



PROPOJENÍ USTANOVENÍ NOREM A VÝSLEDKŮ ŘÍZENÍ RIZIK PRO PODPORU BEZPEČNOSTI

Dana PROCHÁZKOVÁ ¹

LINK OF PROVISIONS OF NORMS AND RESULTS OF RISK MANAGEMENT FOR SAFETY SUPPORT

INTEGRATED SAFETY OF THE ENVIRONS

INTEGRATED SAFETY OF ENVIRONS '2021

¹ ČVUT v Praze, Fakulta strojní Technická 4, 166 00 Praha 6, Česká republika Email: prochdana7@seznam.cz ORCID iD: 0000-0002-4424-3974



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. Copyright: © 2021 by the authors.



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use.



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

ČLÁNEK SLEDUJE SPOLEHLIVOST, ZABEZPEČENÍ A BEZPEČNOST SLOŽITÝCH TECHNICKÝCH DĚL. ZABÝVÁ SE ROLÍ TECHNICKÝCH NOREM A ROLÍ ŘÍZENÍ RIZIK K DANÉMU CÍLI. UKAZUJE, ŽE JE TŘEBA JEJICH CÍLE PROPOJIT A UVÁDÍ PŘÍKLAD.

KLÍČOVÁ SLOVA: Složitá technická díla; technické normy; riziko; řízení rizik; propojení ustanovení norem a výsledků řízení rizik.

ABSTRACT

THE ARTICLE MONITORS THE RELIABILITY, SECURITY AND SAFETY OF COMPLEX TECHNICAL FACILITIES. IT DEALS WITH THE ROLE OF TECHNICAL STANDARDS AND THE ROLE OF RISK MANAGEMENT TOWARDS A GIVEN GOAL. IT SHOWS THAT THEIR OBJECTIVES NEED TO BE LINKED AND GIVES AN EXAMPLE.

KEY WORDS: Complex technical facilities; technical standards; risk; risk management; linking the provisions of standards and the results of risk management.

1. ÚVOD

Složitá technická díla, objektová i síťová jsou nezbytná pro život, ochranu a rozvoj lidstva. V současné době mají povahu socio-kyber-fyzickou, protože je tvoří a provozují lidé, a jsou složeny z technických a kybernetických prvků a propojení. Cílená analýza jejich havárií a selhání [1]



ukázala, že i navzdory velkému množství poznatků o technických dílech, jejich zařízeních, strukturách, vzájemných propojení, rizicích a bezpečnosti, které jsou obsaženy v technických normách pro jejich konstrukci a provoz, se havárie a selhání technických děl stále vyskytují. Příčin jeněkolik: dynamická proměnlivost světa; nedostatečné lidské znalosti a schopnosti; pomalé používání poznatků a zkušeností získaných v praxi; a neuspokojivé povědomí o rizicích a jejich důsledcích pro technická díla a veřejný zájem.

Jelikož svět se dynamicky mění, tak se mění i procesy, které vyvolávají jevy (obecně nazývané pohromy – disasters), jež jsou příčinami rizik. Proto se škodlivý potenciál pohrom v čase mění, tj. mění se i velikosti ohrožení a s nimi i velikosti rizik, ke kterým přispívají i změny v rozložení veřejných aktiv v zájmovém území či sledovaném technickém díle, ke kterým v čase dochází [1]. Proto bezpečnost technických děl a bezpečí jejich okolí musí být sledovány již od konceptu, přes projekt, výstavbu, výrobu, konstrukci, provoz až po odstavení z provozu a revitalizaci zabraného území.

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 (škodlivého jevu z pohledu veřejného zájmu), která se v daném místě vyskytne jedenkrát za definovaný časový interval (tzv. projektová nebo návrhová pohroma) [2]; 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 [2]. Riziko je tudíž místně a časově specifické, protože závisí na množství a zranitelnosti aktiv v daném území a v daném čase.

