

ŘÍZENÍ RIZIK TECHNICKÝCH DĚL PŘI PROJEKTOVÁNÍ

Dana PROCHÁZKOVÁ ¹

RISK MANAGEMENT OF TECHNICAL FACILITIES AT DESIGNING



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

PRO ZAJIŠTĚNÍ BEZPEČNÉ FUNKCE SLOŽITÝCH TECHNICKÝCH DĚL JE NUTNÉ V CO NEJVĚTŠÍ MÍŘE VYPOŘÁDAT RELEVANTNÍ RIZIKA (A TO I TA, KTERÁ SOUVISÍ SE STÁRNUTÍM ZAŘÍZENÍ A KOMPONENT TECHNICKÝCH DĚL A S DYNAMICKÝM VÝVOJEM PROSTŘEDÍ V ČASE) PŘI PŘÍPRAVĚ ZADÁVACÍCH PODMÍNEK A PŘI PROJEKTOVÁNÍ. ABY BYLO MOŽNÉ VYPROJEKTOVAT TECHNICKÉ DÍLO S POVAHOU SOCIO-KYBER-FYZICKOU S TĚMITO VLASTNOSTMI, NESTAČÍ RESPEKTOVAT JEN PLATNÉ NORMY, STANDARDY A POSTUPY DOBRÉ PRAXE. PŘI PROJEKTOVÁNÍ JE TŘEBA RESPEKTOVAT ÚDAJE O VŠECH MOŽNÝCH RIZICÍCH A JEJICH KOMBINACÍCH, A K TOMU POUŽÍVAT TAKÉ OPATŘENÍ UVEDENÁ V PLÁNU ŘÍZENÍ RIZIK PRO PROJEKTOVÁNÍ, KTERÝ SPECIFIKUJE MÍSTNÍ PODMÍNKY A MOŽNOSTI. PROTO MUSÍ BÝT POUŽITA SPRÁVNÁ METODIKA TVORBY PROJEKTU, KTERÁ ZOHLEDŇUJE VŠECHNA RELEVANTNÍ RIZIKA. ČLÁNEK NAVRHUJE METODIKU GENERACE PROJEKTŮ TECHNICKÝCH DĚL SOCIO-KYBER-FYZICKÉ POVAHY, KTERÁ SE OPÍRÁ O ŘÍZENÍ RIZIK (RISK-BASED-DESIGN METHODOLOGY) A KTERÁ JIŽ BYLA OVĚŘENA V PRAXI.

KLÍČOVÁ SLOVA: Rizika; technická díla; projektování; projekt založený na výsledcích řízení rizik; bezpečnost.

ABSTRACT

To ensure the safe operation of complex technical facilities, it is necessary to address all RELEVANT RISKS (NAMELY THOSE RELATED TO THE AGEING OF EQUIPMENT AND COMPONENTS OF TECHNICAL FACILITIES AND WITH DYNAMIC DEVELOPMENT OF THE ENVIRONMENT OVER TIME) IN THE PREPARATION OF SPECIFICATIONS (TERMS OF REFERENCES) AND IN DESIGN. IN ORDER TO DESIGN THE SOCIO-CYBER-PHYSICAL FACILITY WITH THESE PROPERTIES, IT IS NOT ENOUGH TO RESPECT ONLY VALID STANDARDS AND NORMS AND PROCEDURES OF GOOD PRACTICE. AT DESIGNING, THEY NEED TO BE RESPECTED DATA



ON ALL POSSIBLE RISKS AND THEIR COMBINATIONS, AND FOR THIS TO USE MEASURES IDENTIFIED IN THE RISK MANAGEMENT PLAN FOR DESIGN, WHICH SPECIFIES LOCAL CONDITIONS AND POSSIBILITIES. THEREFORE, THE CORRECT METHODOLOGY OF DESIGN CREATION CONSIDERING THE RELEVANT RISKS NEEDS TO BE USED. THE ARTICLE PROPOSES THE METHODOLOGY OF GENERATION OF TECHNICAL FACILITIES RISK-BASED DESIGN, WHICH WAS VERIFIED IN PRACTICE.

KEY WORDS: Risks; technical facilities; designing; risk-based design; safety.

1. ÚVOD

Lidské životy v moderní společnosti jsou usnadňovány prostřednictvím socio-kyber-fyzických zařízení a děl, jejichž složitá systémová povaha je výsledkem znalostí a dovedností předešlých lidských generací. Všechny pozitivní důsledky technického pokroku na fungování lidské společnosti jsou však vykoupeny existencí mnohem většího počtu rizik, která za jistých podmínek vedou k: selhání základních funkcí státu; snížení úrovně bezpečnosti a narušení koexistence socio-kyber-fyzických systémů (*dále jen "SKFS"*) s jejich okolím; a ztrátám na lidských životech a poškození zdraví lidí. Koexistence obecně znamená společnou existenci a v dnešní době, která se vyznačuje mnoha rozmanitými konflikty, roste její potřeba a význam [1–12].

SKFS se skládají z řady částí, které jsou propojeny a mají objektové nebo síťové struktury. Zvláštní pozornost je v současné době věnována rozsáhlým *SKFS*, které poskytují kvalitní základní služby a výrobky lidem. Jsou složité a mnohé z nich zajišťují plnění základních funkcí státu, a proto je s nimi spojeno slovo kritické [1–17]. Inženýrské systémy, od nejjednodušších po nejsložitější, splňují každodenní potřeby a požadavky občanů, a proto vyžadují cílenou antropogenní péči od fáze projektování až po ukončení životnosti.

Složité *SKFS* patří do různých odvětví řízení, a proto se velmi liší jak projektem, tak povahou a posláním. Kritéria a opatření pro řízení a vypořádání jejich rizik jsou proto závislá na odvětví, i když mají stejný cíl, a to bezpečnost. Bezpečnost znamená, že plní spolehlivě úkoly, pro které byly vytvořeny, a ani za kritických podmínek neohrožují sebe a své okolí [1–19]. Z důvodů velké rozmanitosti *SKFS* a prostředí, v němž jsou umístěny, jsou postupy pro budování jejich bezpečnosti specifické pro lokalitu a odvětví. Aspekty důležité pro provoz částí *SKFS* a celých *SKFS* se liší zejména v oblastech: znalostí a technických záležitostí, které podmiňují kapacitní možnosti *SKFS*; organizačních a právních záležitostí umožňujících provoz *SKFS* na určité úrovni bezpečnosti v území a v průběhu času; finančních záležitostí; personálu; sociální; a politiky na vnitrostátní a mezinárodní úrovni.

