jsou občas konflikty – např.:
- při požáru objektu v Chicagu, který byl dobře zabezpečený, lidé v objektu uhořeli, protože se z objektu zachváceného požárem nedostali,
- dobře zabezpečená pilotní kabina umožnila Andreasovi navést letadlo Germanwings, plné lidí do svahu Alp a usmrtit je, protože nemocný člověk se uzavřel v pilotní kabině, a tím neumožnil kapitánovi letadla incidentu zabránit,
- gilotina je na základě fyzikálních zákonů spolehlivý systém, ale z pohledu současného chápaní bezpečnosti [1,10,11] není bezpečný systém, jelikož způsobuje ztrátu života člověka apod.,
- most v Janově byl podle provozovatele spolehlivý (legislativy mnoha zemí jsou dosud založeny jen na spolehlivosti) [12], ale zřítil se, tj. nebyl bezpečný, protože nevydržel reálné podmínky.
- Poznatky z praxe dle údajů shrnutých v práci [4] ukazují, že v řadě případů technických děl opatření na zajištění bezpečnosti se výrazně liší (někdy jsou dokonce konfliktní) při aplikaci inženýrství spolehlivosti od těch, které stanovuje aplikace inženýrství bezpečnosti.

3. SPOLEHLIVOST

Prvním důležitým aspektem spojeným s technickým dílem je volba samotného konceptu pro konstrukci a provoz technického díla. Velmi dlouho se za základ bezpečných technických děl považovala teorie spolehlivosti, jejímž zakladatelem byl v r. 1816 pan Samuel T. Coleridge. Její velký rozvoj nastal ve 40. letech minulého století, hlavně v USA při velkém rozvoji průmyslu.
Spolehlivost (ve smyslu reliability) je schopnost systému bezchybně dodržovat stanovené požadavky po stanovenou dobu za určitých podmínek. Provozní spolehlivost systému (ve smyslu dependability) znamená, že systém (objekt, zařízení) plní stanovené požadavky a že jeho provoz vyhovuje stanoveným podmínkám.

Tato souhrnná vlastnost je pro analytické účely nepraktická, a proto se rozkládá do dvou základních vlastností, kterými jsou zranitelnost a odolnost. Provozní spolehlivost je důležitá u složitých objektů, jejichž systémy hrají klíčovou roli v obslužnosti společnosti, protože ovlivňují rozhodovací cyklus veřejné správy a politickou a sociální soudržnost a napomáhají v odstraňování fyzických a psychických škod, jsou nejen velmi složité, ale i zranitelné [1].
Dle údajů shromážděných v práci [4] u běžných technických zařízení a objektů se prokazuje schopnost bezchybné funkčnosti na stoleté pohromy; u důležitých mostů, přehrad pro tisícileté pohromy; a u jaderných zařízení na deseti tisícileté pohromy (pozn. úložiště aktivního plutonia vyžadují prokázání odolnosti na sto tisíciletou pohromu). Různé prahové hodnoty jsou stanoveny tak, aby zajistily provozuschopnost po celou dobu předpokládané životnosti. Dosavadní řešení jsou prováděná na základě dobré inženýrské praxe a jejich dlouhodobá bezpečnost a spolehlivost se těžko prokazuje.
Spolehlivostní inženýrství (přesněji inženýrství spolehlivosti) se přednostně zabývá chybami a redukováním četnosti jejich výskytu. Spolehlivost je definovaná jako charakteristika daného objektu, která je vyjádřená pomocí pravděpodobnosti, že sledovaný objekt bude vykonávat specifikovaným způsobem funkce, které jsou na něm požadovány během stanoveného časového intervalu a za stanovených resp. předpokládaných podmínek.
Teorie spolehlivosti je matematická disciplína, která se zabývá mírou selhávání prostředků nebo systémů, od kterých se očekává nějaká funkčnost nebo odolnost vůči vnějším vlivům, a rychlostí zotavení z jejich poruchových stavů. V hierarchii matematických odvětví patří pod aplikovanou statistiku. Pomocí nástrojů teorie spolehlivosti se vyčíslují parametry poruch, jako např. provozní bezpečnost nebo spolehlivost, především těch zařízení, jejichž nečinnost nebo nesprávná činnost jsou z nějakého důvodu vysoce nežádoucí.