Vzhledem k dynamickému vývoji světa, stárnutí a opotřebení částí technických děl a omezeným lidským znalostem, zdrojům a možnostem, management technického díla i veřejná správa se musí připravit na budoucí realizace rizik. To znamená mít nástroje, kterými lze snížit realizace známých zdrojů rizik a omezení vzniku rizik nových. Práce prosazuje řízení rizik ve prospěch bezpečnosti. S ohledem na současné poznání, práce nezpochybňuje existující normy a standardy, protože obsahují dřívější poznatky. Bez jejich aplikace by docházelo k opakování minulých chyb. Cílem předložené práce je ukázat, jak propojit poznatky zahrnuté v platných normách s výsledky řízení rizik, což doporučuje nyní i řada norem, např. ISO 31010 (ČSN EN 31010), ISO 9000 atd.

2. TECHNICKÉ NORMY

Technická norma či standard je podrobný předpis, který stanoví důležité parametry či vlastnosti materiálu, výrobku, součásti nebo pracovního postupu, který vede ke standardizaci. Technické normy jsou odborně kvalifikované předpisy, na které se mohou odkazovat smluvní strany při specifikaci předmětu smlouvy nebo státní autorita ve svých obecně závazných předpisech. Umožňují například výměnu výrobků nebo zaměnitelnost součástí a tím zlepšují hospodárnost výroby i bezpečnost výrobků. Stanovením závazných parametrů výrobků přispívají také k ochraně spotřebitele. V současné době v ČR nejsou obecně závazné.

Státní a mezinárodní normy definují také soustavy jednotek, užívané pojmy, kódy, formáty, protokoly nebo rozhraní, například v oblasti informatiky a komunikace, které umožňují propojování různých zařízení, komunikačních a dopravních systémů. Normy jsou mezinárodní, národní, oborové a podnikové. Jsou vydávány autoritami. Technické normy v ČR vydává státní úřad „Úřad pro technickou normalizaci, metrologii a státní zkušebnictví“. Od 20. století se národní normy harmonizují s mezinárodními, vydávanými evropskými nebo světovými organizacemi.

Norma je dokument vytvořený na základě konsenzu, který je schválený uznaným orgánem. Pro všeobecné a opakované používání poskytuje pravidla, směrnice nebo charakteristiky činností nebo jejich výsledků, a přitom je zaměřený na dosažení optimálního



stupně uspořádání v dané souvislosti. Normy jsou založeny na společných výsledcích vědy, techniky a praxe a zaměřeny na dosažení optimálního společenského prospěchu.

Námět na vytvoření české technické normy může příslušnému úřadu podat každý. Následuje posouzení návrhu normy v Technických normalizačních komisích, nebo pokud nejsou, pak v jiných odborných grémiích s cílem dosáhnout shody o užitečnosti navrhovaného řešení pro všechny zúčastněné i pro ČR. Po doporučení se norma zpracuje ve formě návrhu, o kterém se hlasuje. V případě přijetí se schválí a vytiskne. Návrhy evropských norem se schvalují váženým hlasováním, které vyjadřuje hospodářskou významnost členských zemí CEN a CENELEC. ČR má v tomto systému 12 hlasů stejně jako Belgie, Maďarsko, Portugalsko a Řecko. Po schválení jsou členské země povinny normy do 6 měsíců zavést do svých národních norem. V ISO a IEC je ke schválení potřeba 75% kladných stanovisek hlasujících členů[3].

Problematika českých technických norem je obecně řešena ustanoveními zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, který řeší problematiku technických norem v § 4 až § 6. Dle ustanovení uvedeného zákona se **česká technická norma stává harmonizovanou českou technickou normou**, přejímá-li plně evropskou normu nebo harmonizační dokument, které uznaly orgány ES jako harmonizovanou evropskou normu. Evropské harmonizované normy jsou oznamovány v Úředním věstníku evropské unie ve vztahu k jedné či více evropským směrnicím. Jedná se převážně o směrnice tzv. nového přístupu, stanovující především požadavky na bezpečnost výrobků, uváděných na jednotný trh. Harmonizované české technické normy jsou oznamovány ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) ve vztahu k jednomu či více nařízením vlády, kterými byly příslušné evropské směrnice převzaty do právního řádu ČR.