Na základě současných poznatků [13,14] se každý inženýrský systém vyznačuje strukturou, hardwarem, postupy, prostředím, informačními toky, organizací a rozhraními mezi uvedenými komponentami. Základním prvkem bezpečného navrhování *SKFS* v oblasti technických řešení je použití bezpečných prvků (tj. spolehlivých, funkčních a neohrožujících sebe a své okolí), jejich kvalifikovaná propojení a provozní režimy umožňující bezpečný (tj. spolehlivý a bezproblémový) provoz a řádnou údržbu, zálohování prioritních částí prvků, součástí nebo systémů, používání různých zásad zálohování a promyšlené zavádění záloh. Vzhledem ke složitosti *SKFS* nestačí dodržovat platné normy a standardy, ale je nutné uplatňovat zásady inženýrství, která pracují s riziky, jak ukládá novelizace normy ISO 9000 z r. 2016.

Riziko je mírou ztrát, škod a újm na aktivech veřejných i *SKFS*, které způsobí škodlivý jev (pohroma) s velikostí normativně určeného ohrožení rozpočtená na jednotku plochy a času, tj. je místně a časově specifické [12–20]. Aplikací dnes stále propagovaných metod řízení rizik při projektování (risk-based design) se nezpochybňují existující normy a standardy, protože jsou v nich skryty znalosti i zkušenosti z praxe; platí, že bez norem, standardů a legislativy by odborníci i odborná veřejnost byli odsouzeni k opakování chyb z minula.

Poučení z praxe ukazuje, že respektování norem, standardů a dobré inženýrské praxe pokrývá 68.4 % možných scénářů pohrom [16]. Proto novelizace mezinárodní normy ISO 9000, vydané v ČR v r. 2016 vyžaduje aplikovat analýzu rizik v souvislosti se zajišťováním kvality procesů a produktů ve firmách,



kté usilujú o certifikaci či re-certifikaci systému řízení kvality. Předmětná norma odkazuje na další normy: ČSN ISO 31000 Management rizik – principy a směrnice; ČSN EN 31010 Management rizik – Techniky posuzování rizik atd. Předmětné normy však nestanovují, jak předmětné řízení rizik provádět.

Předložená práce ukazuje postup projektování technických děl, ve kterém se respektují požadavky platných norem a standardů a jsou doplněny (zpřesněny) poznatky získanými z řízení rizik. Pro praxi byl v práci [12] vytvořen plán řízení rizik pro projektování, který ukazuje oblasti, ve kterých byly udělány chyby, které zapříčinily později při provozu havárie či selhání, a které v zájmu bezpečnosti musí být v rámci zpracování projektu řádně ošetřeny.

2. SOUHRN ZNALOSTÍ O PROJEKTOVÁNÍ SKFS

Každé území má své vlastní zdroje rizik [18] a vložení každého elementu, tj. *SKFS*, zdroje rizik přibudou, a proto je třeba z pohledu lidského bezpečí se vnějšími i vnitřními zdroji rizik zabývat v souvislosti s projektem *SKFS*. Současné poznatky ukazují, že rizika, která nebyla vypořádána, způsobují *SKFS* dříve či později ztráty, škody a újmy jak na veřejných aktivech, tak na aktivech *SKFS* [19].

SKFS mají formu objektů nebo sítí a představují složité systémy, jejichž formou je systém systémů – SoS [1-12,14,20]. Zahrnují technické, kybernetické, organizační a sociální systémy, tj. jednotlivá zařízení, stroje, komponenty, systémy nebo celé výrobní nebo servisní jednotky, a jejich propojení. Propojení jsou žádaná (vkládaná tvůrci *SKFS*) a nežádaná (tzv. interdependences), která vznikají jen za určitých podmínek (pohromách všeho druhu) a vedou ke ztrátám. Znalosti a zkušenosti ukazují, že *SKFS* jsou umístěny do určitého prostředí, které v každém případě reaguje na tyto *SKFS*, a to dříve či později. Z důvodů bezpečnosti musí být tyto reakce odhaleny předem a zváženy v projektu, aby bylo zajištěno bezpečí lidí, životního prostředí i samotných *SKFS*.

Cílem každého projektu *SKFS* je vytvořit zařízení či dílo, které je ziskové, ekonomické a bezpečné, a proto je nutno řešit širokou škálu problémů, např.: teoretická analýza kritických procesů, vybavení a umístění *SKFS*; postup praktického provádění technicky a finančně dostupných protipatření v *SKFS*; výběr: materiálů; technických principů; konstrukčních postupů; stanovení kritických konstrukčních a montážních procesů atd.; experimentální ověření instalovaných zařízení a jejich provozuschopnosti za normálních, abnormálních a kritických podmínek; a zajištění: trvanlivosti; ovladatelnosti zařízení a procesů; požadované životnosti; kvality; dostatečných lidských zdrojů; udržení nákladů v požadované výši; technických služeb; a realizace budov, sítí a zařízení za stanovených podmínek atd.

Jak již bylo zdůrazněno, tak pro lidské bezpečí je to nutné, aby reakce prostředí po celou dobu životnosti *SKFS* byly přiměřené a aby fungovalo jeho soužití s okolím. ***Zajištění těchto cílů musí být vloženo již do projektu SKFS.*** Za prvé je třeba vzít v úvahu zdroje všech rizik (pohrom), tj. aplikovat přístup „All-Hazard-Approach“ [21]. Do této sady zdrojů rizik patří také zdroje destruktivních jevů, které jsou výsledkem všech vzájemných reakcí uvnitř *SKFS* i v jeho propojení s okolím za normálních, abnormálních a kritických podmínek [12].