4. BEZPEČNOST

Bezpečnost, chápaná jako soubor opatření a činností zajišťujících bezpečí a udržitelný rozvoj lidského systému či jiné entity, tj. i technického díla [1,4] (tj. soubor opatření a činností, který omezuje podmínky vzniku nebezpečí), vytváří lidé, kteří by se měli starat nejen o přežití, moc, sociální shodu a prevenci škod, ale měli by vyřešit následující metodicko-konceptuální problémy:

- Neuvažovat bezpečnost v kulturní izolaci, protože tak se bezpečnost stává sebe referenční. Bezpečnost se musí formovat pod vlivem apriorně definovaných rizik.
- V bezpečnostních studiích je třeba oprostit koncept bezpečnosti od ideologického a politického klišé.
- V metodice řízení bezpečnosti je třeba dát důraz na rozhodování o řešení problémů a na zvažování přínosů a dopadů konkrétních rozhodnutí, a to z pohledu veřejného zájmu.
- Stále mít na paměti vztah mezi rizikem a bezpečnosti; obecně nejde o komplementární veličiny [1,2,4,15]. Podstata problému je v odpovědích na otázky: Jak se identifikují rizika a jejich škodlivé dopady? Odpověď: Stanovují se věrohodnými scénáři. Ale jak se takový věrohodný scénář tvoří? Obvykle se scénář odkazuje na minulé události a jevy, a nebere v úvahu porušování pravidel a pátrání po možných překvapeních.
- Moderní stát hraje roli, která se dá popsat v termínech řízení rizik, protože přerozděluje určité typy rizik prostřednictvím systému blahobytu / veřejného blaha a zdravotní péče [4]. Rostoucí debaty o riziku na úrovni veřejné správy je možné vysvětlit jako důsledek uvědomění rizik, kvůli nimž může selhat poskytování veřejných služeb. Nadto veřejnost se může při špatně zvládaných krizových a nouzových situacích domnívat, že veřejná správa je zdrojem rizik.

Integrální bezpečnost technického díla [1], vycházející z dokumentu OSN [11], je bezpečnost systému jako celku, tj. je založena i na řízení rizik spojených s rozhraními mezi komponentami. Bezpečnost technických děl není proto jen záležitost technická, je směsicí aspektů zabezpečení a spolehlivosti a vysoce souvisí s provozní spolehlivostí technického systému. ***Bezpečnost systému*** je vlastnost systému, která zajišťuje, že ani za kritických podmínek systém neohrozí sebe, ani své okolí.
Zajištění bezpečného systému je výsledkem fungování procesu řízení bezpečnosti (uspořádaného souboru opatření a činností), který je souborem procesů, jež mají pod kontrolou všechny faktory, které by mohly vést ke vzniku škody, ztráty či újmy na systému a jeho okolí. Ze systémového hlediska [2] se bezpečnost skládá z následujících komponent:

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

5. SPOLEHLIVOST VERSUS BEZPEČNOST

Již v r. 1978 Barry Turner [13] na základě analýz havárií technických děl vyslovil myšlenku, že složitost systému, kterým je technické dílo, zabraňuje stanovit všechna rizika, která mohou poškodit technické dílo a jeho okolí. Předmětný poznatek rozpracoval a potvrdil Charles Perrow na základě důkladné analýzy jaderné havárie Three Mile Island [10] a také závěry EU v r. 1981, které vedly k vydání direktivy SEVESO [14].
Předmětné poznání pochopitelně narušilo hegemonii teorie spolehlivosti a vzniklo soupeření mezi oběma směry, na které poukázal Scot Sagan [16]. Do dnešního dne dohady mezi zástupci inženýrství spolehlivosti a inženýrství bezpečnosti pokračují. Spolehlivostní inženýři věří, že haváriím může být zabráněno dobrým organizačním projektem a řízením (tj. jde o přístup založený na vysoké spolehlivosti). Předmětný přístup dle údajů shromážděných v [4] tvrdí:

- bezpečnost je primárně organizační cíl; zálohování zvyšuje bezpečnost, protože duplikace a překrytí zajistí, že spolehlivý systém nemá nespolehlivé části,
- decentralizované rozhodování dovoluje promptní a flexibilní odezvy na překvapení,
- kultura spolehlivosti zvyšuje bezpečnost podpořením jednotné aktivity obsluhy, protože vyžaduje striktní organizace činností; kontinuální akce, výcvik a simulace vytváří a udržují vysokou úroveň spolehlivosti systému,
- testy a poučení z havárií jsou efektivní a mohou být doplňovány předtuchami a simulacemi.
- Spolehlivostní inženýři často považují spolehlivost a bezpečnost za synonyma. To je pravda jen v některých speciálních případech. Všeobecně má bezpečnost širší / vyšší význam a je pravda, že spolehlivost a bezpečnost mají mnoho společných vlastností [1,4].
- Inženýři prosazující řízení rizik ve prospěch bezpečnosti [1,8-10,14] tvrdí, že u složitých technických děl jsou havárie a selhání nevyhnutelné a že zálohování často zvyšuje složitost systému. Údaje shromážděné v [15] ukazují, že:
- mnohé havárie nastaly bez toho, že by selhala nějaká komponenta. Právě naopak, častokrát všechny komponenty při haváriích fungovaly podle očekávání a bezchybně,
- jindy se stalo, že komponenty selhaly (měly poruchu) a přitom nedošlo k havárii,
- havárie a nehody mohou být zapříčiněny provozem zařízení mimo povolené rozsahy hodnot parametrů nebo časových limitů, z kterých vycházely analýzy bezpečnosti či analýzy spolehlivosti. To znamená, že systém může mít vysokou spolehlivost a přece může dojít k havárii. Navíc, generalizované pravděpodobnosti a analýzy spolehlivosti se nemohou přímo aplikovat na specifické, anebo lokální podmínky. Nejdůležitější je, že havárie a nehody mnohdy nejsou výsledkem jednoduchých kombinací chyb (selhání) komponentů [1,15].

Spolehlivost technického díla je definovaná jako charakteristika daného technického díla, která je vyjádřená pomocí pravděpodobnosti, že sledované technické dílo bude vykonávat specifikovaným způsobem funkce, které jsou na něm požadovány během stanoveného časového intervalu a za stanovených resp. předpokládaných podmínek.
Jakmile přijmeme fakt, že technická díla jsou systémy systemů, na jejichž tvorbě a provozu se podílí člověk a jeho finance, tak se objeví zcela nové problémy, protože musíme zvažovat záměr investora a otázky právní, finanční, pojišťovací, organizační, politické a sociální, přírodní a jistě i nějaké další. Proto v souladu s [1,4] platí, že problém je však v tomto rozšířeném pojímání složitější, neboť se nedá jednoduše abstrahovat do matematických, matematicko-statistických a pravděpodobnostních řešení vyúsťujících do soustavy

součinitelů spolehlivosti, do návrhových pravděpodobností poruchy nebo jiných veličin, se kterými pracujeme při navrhování stavebních konstrukcí. Když připočteme ještě korupci, tak daným způsobem bezpečnost zajistíme jen výjimečně. Proto musíme aplikovat metody inženýrských disciplín pracujících s riziky zacílené na integrální (systémovou, komplexní) bezpečnost a reálné možnosti lidí.

Bezpečnost v současném pojetí má cíle vyšší, tj. technické dílo musí nejen plnit řádně své funkce po dobu životnosti, ale ani za kritických podmínek nesmí ohrozit sebe a své okolí [1,14,15]. Právě tento fakt upřednostňuje řízení bezpečnosti. Navíc koncept integrální bezpečnosti řeší konflikty proaktivně, od počátku projektu a uplatňuje princip předběžné opatrnosti [1,4]. Podle něho řídicí systém sledovaného technického díla musí udržovat určené fyzikální veličiny (parametry dílčích systémů) na předem určených hodnotách. 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 dle [4] 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 [4,15].