Ustanovení § 6 zákona č. 22/1997 Sb. stanovuje podmínky tvorby a vydávání českých technických norem. Při tvorbě a vydávání českých technických norem, jejich změnách a zrušení musí být zajištěny podmínky stanovené v rozhodnutí o pověření, kterými jsou zejména:

- včasné zveřejňování oznámení o připravovaných návrzích českých technických norem, jejich vydání, změnách a zrušení ve Věstníku Úřadu,
- jednotnost a vzájemný soulad českých technických norem a jejich soulad s právními předpisy,
- využívání dosaženého stupně rozvoje vědy a techniky,
- uplatňování ochrany oprávněného zájmu,
- plnění povinností vyplývajících z mezinárodních smluv, kterými je Česká republika vázána, z členství v mezinárodních a evropských normalizačních organizacích a využívání výsledků mezinárodní spolupráce,
- projednání návrhu české technické normy, její změny nebo zrušení s každým, kdo se ve lhůtě stanovené ve zveřejněném oznámení o zahájení zpracování návrhu české technické normy nebo o návrhu na změnu nebo zrušení české technické normy přihlásí u osoby uvedené v tomto oznámení, nebo s každým, kdo zašle své stanovisko ke zveřejněnému návrhu ve lhůtě stanovené v oznámení o jeho zveřejnění,
- zrušení české technické normy, které bylo projednáno podle předchozí odrážky, pokud neodpovídá podmínkám stanoveným v druhé a čtvrté odrážce,
- řádná distribuce vydaných českých technických norem a jejich změn do dvou týdnů po doručení objednávky.

Podstatný je výše uvedený fakt, že u norem jde o „dokument vytvořený na základě konsenzu“. Jelikož prostředí se dynamicky vyvíjí, návrhy ustanovení norem zahrnují výsledky určitého intervalu, který označujeme jako „medián $\pm \sigma$ “, kde σ je standardní odchylka, která se určuje podle teorie pravděpodobnosti. V uvedeném případě si však musíme uvědomit skutečnost, že v žádném případě vybrané řešení nepokrývá všechny možné varianty sledované problematiky. Pro normální rozdělení platí, že interval $(-\sigma, +\sigma)$ pokrývá 68.5 % případů; interval $(-2\sigma, +2\sigma)$ pokrývá 95.4 % případů; interval $(-3\sigma, +3\sigma)$ pokrývá 99.8 % případů [4]. To znamená, že normy pokrývají 68.5 % případů. Uvedená skutečnost v praxi znamená, že cíl norem je omezen tzv. limity a podmínkami; tj. řešení



platí jen pro určité podmínky (a při jejich překročení dochází k nesplnění cíle, což vede až k selhání či havárii prvku, objektu či procesu) [1,4].

3. RIZIKO A BEZPEČNOST

Cílem lidí je, aby 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 [5].

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“.

Bezpečnost je chápána jako vlastnost na úrovni systému, kterou formuje člověk svými opatřeními a činnostmi [1,2,5]. Veličiny riziko a bezpečnost nejsou komplementární veličiny, protože bezpečnost prostředí i každého technického díla lze zvýšit pomocí organizačních opatření, např. zavedením varovacích systémů a záložních řešení, aniž bychom snížili velikost rizika; doplňkovým pojmem k bezpečnosti je kritičnost [1,2,5].

Bezpečnost technického díla a jeho okolí lze zajistit jen kvalitním antropogenním řízením [1,2,5,6]. 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 [6].

4. ŘÍZENÍ RIZIK TECHNICKÝCH DĚL ZACÍLENÉ NA BEZPEČNOST

Řízení je druh činnosti, který vyvolává a zajišťuje fungování sledovaných systémů. Je to uvědomělý způsob aplikace teoretických a praktických znalostí člověka (řídícího pracovníka) zaměřený na identifikaci a rozpoznání problémů a cílů ve sledovaném systému, způsoby zvládnutí problémů, stanovení postupů k dosažení žádoucích cílů a na implementaci postupů spojenou s kontrolními mechanismy zaměřenými tak, aby žádoucí cíle byly dosaženy optimálně. Jeho prvním úkolem je správně diagnostikovat či specifikovat každý problém, racionálně rozhodnout, rozhodnutí akceptovat a realizovat v daných konkrétních podmínkách. Řízení má predispozici být úspěšné, když je založené na odborných znalostech a zkušenostech a když jednotlivá rozhodování, z nichž se řízení nebo lépe proces řízení skládá, jsou kvalifikovaná. Získání předmětných znalostí a zkušeností znamená neustále shromažďovat, vyhodnocovat i ověřovat data a provádět kvalifikovaná hodnocení.