Identifikace interních zdrojů rizik v *SKFS*, které jsou spojené na jedné straně s jednotlivými technickými zařízeními, jejich uspořádání do konstrukčních částí a systémů a na straně druhé s výrobními procesy a jejich řízením, je činnost specifická pro konkrétní místo, která vyžaduje identifikaci rizik na několika úrovních, a to: technické vybavení; komponenty; systémy; technická, organizační a kybernetická propojení za běžných provozních podmínek; technická, organizační a kybernetická propojení za abnormálních provozních podmínek; technická, organizační a kybernetická propojení za kritických provozních podmínek; a pro vysoce důležité *SKFS*, jako jsou jaderné elektrárny, přehrady atd., technické, organizační a kybernetické propojení za extrémních provozních podmínek [13,14,22].

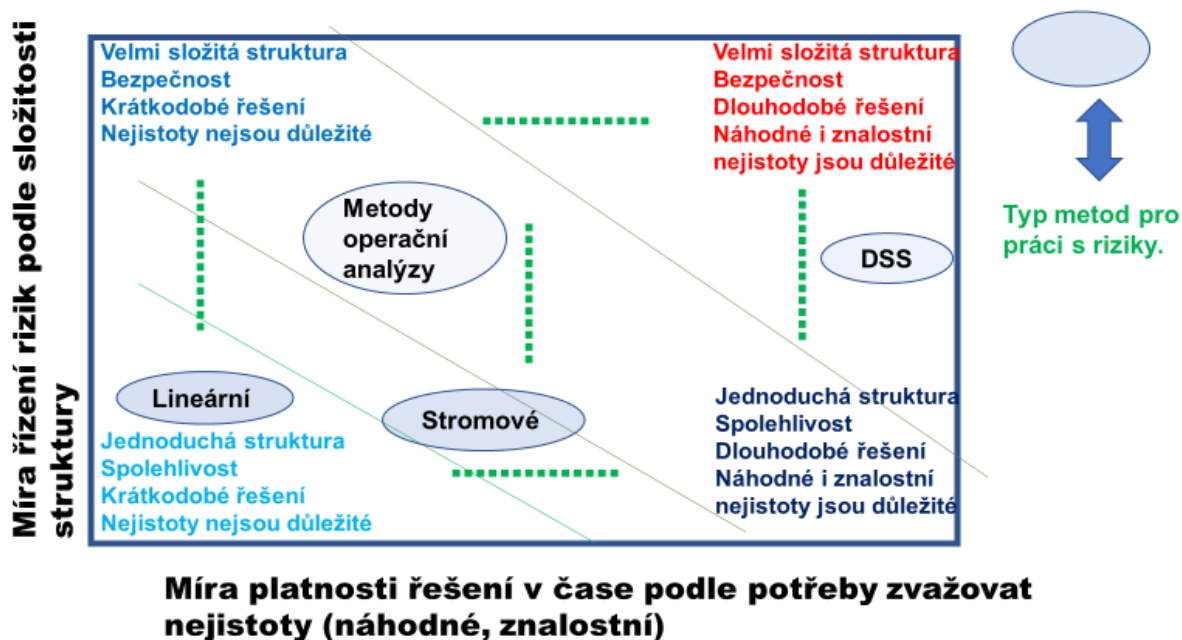
Při identifikaci zdrojů rizik *SKFS* je velmi důležité vzít v úvahu všechny stabilní a mobilní zdroje rizik uvnitř i vně *SKFS*: požáry (mžikový, proudový, kaluže, zážehový, tryskový, ohnivá koule – BLEVE, VCE); výbuchy (mechanické, elektrické, chemické, exploze mraků plynu, prachů a popř. jaderné);

úniky nebezpečných látok, pretože jejich dopady způsobí, jak přímě škody, tak i dominové efekty, které škody znásobují [6].

Každý nebezpečný jev může mít různé velikosti a různé pravděpodobnosti výskytu, a proto je důležité stanovení ohrožení pro každý možný jev. Vzhledem k tomu, že extrémní nebezpečné jevy (pohromy) se vyskytují zřídka a nepravidelně, je stanovení ohrožení jedním z hlavních kroků pro určení rizika [20].

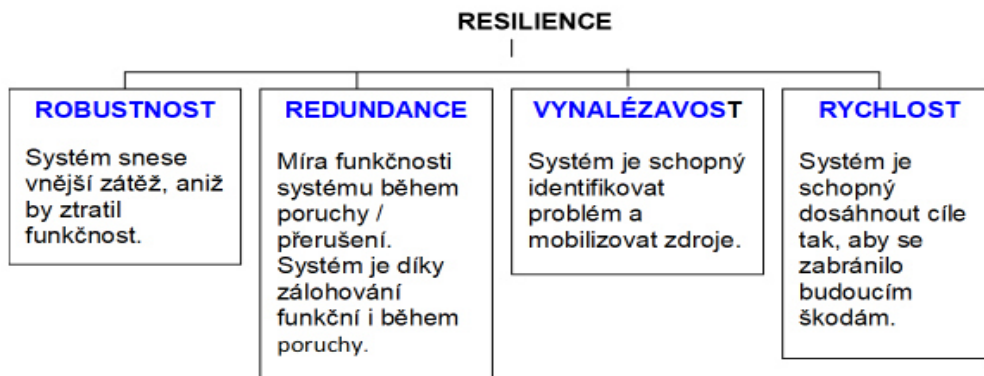
Stanovení ohrožení je technicko-metodická metoda stanovení maximální očekávané velikosti pohrom (včetně havárií a selhání všeho druhu). Vzhledem k tomu, že k závažným událostem dochází náhodně a nepravidelně, a svět se dynamicky vyvíjí v prostoru a čase (což také vede ke změnám podmínek, které vedou k pohromám, a samozřejmě také ke změnám vlastností pohrom), nelze použít jednoduché statistické metody (jejich předpoklady vyžadující stabilní procesy nejsou plně splněny). Vzhledem k tomu, že o této oblasti nemáme dostatek znalostí, musíme zvážit existenci nejistot, náhodných i znalostních, a používat metody založené na teoriích extrémů [23].