Na základě současného poznání není tudíž možné, aby spolehlivostní inženýrství nahrazovalo systém řízení bezpečnosti, může ho ale doplnit. Musí to však být provedeno s jasným vědomím, že konečným cílem je zvýšení odolnosti systému vůči nebezpečím spojeným s výskytem náhodných chyb. Je vždy lepší, když se zařízení (systém) navrhuje tak, že individuálně náhodné chyby nemohou způsobit havárii, i kdyby se vyskytly (např. princip zabudovaný do ovládání zařízení – nemůžeš splnit úkon v požadované kvalitě, neproveď ho; nemůžeš splnit úkon v požadované kvalitě, informuj a nastartuj odezvu); je si však třeba uvědomit, že to není vždy možné. Velké opatrnosti je třeba při aplikování technik odhadování spolehlivosti pro posuzování bezpečnosti [10]. Pokud nejsou havárie nevyhnutelně zapříčiněné událostmi, které se dají vyjádřit pravděpodobnostmi, nelze pro ně všeobecně používat míry pravděpodobnosti rizika. Odhady pravděpodobnosti měří pravděpodobnost náhodných chyb a ne rizik a nehod anebo havárií. Když se při analýzách systému řízení bezpečnosti najde projektová chyba, je daleko účinnější ji odstranit, než někoho přesvědčovat pomocí vypočítaných pravděpodobností, že tato chyba nikdy nezpůsobí havárii. Nízké hodnoty pravděpodobnosti výskytu havárie nezaručují bezpečnost a bezpečnost nevyžaduje mnohdy ultra vysokou spolehlivost zařízení.

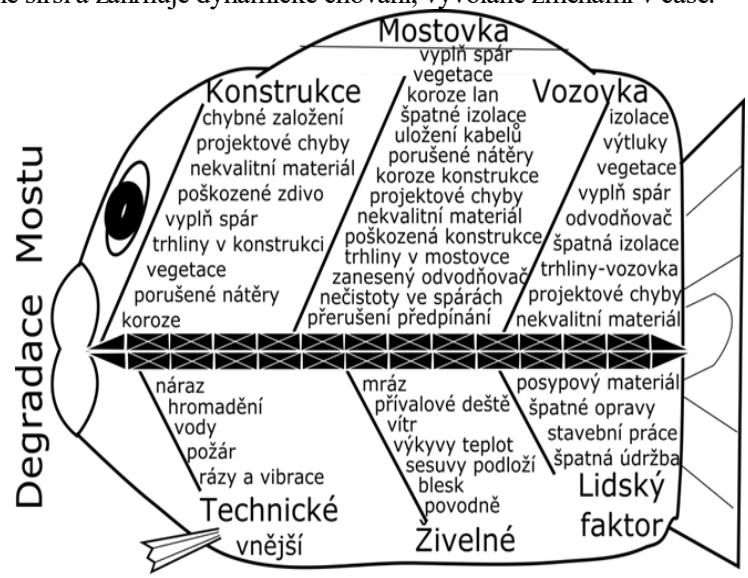
Hlavním nedostatkem pravděpodobnostních modelů nejčastěji není to, co zahrnují, ale to, co nezahrnují. Nízké hodnoty pravděpodobnosti jednoduše hovoří o tom, že systém neselže uvažovaným způsobem, ale naopak, selže s daleko vyšší pravděpodobností způsobem, o kterém uvažováno nebylo. Odlišování rizika nehody od chyb je podstatné pro to, abychom porozuměli rozdílu mezi bezpečností a spolehlivostí.
Je třeba si uvědomit, že integrální (systémová) bezpečnost a provozní bezpečnost nejsou u technických děl totéž. Provozní bezpečnost technických děl, tj. ***technická bezpečnost***, je směsicí aspektů bezpečí a spolehlivosti a vyjadřuje se pomocí ***provozní spolehlivosti*** technického díla [2,4,15], která se popisuje

zkratkami ***RAMS*** (Reliability, Availability, Mantainability, Security) nebo ***ARSS*** (Availability, Reliability, Safety, Security), přičemž platí:

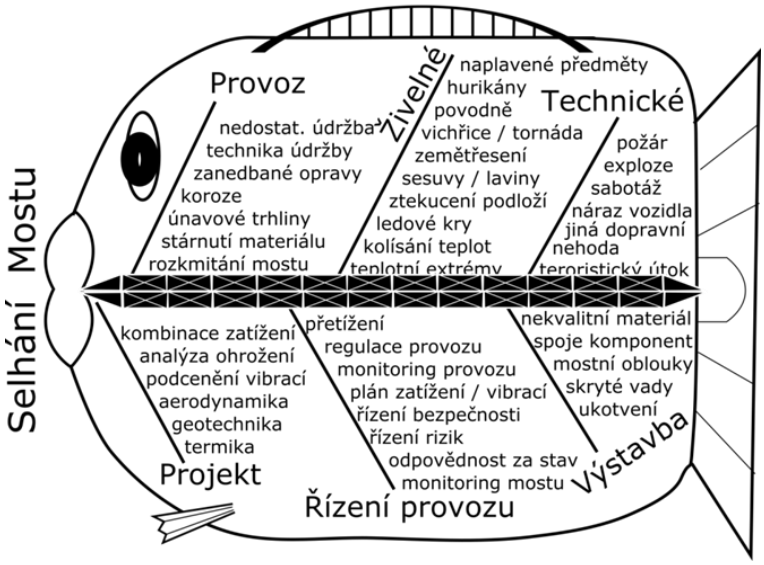
- Availability (***dostupnost***) je schopnost systému poskytovat služby, když se požadují.
- Reliability (***spolehlivost***) je schopnost systému fungovat tak, je zamýšleno, tj. plnit úkoly tak, jak mu byly předepsány.
- Safety (***bezpečnost***) je schopnost systému fungovat tak, že nepůsobí škodlivě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

Z pohledu lidí, tj. veřejného zájmu zahrnutého v konceptu OSN [11], je správné se soustředit u technických děl na řízení integrální bezpečnosti.

Na závěr pro pochopení problematiky ukážeme dva diagramy rybí kosti, které ukazují zdroje rizik sledované při řízení spolehlivosti mostů, obrázek 3, a při řízení bezpečnosti mostů, obrázek 4; převzaté z práce [17]. Vidíme, že zdroje sledovaných rizik nejsou totožné a že u řízení rizik, které je zacílené na bezpečnost mostů je soubor rizik podstatně širší a zahrnuje dynamické chování, vyvolané změnami v čase.



Obr. 3 - Zdroje rizik sledované při řízení spolehlivosti mostů [17].



Obr. 4 - Zdroje rizik sledované při řízení bezpečnosti mostů [17].

6. POZNATKY PRO ŘÍZENÍ BEZPEČNOSTI TECHNICKÝCH DĚL

Podle prací [1,4,18] mají rozhodující vliv na bezpečnost technických děl a bezpečnost entit obecně, následující faktory: odpovědná autonomie; adaptabilita, celistvost; a smysluplnost úkolů. 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, tj. v daném případě technická díla, charakterizují *strukturou, hardwarem, procedurami, prostředím*, t*oky informací, organizací* (problém organizačních havárií – [2,19,20]) a *rozhraním mezi uvedenými položkami.*

Na základě současného poznání shrnutého v pracích [1,4] orientace na bezpečnost musí být součástí systému řízení technického díla při respektování omezení reálného světa. V praxi to znamená zvažovat:

- technické dílo jako kombinaci lidí, postupů a zařízení, které jsou integrované tak, aby se prováděl specifický provozní úkol nebo funkce ve specifickém prostředí,
- koncept bezpečnosti systému jako aplikaci speciálních technických a organizačních dovedností s cílem systematicky předcházet identifikací ohrožení a řízením rizik a škodám a ztrátám na aktivech lidského systému s nimi spojených, a to během celé životnosti každého zařízení vytvořeného a realizovaného člověkem,
- bezpečnost kybernetických nástrojů použitých v systémech řízení.