Total Quality Management (TQM) [7,8] je typ řízení, který pomohl po druhé světové válce evropskému průmyslu zotavit se z propadu, který mu způsobila válka [9]. Pro úspěšnost byl do veřejného sektoru v EU zaveden smlouvou v Maastrichtu v r. 1989. 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 řídicí pracovníky. Proces zlepšování jakosti vychází z impulsu podle potřeb od zákazníka /občana. TQM vychází z poznání, 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 [8]. Jde o 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.

Výstupy z procesu řízení rizik při aplikaci TQM pro zajištění bezpečnosti jsou následující:

1. **Seznam vyhodnocených rizik** (risk assessment document) - zde se zaznamenávají veškeré informace o příslušných rizicích.
2. **Seznam rizik vyžadujících nejvyšší pozornost** (top risks list) - obsahuje seznam vybraných rizik, jejichž řešení má nejvyšší nároky na zdroje a čas (u technických děl jde o rizika, která je třeba stále sledovat a podle výsledků monitoringu aplikovat opatření a činnosti vedoucí k bezpečnosti [6]).
3. **Seznam neaktuálních / vyřešených rizik** (retired risk list) - slouží jako historický odkaz pro budoucí rozhodování při změnách a modernizacích (např. aby se neodstranily bariéry, které byly do systému vsazeny z důvodu prevence nebo zmírnění [10]).

Podle údajů shrnutých v práci [1] jsou pro technická díla používané různé typy řízení. V současné době se používají:

- Řízení spolehlivosti (reliability management).
- Řízení zabezpečení (security management).
- Řízení bezpečnosti (safety management).
- Řízení kontinuity (continuity management).
- Řízení pružné odolnosti (resiliency management).
- Řízení aktiv (asset management).

Každý z těchto typů má jistá specifika. První typ řízení je nejstarší a upravují ho technické normy a standardy. Druhý typ řízení se kromě řízení spolehlivosti soustřeďuje na ochranu technických děl před vnitřními i vnějšími škodlivými jevy (pohromami), a to včetně chování lidí, kteří je vytváří a provozují [2]. Zabezpečení (anglicky security) ve spojení s jistým objektem znamená obecně soubor opatření a činností, kterými se zajistí, že sledovaný objekt neutrpí ztráty, škody a újmy při výskytu vnitřních i vnějších škodlivých jevů. K jeho realizaci se používá fyzická a kybernetická ochrana objektu [11], a to nejen proti útokům zevnějšku, ale i z vnitřku.

Pravidla pro zabezpečení technických děl jsou rozpracovaná v práci [12], ve které jsou i vymezení oproti bezpečnosti technických děl [13]; odlišení mezi zabezpečením a bezpečností je též v dokumentech IAEA [14]. Přestože logicky je bezpečný objekt též objekt zabezpečený [6], tak existují stále dohady, co je důležitější. Shoda je v tom, že **zabezpečené technické dílo** stejně jako bezpečné technické dílo bezchybně plní stanovené úkoly po stanovenou dobu za určitých podmínek, a přitom je ochráněno proti všem vnitřním a vnějším pohromám, včetně lidského faktoru. Rozdíl je v tom že zabezpečené technické dílo nemá zabudovanou ochranu okolí.

Abychom zajistili bezpečnost technických děl, řešíme problém bezpečnosti systému systémů [1,6], 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,
- charakteristiky kritických stavů systému systémů.