Podle křivek ohrožení určujeme projektovou (normální) pohromu, což je velikost pohromy, jejíž pravděpodobnost výskytu je jednou za časový interval, který je stanoven právními předpisy [20]. Parametry projektových pohrom se používají při projektování technických děl, výstavbě, vybavení komponentami a systémy a později i při provozu. Na základě místních podmínek se na základě normativně určených hodnot ohrožení se určují rizika a jejich rozložení. Metody pro jejich určení závisí na složitosti SKFS [12]; obrázek 1.



Obr. 1 - Skórování způsobů řízení rizik podle složitosti struktury SKFS a cíle řízení rizik s identifikací potřeby zvážení nejistot a vhodných metod identifikace rizik.

Pro potřebu projektování parametry projektových pohrom vytvářejí zadávací podmínky SKFS. Jejich respektování při výběru materiálů, prvků, způsobu propojování prvků atd. zajišťuje, že do SKFS se vloží schopnosti pro prevenci, zmírňování a reakci na nepřijatelné situace způsobené vnitřními, vnějšími a organizačními zdroji nehod, havárií a selhání prvků, součástí a systémů, a to pro pohromy, které jsou menší než projektové pohromy. Zadávací podmínky jsou proto klíčovou součástí projektové dokumentace SKFS, která obsahuje technické, finanční, časové a další údaje určující bezpečné, spolehlivé a funkční SKFS. Vytvářejí tzv. limity a podmínky pro bezpečný provoz SKFS [12]. Identifikují míru resilience (tj. souhrn robustnosti, redundance, vynalézavosti a rychlosti), obrázek 2, kterou bude mít SKFS.



Obr. 2 - Vlastnosti zabudované do systému pomocí vložení resilience[16,17].

Podle údajů v [12,20] je nezbytné mít při vytváření zadávacích podmínek:

- znalosti: předpisů; rizik v místě, do kterého je *SKFS* umístěn; technického systému, který představuje *SKFS*; modelů a teorií spojených s haváriemi; metod analýzy, řízení a vypořádání rizik; a řízení podniku (finance, lidské zdroje, organizace, technologie, inovace...),
- kompetence pro: uplatňování výsledků metod analýzy a hodnocení rizik; provádění metodiky analýzy a hodnocení rizik přízpusobených problému; řízení nouzových a krizových situací; analýzu situací / činností / nehod; přeměnu politiky na skutečná opatření; přeměnu statistik nehod na akční plány; strategické plánování; hierarchizaci problémů; vyhledání a aplikaci správných informací a poučení; kritickou analýzu; navrhování správných řešení; psanou a mluvenou komunikaci; provádění syntézy a přizpusobování formulace určené veřejnosti; a prosazování etiky.

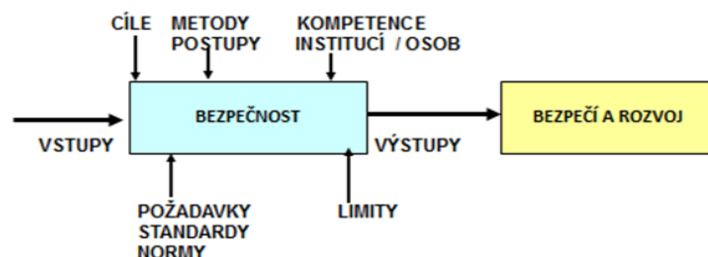
Pokud jde o vytváření zadávacích podmínek, je s ohledem na možné pohromy v lokalitě a v souvislosti se koexistencí *SKFS* s okolím nezbytné: upřesnit pro každou relevantní pohromu velikost ohrožení podle dané normy; určit kritické úkoly *SKFS* z hlediska integrální bezpečnosti; pochopit úkoly *SKFS* a příčiny jejich závažnosti; identifikovat možná lidská selhání při provozu *SKFS*; a navrhnout opatření pro zajištění bezpečnosti s ohledem na proměnlivé podmínky.

Kritické úkoly *SKFS* z hlediska integrální bezpečnosti jsou fyzické činnosti, kterými provozovatel přispívá k: vyvolání nežádáných a nepřijatelných jevů; detekci a prevenci těchto jevů; řízení a zmírňování těchto jevů; a reakce na mimořádnou situaci. Při vytváření zadávacích podmínek je třeba vzít v úvahu, že ke kritičnosti přispívají dle [12] také: nedostatečná komunikace (chyby a přerušení toku informací); rutinní přístup (jistota vyplývající z dlouhodobé praxe v kombinaci se ztrátou povědomí o rizicích způsobenou častými opakujícími se činnostmi a unavenou prací); nedostatek znalostí (nejednoznačnost nebo nepochopení); rozptýlení (zmatek, duševní chaos); nedostatečná týmová spolupráce (nekonzistentní úsilí skupiny lidí kvůli nedostatku sounáležitosti, strachu z jiných chyb, nevhodnému stylu vedení nebo nevhodné komunikaci); únava (je ignorována, protože ji lidé vnímají poté, co je nadměrná); nedostatek prostředků (nedostatek zdrojů, nástrojů a materiálů, nedostatečná dokumentace, nevhodné pracovní podmínky); nátlak (od nadřízených nebo kolegů, nedostatek času, nesprávné nastavení úkolu); nedostatek sebevědomí (neschopnost odmítnout provádět úkoly vyplývající z nedostatku sebevědomí, úzkosti nebo komplexů); stres (nervozita způsobená např.: časový tlak, nová metodika, změna rozsahu úkolů, soutěže nebo soukromé faktory); nedbalost (nesprávné posouzení možných důsledků jednání způsobeného např.: nátlakem, nedostatkem zkušeností nebo nedostatkem znalostí); přijatelnost velkého počtu odchylek od pokynů a norem s cílem usnadnit práci.