Pro dosažení určité optimální bezpečnosti technických děl, je nutné řízení bezpečnosti, které je povahy multidisciplinární a interdisciplinární, které chápe vnitřní závislosti, tzv. interdependences, a umí se s nimi vypořádat. Nezbytným předpokladem je používání systémového myšlení. Z teoretického pohledu [1,4] je třeba:

- Vytvořit popis a charakteristiku technického díla chápaného jako systém systémů, který má jak veřejná aktiva, tak aktiva systému samotného (jimiž jsou dobrý stav dílčích prvků, spolehlivost a správná funkčnost dílčích systémů i celého systému), mezi kterými existují vnitřní vazby.
- Určit závažná rizika (v systému je více chráněných aktiv, které jsou propojené vnitřními vazbami) pro zdroje rizik uvnitř i vně systému.
- Stanovit kritéria pro integrální bezpečnost systému systémů.
- Stanovit pojmy a základy komunikace pro multidisciplinární a mezioborovou spolupráci při zajišťování bezpečnosti systému systémů.
- Stanovit zásady pro řízení bezpečnosti systému systémů.
- Stanovit legislativu pro podporu řízení bezpečnosti systému systémů.
- Vytvořit kontrolní mechanismy pro monitorování bezpečnosti systému systémů.

Bezpečnost je záležitostí všech zúčastněných. Proto se v praxi používají tzv. ***zlatá pravidla všech zúčastněných*** [21]; jde o budování kultury bezpečnosti zahrnující i motivaci lidí pracovat bezpečně. V dané souvislosti je ***bezpečnost technického díla*** vlastnost technického díla, která je nadřazena spolehlivosti [4]. Proto jsou parametry technického díla, které určují kvalitu technického díla jako systému systémů, uspořádány do pořadí:

- *bezpečnost,* tj. schopnost technického díla předcházet kritickým stavům technického díla (aktivní bezpečnost využívá prvky řízení; pasivní bezpečnost využívá ochranné prvky) a při jejich výskytu neohrozit existenci ani sebe, ani svého okolí,
- *spolehlivost,* tj. schopnost technického díla poskytovat požadované funkce za daných podmínek, v dané kvalitě a v daném časovém intervalu,
- *dostupnost,* tj. schopnost technického díla poskytovat požadované funkce při výskytu procesu, který danou funkci využívá,
- *integrita,* tj. schopnost technického díla poskytovat časově korektní a platná hlášení uživatelům o poruchách technického díla,
- *kontinuita*, tj. schopnost technického díla poskytovat požadované funkce bez přerušení během vyvolání procesu,

- *přesnost,* tj. schopnost technického díla zajistit požadované chování technického díla v požadovaném rozmezí.

Z důvodů složitosti technických děl jsou u nich typické vzájemné závislosti, které mají povahu fyzickou, kybernetickou, logickou a územní [1,4,15]. V důsledku závislosti dochází ke spřažením trvalým nebo dočasným jen za jistých podmínek. Předmětná spřažení jsou příčinou průřezových rizik, která se realizují jen za jistých podmínek a vedou ke kaskádovitým jevům, neočekávaným jevům, které působí významné ztráty a škody jak na aktivech technického díla, tak na okolí, tj. veřejných aktivech. Ve složitých systémech, kterými jsou výkonná technická díla, je možné velké množství kombinací procesů, a proto nejsme schopni stanovit všechny možné scénáře jejich havárií. Nerozluštitelnost chování technického díla spočívá v tom, že systémy: jsou vystaveny skrytým propojením, která mohou neutralizovat zálohování, spojky, firewalls, a tím vytvořit situace, pro které inženýři nepřipravili rozumný postup. Kaskádová selhání mohou akcelerovat ztrátu kontroly, zmást obsluhu a odepřít možnost obnovy normálního režimu [1,4].

Proto na základě současného poznání je třeba počítat jak s proměnnou technických děl v čase, tak s dynamickým vývojem okolí technických děl, což znamená i proměnu vzájemných vztahů technických děl a jejich okolí. Proto cíl zajistit bezpečné technické dílo znamená řídit integrální bezpečnost pomocí zacíleného řízení rizik, a to na několika úrovních: technické, funkční / operativní, taktické, strategické i politické [4]. Je zřejmé, že kvalifikované řízení na úrovních technické až strategické musí provádět systémoví inženýři, kteří nemusí být experty na všechny aspekty systému, ale musí rozumět podsystémům a různým jevům v nich natolik, aby byli schopni popsat a modelovat jejich charakteristiky, pochopit rizika, jejich zdroje a dopady a včasnými zásahy zabránit škodám a ztrátě konkurenceschopnosti technického díla. Žádoucí je spolupráce inženýrů ze všech zúčastněných oborů [1,4,15,21], která však v ČR chybí, jak ukazují závěry šetření provedených v podnicích [5].