Řízení kontinuity je zacílené na bezpečnost technického díla i jeho okolí za všech možných podmínek [1]. Řízení pružné odolnosti je předstupněm řízení bezpečnosti a řízení kontinuity; snaží se zvýšit houževnatost systému a okolí, aby byl získán čas na zformování účinné odezvy objektu při výskytu škodlivého jevu [1]. Řízení aktiv upřednostňuje řízení rizik ve prospěch výroby před bezpečím lidí a okolí technického díla [1], tj. nepreferuje veřejný zájem.

Součástími všech typů řízení jsou pak specifické typy, kterými jsou nouzové řízení a krizové řízení. Srovnání typů ukazuje, že:

- všechny typy používají stejné metody a nástroje pro práci s riziky, které z důvodů různých cílů předmětných postupů v konkrétních případech nedávají stejné výsledky [6],
- všechny typy mají stejný cíl, kterým je zvládnutí rizik a ochrana aktiv (je však rozdíl v tom, která rizika a která aktiva zvažují),
- počínaje druhým typem jsou nadstavbou řízení spolehlivosti (reliability management), které bylo po dlouhá léta královskou disciplínou při řízení technických děl [6],

Přes různé názvy typů řízení, jejich metodologie je stejná, a to získat: povědomí o riziku; pochopení rizika a jeho vztahu k aktivům a jejich bezpečí; a aplikovat příslušné znalosti o tom, co dělat pro dosažení cíle. Pro strategický rozvoj lidské společnosti i technických děl je zásadní řízení rizik ve prospěch bezpečnosti, která je zacílená na celek (tj. safety management).

V rámci řízení rizik technického díla ve prospěch bezpečnosti je třeba kvalitně provést pět klíčových aktivit [2], a to:

- Vymezení cíle a centra zájmu řízení bezpečnosti: identifikovat kontext; určit prioritní cíle; a určit oblasti a zásadní úkoly. Výběry jsou založeny na hodnocení aktiv a cílů. Tím stanovíme, které riziko je v daném případě prioritní.
- Popis: směřuje k objektivnímu pochopení pravděpodobnosti výskytu a velikosti dopadů (v kvalitativním nebo lépe kvantitativním vyjádření) možných pohrom a selhání technického díla. Jedná se o vysoce odbornou činnost vyžadující hluboké znalosti a kvalitní data.
- Rozhodnutí: vyhodnocení kvality předpovědi vývoje technického díla, pokud možno jako optimum při zvážení přínosů a ztrát při provozu technického díla v dynamicky proměnném okolí. Rozhodnutí, jak zmírnit a řídit rizika a jak implementovat opatření, reprezentuje klíčový krok v rámci řízení rizika.
- Komunikace: projednání souboru opatření a činností s klíčovými aktéry procesu provozu technického díla a s ostatními zúčastněnými. Legislativa vyžaduje v důležitých otázkách komunikaci s veřejností, konzultace, odstranění konfliktů a stanovení partnerství.
- Monitoring a poučení: sledování určených veličin a jejich hodnot, které charakterizují důsledky rozhodnutí a činností na technické dílo, a v případě zjištění významných odchylek, které mohou narušit dosažení cíle, aplikovat korekce.

Zvládání rizik v případě, že riziko není přijatelné, spočívá dle [2,5,6] ve výběru některé z dále uvedených alternativ:

- vyhnout 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,
- retence rizika.



Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá dle [2,5,6] v rozdělení rizik do kategorií:

- část rizika se sníží, tj. preventivními opatřeními se odvrátí realizace rizika,
- část rizika se zmírní, tj. preventivními opatřeními a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se sníží nebo odvrátí nepřijatelné dopady,
- část rizika se pojistí,
- část rizika, pro kterou se připraví rezervy na odezvu a obnovu,
- část rizika, která je neřiditelná nebo příliš nákladná nebo málo častá, pro kterou se připraví plán pro nepředvídané situace (Contingency plan).

K tomu se rovněž připojuje rozdělení zvládání rizik mezi všechny zúčastněné. Rozdělení ve správném řízení [5] 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. Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika.