Jak již bylo výše uvedeno, cílem návrhu *SKFS* je vytvořit výrobní proces, který je ziskový, ekonomický, bezpečný a neohrožuje veřejná aktiva, zejména lidi a životní prostředí. Toho lze dosáhnout optimalizací bezpečnostních, ekonomických a funkčních kritérií. Proto projekt *SKFS* pokrývá širokou škálu problémů, např. výběr: materiálů; technických principů; postupy výstavby;

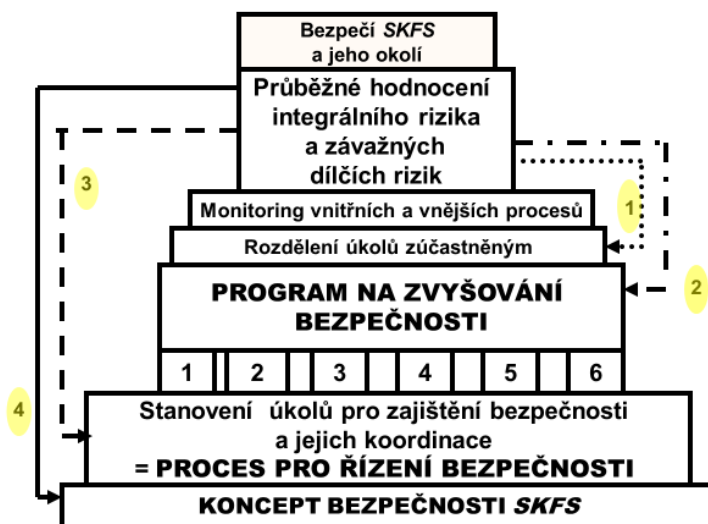
postupy konstrukce; stanovení kritických procesů výstavby a konstrukce; způsobů ochrany v doménách fyzických, kybernetických atd.

Projektování proto vyžaduje účast mnoha různých znalostních oborů, tj. Je třeba mít na paměti, že zde se právě nejvíce projevuje lidský faktor. *Nízká spolupráce odborníků vede k chybám, ke kterým dojde později při provozu*, např. problémy s údržbou [13,14]; nemožnost opravovat důležité díly [25] atd. Proto je třeba již od začátku zvažovat základní logiku zacílenou na budování bezpečí, která je zobrazena na obrázcích 3 a 4.



Obr. 3- Procesní model vytváření bezpečí, jeho vstupy a výstupy.

V každém projektu SKFS z hlediska bezpečnosti je nutné dodržovat požadavky na: trvanlivost; ovladatelnost zařízení a procesů; životnost; lidské zdroje; náklady; technické a jiné služby; bezpečí zaměstnanců, lidí v okolí a životního prostředí. Zvážení a řádné zajištění těchto požadavků určuje budoucí náklady na zajištění bezpečnosti a koexistence technického díla či zařízení s okolím. Například nezajištění lidských zdrojů pro provoz vede k omezení výroby nebo služeb poskytovaných SKFS [12]. Do ovladatelnosti patří i jasné naplánování rozdělení odpovědností za úkony, a to jak technické, tak organizační a kontrolní [14].



Obr. 4 - Model řízení bezpečnosti SKFS v čase. Procesy: 1- koncepce a řízení; 2 - administrativní postupy; 3 - technické záležitosti; 4 - vnější spolupráce; 5 - nouzová připravenost; a 6 - dokumentace a šetření havárií. Čísla ve žlutém kroužku označují zpětné vazby, které se aplikují, když integrální riziko nebo závažné dílčí riziko se ukáže nepřijatelné.

Projektování SKFS je velmi složitá činnost a v každé zemi je upravena vnitrostátní legislativou (např. v České republice zákon č. 183/2006 Sb.) a v některých případech mezinárodními předpisy [26,27]. Výsledky výzkumu [12] ukazují, že z hlediska bezpečnosti je hlavním cílem odvrátit nežádoucí kombinace nehod a selhání, které mohou způsobit havárie doprovázené velkými škodami. K tomuto účelu se používají proaktivní ukazatele nebo bezpečnostní funkce, které udržují bezpečnost při

hraničných a popř. i přeshraničních (nadprojektových) podmínkách tak, aby nedošlo k výskytu závažné havárie.

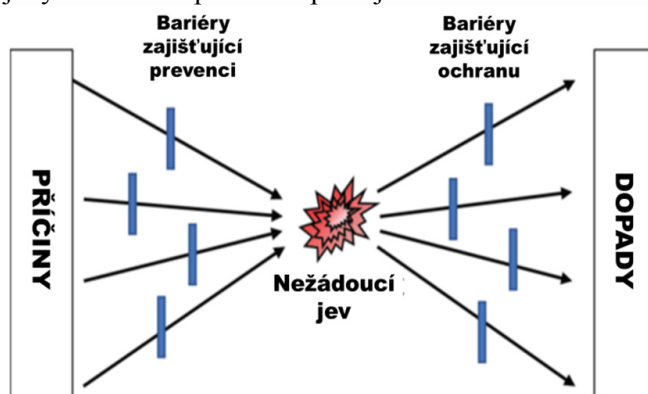
Při projektování se používá sedm principů resilience (pružné odolnosti): zálohování; vkládání schopnosti pozvolné a řízené degradace; vkládání schopnosti návratu zařízení ze zhoršeného stavu do stavu normálního; flexibilita jak v systému, tak v organizaci provozu; vkládání schopnosti řídit mezí podmínky v blízkosti rozhraní; vkládání optimálních modelů řízení; snižování složitosti; a snižování možnosti výskytu nežádáných spřažení.

Do projektu je nutné zahrnout možnosti pro aplikaci programu na zvyšování bezpečnosti (obrázek 4), který zajišťuje: bezpečnost a funkčnost všech zařízení, které odpovídají jejich poslání; identifikaci, hodnocení, eliminaci nebo regulaci potenciálních rizik na přijatelné úrovni pro důležitá zařízení, systémy a jejich různé části; řízení rizik od všech zdrojů uvnitř i vně SKFS, které nelze odstranit; ochranu personálu, osob v okolí, zařízení a majetku; používání nových materiálů nebo výrobků a zkušebních technik pouze způsobem, který je spojen pouze s minimálním rizikem; vkládání faktorů pro podporu bezpečnosti, které zajišťují nápravná opatření, která vedou ke zlepšení; a zvažování všech vhodných historických údajů pro zajištění bezpečnosti generované podobnými programy na zvyšování bezpečnosti.

Umění projektanta spočívá v tom, jak rozdělí zvládání rizik mezi preventivní opatření zabudovaná do projektu a opatření, které se provedou při odezvě, až se riziko realizuje; diagram bow-tie na obrázku 5. V druhém případě musí projektant uspořádat technické prvky a komponenty tak, aby byla možná údržba, testování, inspekce a byly tam i technické prvky, které umožní odezvu.