Podle úvah současných filosofů, rizika ve společnosti mají svoji objektivní i subjektivní stránku, navíc nestojí mimo kulturní a hodnotové souvislosti (nejsou v tomto směru ani „čistě vědeckým“ problémem a zasluhují pozornost i z hlediska občanské participace). I když moderní společnost uplatňuje onu pohodlnou strategii pojištění a odškodnění, nelze na ni plně spoléhat, neboť některá rizika jsou schopna zasáhnout podstatu sociálního systému lidské společnosti, což platí pro některá rizika, která mohou významně poškodit bezpečnost technických děl.

Je si třeba uvědomit, že riziko není komplementární veličinou k bezpečnosti. Lze zavést organizační opatření, např. systémy varování, organizační resilienci apod., kterými lze zvýšit bezpečnost, i když velikost rizika se nesníží [4]. Komplementární veličinou k bezpečnosti technického díla je kritičnost technického díla (C), chápaná jako míra, s jakou může dojít v souvislosti s činností sledovaného technického díla k úrazu osob, zničení materiálu, škodě či jiným velkým ztrátám. Platí vztah:

$$\boldsymbol{C = S * O * B}$$

ve kterém ***S*** je závažn*ost největšího dopadu dané pohromy;* ***O*** pravděpodobnost výskytu pohromy; a ***B*** je podmíněná pravděpodobnost, že se při dané pohromě vyskytne nejzávažnější dopad. Kritičnost označuje určitou prahovou hodnotu pro sledovaný objekt. Jsou-li její hodnoty pod tímto prahem, tak je stav žádoucí a opačně. Ve světě existuje řada standardů, které upravují řízení zvyšování bezpečnosti či snižování kritičnosti [4].
Dle současného poznání, má v technických dílech zásadní význam kultura bezpečnosti, která souvisí s organizační kulturou. Jde o soubor dohodnutých pravidel uplatňovaných v řízení technického díla pro vytváření norem institucionálního chování. Znamená správné aplikování znalostí, přemýšlení a správné reakce na reálné situace. Nejde totiž jenom o dodržování norem a předpisů zacílených na spolehlivost našich opatření a činností, protože tím můžeme přehlédnout jevy, které normy a předpisy nevidí. Jde o chování založené na řízení znalostí [22].