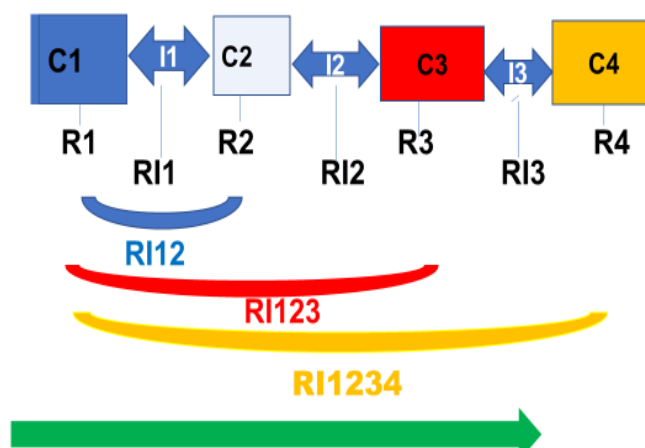
5. ZÁVĚR

Z výše uvedeného vyplývá, že při sestavování konceptu technického díla i při jeho umístění, projektování, zhotovení a provozu jsou důležité jak normy, tak výsledky řízení rizik ve prospěch sledovaného cíle, kterým je dnes celková (integrální) bezpečnost. Proto v souladu s poznáním, jsou vytvářeny nástroje risk-based design [10] a risk-based operation [1], které propojují normy a výsledky řízení rizik.

Příklad propojení norem a řízení rizik při projektování je uveden na obrázku 1. Dle [15] Nejprve se sestaví pro dané technické dílo systém pro podporu rozhodování o rizicích jednotlivých komponent a jejich propojení, stanoví se stupnice pro hodnocení míry rizika – tabulka 1; a určí se postup budování projektu. Pak následuje:

- navržení komponent (C1, C2, C3, C4) a jejich propojení podle norem,
- podle scénářů pohrom se stanoví rizika komponent (R1, R2, R3, R4) a jejich propojení (RI1, RI2, RI3) a posoudí se dle tabulky 1 a v případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení,
- podle DSS se určí riziko souboru propojení RI12 a posoudí se dle tabulky 1 a v případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení,
- podle DSS se určí riziko souboru propojení RI123 a posoudí se dle tabulky 1 a v případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení,
- podle DSS se určí riziko souboru propojení RI1234 a posoudí se dle tabulky 1 a v případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení.

Podle zjištěných hodnot rizika se výsledky posouzení rizika řadí do tří skupin: riziko přijatelné – kategorie 0 a 1; riziko ALARA, tj. podmíněně přijatelné – kategorie 2 a 3; a riziko nepřijatelné – kategorie 4 a 5. Jeli riziko přijatelné, tak není třeba dělat žádné další opatření na zmírnění rizika. Je-li riziko ALARA, tak je třeba v projektu zabudovat technické prvky, které umožní odezvu v případě realizace rizika. V případě nepřijatelného rizika, je nutné provést korekce, např. v materiálu, konstrukci či způsobu propojení a znovu riziko posoudit.



Obr. 1 - Schéma procesu projektování založeného na řízení rizik. Zelená šipka zobrazuje postup vytváření projektu.

Tab. 1 - Hodnotová stupnice pro stanovení míry rizika.

Kategorie rizika	Hodnoty míry rizika v %
Extrémně vysoká – 5	Více než 95 %
Velmi vysoká – 4	70–95 %
Vysoká – 3	45–70 %
Střední – 2	25–45 %
Nízká – 1	5–25 %
Zanedbatelná – 0	Méně než 5 %

Poznatky uvedené v pracích [10,15] ukazují, že u projektanta jsou velmi důležité kompetence pro: uplatňování výsledků metod analýzy a hodnocení rizik; provádění metodiky analýzy a hodnocení rizik přizpůsobených problému; řešení mimořádných situací a krizí; analýzu situací / činností / nehod; přeměnu politiky na skutečnou akci; přeměnu statistik nehod na akční plány; strategické plánování; stanovení hierarchie problémů; nalezení správných informací a poznatků; provádění kritických analýz; navrhování správných řešení; komunikaci; provádění syntézy a přizpůsobování znění určeného veřejnosti; a dodržování etiky. Při každém rozhodování ve prospěch bezpečnosti je třeba mít na paměti: všechny faktory a procesy, které mohou být nebezpečné a jak často se mohou vyskytnout; jak velké mohou být jejich dopady; jak lze snížit velikost dopadů nebo četnost výskytu; zda navrhovaná opatření nemohou být zdrojem nových nebezpečí; a kterými technickými a řídicími systémy lze ovládat ohrožení, kterým nelze zabránit.