Z technického hlediska v projektu SKFS:

- jsou: stanoveny podmínky a limity pro provoz; instalovány systémy pro podporu bezpečnosti (aktivní, pasivní a hybridní); a zajištěny vhodné zálohy,
- je vyřešeno: jaké systémy pro podporu bezpečnosti jsou vhodné a co musí být jejich zálohou; kde / kdy systémy pro podporu bezpečnosti systémy fungují nejúčinněji; proč musí být používány právě tam a ne jinde; a v jakých mezích spolehlivě pracují.



Obr. 5 - Bow-time diagram – rozdělení opatření na snížení rizik mezi projekt a odezvu při provozu SKFS.

Je skutečností, že při navrhování SKFS se často používají software pro identifikaci šíření škodlivých jevů založená na stromových modelech. Na základě současných poznatků shrnutých v [20] je třeba mít na paměti, že modely stromů nevytvářející základ pro zvládnutí všech možných pohrom, které jsou zdrojem rizik, jež ovlivňují celý SKFS, protože začínají v jednom bodě technického díla či zařízení. Např. nelze jimi modelovat dopady vnějších živelních pohrom, útoků a lidského faktoru, které postihnou najednou více míst SKFS. Přitom právě většina velkých havárií technických děl vznikla současnou kombinací několika malých nehod a selhání [19].

Podle [10,11,30-33] je pro bezpečnost SCPS během životnosti nutné při navrhování zvážit u každého kritického procesu problémy spojené s: daným procesem; projektem procesu; řízením procesu; provozním personálem a signalizováním jeho stavu; systémem řízení bezpečnosti; dalšími



technickými systémy, ktoré podporujú bezpečnosť; externími aktívnymi a pasívnymi systémy pro zmírnění rizik, která vedou k selhání procesu; nouzovou odezvou *SKFS*; a odezvou v okolí *SKFS*.

Podle poznatků shrnutých v [12,14] je důležité, aby strategie řízení rizik procesů používala: zásady inherentní bezpečnosti; systémy pasivní bezpečnosti; systémy aktivní bezpečnosti; různé typy bariér; a procedurální postupy, které jsou prokázány nebo důkladně otestovány tak, aby za možných podmínek neobsahovaly latentní zdroje nebezpečí [12].

Pro zajištění bezpečnosti *SKFS* se při projektování používá princip "obrana do hloubky" [32]. Uvedený princip je zajištěn promyšlenou kombinací několika následných, téměř nezávislých úrovní ochrany. Jeho základním cílem je zajistit, že když selže jedna úroveň ochrany nebo bariéry, tak je k dispozici následující úroveň. Pokud je přístup dobře aplikován, tak by nemělo individuální technické, lidské nebo organizační selhání vést k ničivým dopadům a kombinace současných několika selhání vedoucí k ničivým dopadům by měla mít jen nízkou pravděpodobnost výskytu [12,25].

Z odborného hlediska musí finální projekt obsahovat dokument o bezpečnosti (bezpečnostní zpráva) *SKFS*, ve kterém jsou obsaženy odpovědi na otázky: co se může porouchat; co nemusí fungovat (identifikace nebezpečí a jeho analýza); jak závažné mohou být důsledky (posouzení rizik); jaká opatření je třeba přijmout, aby se tomu zabránilo (řízení rizik); co je třeba udělat, když k tomu dojde (opatření odezvy).

3. ÚDAJE A METODY POUŽITÉ PŘI VÝZKUMU

Pro výzkum byla sestavena původní databáze havárií a selhání *SKFS* ze světových údajů [25]. Databáze obsahuje 7829 událostí ze světových zdrojů za posledních 35 let, které byly autorům práce [12] přístupné; 521 událostí vzniklo kvůli chybám při projektování. V práci [12] je podrobně analyzováno několik případových studií, které ukazují, jak zanedbání v projektu vede k nepřijatelným dopadům. Při jejich vyhodnocení byly použity metody: What, If; Kontrolní seznam; diagram rybí kosti; případové studie; strom událostí; FMECA; atd. [33].

Příčiny selhání *SKFS* vzniklé při projektování byly kriticky posouzeny a rozděleny do tříd podle podobnosti příčin a vytvořily základ pro zpracování systému pro podporu rozhodování o rizicích (decision support system-*DSS*). Předmětný nástroj umožňuje vícekritériální posouzení možných rizik *SKFS* a stanovení velikosti celkového (integrálního) rizika [12]. Výsledky získané z analýzy faktů získaných z poučení při odezvách na dopady rizik byly rovněž kriticky posouzeny a rozděleny do tříd podle podobnosti nástrojů odezvy a vytvořily základ pro plán řízení rizik, který je založen na metodě řízení TQM [34] a je doporučen normou ISO 31000 [35]. Předmětný plán obsahuje opatření, která je třeba přijmout při projektování, aby se předešlo realizaci závažných rizik.

4. PŘÍČINY RIZIK *SKFS*, KTERÉ MAJÍ PŮVOD V PROJEKTOVÁNÍ

Jelikož projektování je lidská činnost, tak jde o řízení rizik, které vyvolávají tzv. organizační havárie. Původci organizačních havárií jsou projektant, zadavatel projektu a dozorné orgány [12,14,36]. Příčiny selhání *SKFS* a nehod v databázi [25] byly rozděleny do kategorií: věcné nedostatky v projektování *SKFS*; nedostatky při výkonu dohledu investora, budoucího provozovatele a veřejné správy nad projektováním; nedostatky právních předpisů; a další. Tyto kategorie byly pak dále rozděleny. Konkrétními zjištěné příčiny selhání a nehod *SKFS* zjištěných při navrhování jsou opomenutí, chyby a nedostatky při:

1. Projektování *SKFS* – věcná oblast:

- chyby v zadávacích podmínkách (nepoužit postup All Hazard Approach – tj. zanedbání některých možných pohrom možných v lokalitě; nesprávně stanovená velikost ohrožení (podcenění velikosti pohrom – např. jen aplikací deterministických anebo pravděpodobnostních metod; tj. nepoužití teorií dovolujících stanovení extrémů z důvodu nepravidelnosti a řídkosti výskytu extrémních jevů),