7. ZÁVĚR

Na základě analýzy havárií je třeba konstatovat, že u technických děl je bezpečnost nadřazená spolehlivosti. Bezpečnost technických děl z hlediska provozovatele technického díla má tři cíle z hlediska veřejného zájmu [4]. Prvním cílem je zajistit provozní spolehlivost (dependability) technického díla, protože tím technické dílo zabezpečuje služby a výrobky, ke kterým je technické dílo vybudováno. Druhým cílem je zajistit integrální (systémovou) bezpečnost technického díla, tj. ochránit technické dílo před pohromami všeho druhu (vnitřními i vnějšími, a to včetně lidského faktoru). Třetím cílem je zajistit, aby technické dílo ani při svých kritických podmínkách neohrožovalo sebe a své okolí, tj. ostatní veřejná aktiva.
Příklady z praxe [23] ukazují, že bezpečnost v řadě případů nevyžaduje vysokou spolehlivost (např. vlak za nepříznivých podmínek nesmí s ohledem na možné ztráty lidských životů a materiální škody při případné havárii upřednostnit spolehlivost před bezpečností, tj. snažit se včas dojet do stanice a přitom ohrozit životy a zdraví lidí). Jelikož se v současné době budují autonomní systémy řízení technických děl, tak se ukazuje jako velmi důležité sestavení pořadí kritérií, dle kterých bude autonomní systém rozhodovat s ohledem na bezpečí a zdraví lidí.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] PROCHÁZKOVÁ, D., 2015: Bezpečnost složitých technologických systémů. ISBN: 978-80-01-05771-1. Praha: ČVUT, 208p.
[2] PROCHÁZKOVÁ, D., 2018: Analýza, řízení a vypořádání rizik spojených s technickými díly. ISBN 978-80-01-06480-1. Praha: ČVUT, 222p. http://hdl.handle.net/10467/78442
[3] FILIPPINI, R., SILVA, A., 2015: A Modelling Language for the Resilience Assessment of Networked Systems of Systems. In: Advances in Safety, Reliability and Risk Management. CRC Press, Taylor & Francis Group, a Balkema Book, ISBN 978-0-415-68379-1 – Hbk, pp. 2443-2450.
[4] PROCHÁZKOVÁ, D., 2017: Zásady řízení rizik složitých technologických zařízení. ISBN: 78-80-01-06182-4. Praha: ČVUT, 364p. http://hdl.handle.net/10467/72582
[5] PROCHÁZKOVÁ, D., PROCHAZKA, J., 2018: Checklist for Judgemet of Technical Facility Safety and Results Obtained by Its Application in Practice. judgement of technical facility safety level and results obtained by its application in practice. Proceedings of International European Safety and Reliability Conference, ESREL2018. ISBN: 978-0-8153-8682-7. London: Taylor & Francis Group, pp. 1175-1184.
[6] PROCHÁZKOVÁ, D., 2011: Metody, nástroje a techniky pro rizikové inženýrství. ISBN 978-80-01-04842-9. Praha: ČVUT, 369p.
[7] KECECIOGLU, D., 1991: Reliability Engineering Handbook. Englewood Cliffs, New Jersey: Prentice-Hall.
[8] ANDERSON, R., 2008: Security Engineering- A Guide to Building Dependable Distributed Systems. ISBN 978-0-470-068552-6. J. Willey, 1001p.
[9] ROLAND, H. E., MORIARITY, D., 1990: System Safety Engineering and Management. ISBN 0-471-6186-0. J. Willey, 321p.
[10] PERROW, CH., 1999: Normal Accidents: Living with High-Risk Technologies. Princeton: Princeton University Press.
[11] UN, 1994: Human Development Report. New York: UN, www.un.org.
[12] ČR, 2018: Všechno špatně. Most v Janově byl špatně navržen i špatně postaven. Právo, 15. srpna 2018.
[13] TURNER, B., 1978: Man-made disasters. New York: Wykeham Science Press.
[14] EU, 1982: Council Directive 82/501/EEC of 24 June 1982 on the Major-Accident Hazards of Certain Industrial Activities. Brussels: EU.

[15] PROCHÁZKOVÁ, D., 2013: Základy řízení bezpečnosti kritické infrastruktury. ISBN 978-80-01-05245-7. ČVUT, Praha, 223p.
[16] SAGAN, S. The limits of safety. Princeton: Princeton University 1993.
[17] PROCHÁZKA, J., PROCHÁZKOVÁ, D., PROCHÁZKA, Z., 2018: Mosty a jejich rizika. Připraveno do tisku.
[18] ALE, B., PAPAZOGLOU, I., ZIO, E. (eds), 2010: Reliability, Risk and Safety. ISBN 978-0-415-60427-7. London: Taylor & Francis Group, 2448p.
[19] REASON, J., 1990: Human Error. Cambridge: University Press.
[20] WIEGMANN, D. A., SHAPPELL, S. A., 2010: A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System. ISBN 0754618730. Ashgate Publishing, Ltd.. pp. 48–49.
[21] OECD, 2002: Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response. OECD, Paris, 191p.
[22] PROCHÁZKOVÁ, D., 2011: Ochrana osob a majetku. ISBN: 978-80-01-04843-6. Praha: ČVUT, 301p.
[23] ČVUT, 2018. Řízení rizik a bezpečnost složitých technologických objektů (RIRIZIBE)“ CZ.02.2.69/0.0/0.0/16 _018/000. Praha: ČVUT.

ADRESA AUTORA

Dana PROCHÁZKOVÁ, doc., RNDr., PhD., DrSc.,
ČVUT v Praze, Fakulta dopravní, Konviktska 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.