A konečně je třeba poznamenat, že v souladu s výsledky v [6,10] je nezbytné, jaká je politická vůle vytvořit systém na ochranu před nepřijatelnými dopady škodlivých jevů. Výzkum ukázal, že:

- každý projekt technického díla či zařízení má určitá nebezpečí. Umění projektanta spočívá v tom, že umí zvolit optimální řešení, tj. řešení dostatečně bezpečné a realizovatelné s ohledem na možnosti investora a veřejné správy,
- působivé a málo robustní konstrukce s nedostatečnými bezpečnostními rezervami často dříve nebo později selžou,
- chybně stanovené limity a podmínky pro kritické části technického díla či zařízení vedou k častým poruchám až k vážným nehodám; taková technická díla nejsou schopná reagovat na změny stavu.



Analýza dostupných právních předpisů [16] odhalila, že dle platných pravidel není vyžadováno sledovat bezpečnost procesů při provozu ve fázi projektování, což občas vede k problémům v provozu [1]. Další chybou legislativy je skutečnost, že nevyžaduje opatření na snížení rizik, která se vyskytnou při náhlé časové kombinaci řady škodlivých jevů. Podle posledních zkušeností je třeba do legislativy zavést povinnost na zvažování vyšších hodnot projektových pohrom, alespoň u objektů kritické infrastruktury.

Postup pro řízení rizik při provozu technického díla je popsán v práci [1] a jeho účinnými nástroji jsou: inspekce založené na rizicích (risk-based inspections), údržba založená na rizicích (risk-based maintenance) a plán řízení rizik.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] PROCHÁZKOVÁ, D., PROCHÁZKA, LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., a L. OUHRABKA. *Řízení rizik procesů spojených s provozem technického díla během jeho životnosti*. ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p.
doi:10.14311/BK.9788001066751.
- [2] PROCHÁZKOVÁ D. *Analýza, řízení a vypořádání rizik spojených s technickými díly*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222p. <http://hdl.handle.net/10467/78442>
- [3] <http://www.technické-normy-csn.cz>
- [4] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.
- [5] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN 978-80-01-04844-3. Praha: ČVUT 2011, 483p.
- [6] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364p. <http://hdl.handle.net/10467/72582>
- [7] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991.
- [8] NENADÁL, J. TQM. Role ekonomiky jakosti v koncepci TQM. 1999,
<http://fmml10.vsb.cz/639/qmag/mj03-cz.htm>.
- [9] PROCHÁZKA, T. Spolupráce veřejného a soukromého sektoru. *Diplomová práce*. Praha: VŠFS 2008, 107p.
- [10] 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, 207p. <http://hdl.handle.net/10467/8446634>
- [11] PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. ISBN 978-80-01-04843-6. Praha: ČVUT 2011, 301p.
- [12] ANDERSON, R. *Security Engineering- A Guide to Building Dependable Distributed Systems*. ISBN 978-0-470-068552-6. J. Willey, 2008, 1001p.
- [13] ROLAND, H. E., MORIARITY, B. *System Safety Engineering and Management*. ISBN 0-471-6186-0. J. Willey, 1990, 321p.
- [14] IAEA. *Safety Guides and Technical Documents*. Vienna : IAEA 1954 – 2019.
- [15] PROCHÁZKOVÁ, D. Risk-based Design of Technical facilities. In: *JUFOS 2021*. ISBN 978-80-214-5963-2. Brno: VUT 2021, pp. 40-51.
- [16] ČVUT. *Databáze pohrom, havárií a selhání technických děl, jejich příčin, poučení a opatření odezvy*. Praha: CVUT 2021.