- chyby v projekte (pro výpočty použit nevhodný model stavby s ohledem na podmínky v lokalitě, a to buď příliš teoretický, nebo obecný či neměl vypořádaný nejistoty a neurčitosti; nezpracován správně princip Defense-in-depth)
 - nezvážení zranitelnosti lokality (např. velké množství obyvatel, existenci objektů jako jsou nemocnice, školy apod.; nedostatečně kapacitní zdroje energie, vody a kanalizace, nedostatečná kapacita dopravních cest, nedostatek personálu k obsluze apod.),
 - neurčení kritických míst stavby, a tudíž nepřijetí opatření na základě vyhodnocení rizik k jejich bezpečnosti, tj. k zajištění jejich spolehlivosti a zachování provozuschopnosti za abnormálních a kritických podmínek (bariéry, zálohy),
 - neurčení kritických míst technologie a výrobních procesů, a tudíž nepřijetí opatření na základě vyhodnocení rizik k jejich bezpečnosti, ochraně a k zachování provozuschopnosti za abnormálních a kritických podmínek (bariéry, zálohy, principy ke zvýšení bezpečnosti),
 - nebyla určena a v projektu zvážena a odpovídajícím způsobem řešena kritická místa technologie (tlaková zařízení, ve kterých jsou nebezpečné látky, anebo v nich probíhají nebezpečné reakce či natlakovaná potrubí, hlavně ta s nebezpečnými látkami) a místa, ve kterých je nebezpečí selhání obsluhy z pohledu možných rizik,
 - nedodržení norem a přístupů dobré praxe či použití chybných norem, což způsobilo, že v projektu navrženy: nevhodné materiály; nevhodné technické principy; nevhodné postupy výstavby; nevhodné postupy konstrukce; nebyly stanoveny kritické procesy výstavby a konstrukce a navržena specifická opatření pro jejich kvalitní provedení; zařízení, stroje, komponenty a systémy nesplňovaly požadavek na bezpečnost, spolehlivost a dlouhodobou funkčnost, tj. trvanlivost a snadnou ovladatelnost zařízení a procesů; nerespektovány ergonomické požadavky obsluhy, nároky servisu, údržbu a finanční náklady s nimi spojené; nevhodné umístění ochranných zařízení a systémů na podporu bezpečnosti; nevhodné technologie výstavby, konstrukcí a montáže,
 - při vytváření projektu automatických a poloautomatických systémů řízení byly nedostatky způsobené nedostatečným poznáním nebo nedostatečnou spoluprací specialistů z různých oborů či použitím chybných nebo nedokonalých nástrojů IT,
 - nezpracování technických opatření pro základní fyzickou a kybernetickou ochranu SKFS,
 - nezvážení možností změn v: zákonech během výstavby; systému daní během výstavby; systému úroků během výstavby; situaci na trhu – inflace, deflace, změny poptávky aj.; podpory SKFS ze strany státu (např. při změně politické reprezentace); dodávkách zásadních materiálů a technologií a spoléhalo se jen na jednoho dodavatele, což vedlo k problémům při výstavbě a provozu – např. z nedostatku financí či nedostupnosti daného materiálu pak byly ošizeny některé stavby a vybavení.
2. Dohled veřejné správy nad projektováním a zhotovováním SKFS– organizační oblast:
- nedostatečný dohled veřejné správy, např. nevyžadovala dokumentaci o průkazu bezpečnosti technického díla (tj. v českém slangu bezpečnostní dokumentaci) ve všech důležitých sledovaných šesti etapách SKFS,
 - zanedbání řešení dostatečné kapacity místních zdrojů energie, vody a kanalizace, dopravních cest a personálu při umístění a projektování SKFS,
 - dovolena významná kontaminace životního prostředí a dlouhodobé narušení života místních obyvatel při výstavbě,
 - zanedbání posouzení finanční schopnosti zhodnotitele a investora při udělování příslušných povolení.
3. Nedostatečná legislativa:
- nedostatečná kontrolní pravomoc veřejné správy,
 - nedostatečná legislativa upravující požadavky na projektování, zhotovení a uvedení do provozu SKFS (příliš obecná, neúplná, dovoluje několikerý výklad),
 - nedostatečná vynutitelnost práva na úseku bezpečnosti, ochrany zaměstnanců, ochrany veřejnosti a životního prostředí.

4. Jiné:

- stát neměl zajištěnu odbornou instituci, která byla schopna odborně posoudit proces zhotovení SKFS po všech stránkách,
- uspěchanost při projektování a výstavbě kvůli tlaku politiků,
- stát neměl vypracován systém dohledu nad projektováním a zhotovováním SKFS,
- stát neměl kritéria na posuzování správnosti projektování a zhotovování SKFS,
- zhotovitel a investor během projektování a zhotovování SKFS nespolupracovali s veřejnou správou,
- výskyt přírodní katastrofy jako: zemětřesení; sesuv půdy; povodeň; Oheň výskyt jevů jako: korupce; útok zasvěcených osob; útok hackerů; teroristického útoku.

Schématický jsou příčiny rizik spojené s projektováním ukázány na obrázku 6.

Kritická vyhodnocení havárií a selhání SKFS [19] ukázala, že předmětné jevy jsou způsobeny buď velkou pohromou (obvykle živelnou), anebo náhodnou kombinací mnoha “malých” škodlivých jevů nahromaděných v krátkém časovém okamžiku, která se stane ničivou, i když jednotlivé škodlivé jevy ničivý potenciál nemají. Protože druhý případ je častější (70-80 %), je třeba již v projektování **zvažovat kombinace škodlivých jevů**. Některé kombinace zatížení se zvažují u jaderných zařízení [27], ale i tam je třeba podle výsledků analýz havárií v posledních 30 letech zvýšit jejich počet.

5. PLÁN ŘÍZENÍ RIZIK PŘI PROJEKTOVÁNÍ

Plán řízení rizik pro proces projektování je po principech prevence druhým důležitým nástrojem pro projektování SKFS. Zabraňuje opakování chyb minulých projektantů SKFS. Při vytváření tohoto špičkového nástroje řízení bezpečnosti v konkrétním případě je nutno zvažovat jak současné znalosti a zkušenosti s riziky spojenými s SKFS a jejich okolím shrnuté v [12], tak nové skutečné poznatky, které se získají analýzou místních podmínek. Cílem plánu řízení rizik je zajistit koexistenci SKFS s okolím. Uvažuje se o dvou hlavních aktérech, a to veřejné správě, která dohlíží na činnost na území včetně SKFS s cílem zajistit bezpečnost území a občanů, a projektantovi, který je zodpovědný za bezpečnost projektu SKFS, která zahrnuje také ochranu okolí a obyvatel. Povinnosti v oblasti druhého aktéra mají i investor a budoucí provozovatel SKFS. Plán řízení rizik se připravuje ve formě tabulky. Tabulka 1 ukazuje výtah z kompletního plánu řízení rizik při projektování, který je uveden v [12].



Obr. 6 - Příčiny selhání koexistence SKFS a jeho okolí z důvodu nedostatků či chyb při projektování, zhotovení a spouštění technického díla do provozu

Tab. 1 - Plán řízení rizik pro projektování technického díla (SKFS)

Oblast původců rizika	Popis rizika	Pravděpodobnost výskytu Velikost dopadů	Opatření na zmírnění rizika
Veřejná správa	V důsledku neexistence strategie státu na úseku řízení projektování technických děl zacílené na bezpečnost je možné upřednostnění momentálních politických zájmů, prosazení požadavků nátlakových skupin či nezvládnutí extrémních politických situací (válka, teroristické útoky), což následně vede ke snížení životní úrovně a bezpečí občanů, ekonomické nestabilitě apod.	Pravděpodobnost: velká Dopady: velké	Opatření: vypracovat příslušnou strategii ČR a upravit stavební zákon Provede: předseda vlády Odpovědnost: předseda parlamentu
			
	V důsledku nedostatečné kompetence orgánu veřejné správy při dozoru nad projektováním technických děl dochází k prodlužování výstavby, problémům při uvedení do provozu či k haváriím doprovázenými enormními výdaji z veřejného rozpočtu, narušení bezpečí občanů	Pravděpodobnost: velká Dopady: velké	Opatření: upravit kompetenční zákon a zákony s ním spojené, zákon o krajích a zákon o obcích Provede: předseda vlády ministr vnitra Odpovědnost: předseda Parlamentu
Investor technického díla			
	V důsledku chyb při výběru autorizovaného projektanta (nedostatečné znalosti a zkušenosti ze všech oborů, které musí být zohledněny v projektu) je projekt nekvalitní, což dříve nebo později naruší výstavbu nebo provoz technického díla a povede k haváriím doprovázenými enormními výdaji, narušení bezpečí občanů a k problémům s veřejnou správou	Pravděpodobnost: střední Dopady: velké	Opatření: změna projektanta Provede: pověřený pracovník investora Odpovědnost: ředitel investora
	V důsledku nezvážení průřezových rizik (spojených s propojeními zařízení, IT a člověk-stroj) v provedených bezpečnostních analýzách dojde dříve nebo později k narušení výstavby nebo provozu technického díla a povede k haváriím doprovázenými enormními výdaji, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: velká Dopady: velké	Opatření: zajistit, aby projektant provedl nápravu na své náklady a ve stanovené době Provede: pověřený pracovník investora Odpovědnost: ředitel investora
Budoucí provozovatel			
	V důsledku nepřesně zadaných požadavků na technické dílo projekt nekvalitně vyřeší místní specifika a dojde dříve nebo později k narušení výstavby nebo provozu technického díla a povede k haváriím doprovázenými enormními výdaji, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: zajistit, aby investor provedl nápravu Provede: pověřený pracovník budoucího provozovatele Odpovědnost: ředitel budoucího provozovatele

	V dôsledku špatného odhadu nárokov technického diela na energiu, dopravu, dodávky vody, kanalizáciu, likvidáciu odpadů je projekt postavený na nereálnych datech, čož dříve nebo později k narušení výstavby nebo provozu technického diela, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: zajistit, aby investor provedl nápravu, a jednat s veřejnou správou s cílem najít vyřešení problému Provede: pověřený pracovník budoucího provozovatele Odpovědnost: ředitel budoucího provozovatele
			
Autorizovaný projektant technického diela			
	V důsledku neznalosti nebo nepoužití požadované legislativy, norem a osvědčených principů dobré inženýrské praxe a výsledků práce s riziky je projekt nekvalitní a dříve nebo později k narušení výstavby nebo provozu technického diela, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: zajistit nápravu, buď vlastními zdroji, anebo vnějšími zdroji přes objednávku Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
	V důsledku nejasného a nekompletního plánu prací na projektu ve formě ověřeného kontrolního seznamu a dříve nebo později dojde k narušení výstavby nebo provozu technického diela, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: stanovit jasný harmonogram prací, jejich kvality, cílů a termínu dodání Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
	V důsledku nedostatečných znalostí nebo financí nebyl vyžádán specifický průzkum místních podmínek, což vede dříve nebo později k narušení výstavby nebo provozu technického diela, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: u investora vyžádat nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
	V důsledku nedostatečné legislativy chybí v projektu opatření pro ochranu veřejných aktiv, limity a podmínky pro provoz kritických zařízení, záložní zdroje pro zvládnutí nouzových a kritických situací, což vede dříve nebo později k narušení výstavby nebo provozu technického diela, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: u investora vyžádat nápravu a popř. požádat o podporu veřejnou správou Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
	V důsledku nedostatečných znalostí zpracovatele projektu a špatného dohledu investora a veřejné správy použita technologie zpracování projektu způsobila nedostatky v projektu, které dříve nebo později povedou k narušení výstavby nebo provozu technického diela, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: doplnit tým o odborníky ve spolupráci s investorem a provést nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
	Nezpracování kompletní technické dokumentace (např. není přesný popis všech zařízení a způsobu jejich provozu) vede dříve nebo později k narušení výstavby nebo provozu technického diela, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: střední Dopady: velké	Opatření: doplnit tým o odborníky ve spolupráci s investorem a provést nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta

	Nezvážení technických děl v okolí, která mohou způsobit selhání či havárii předmětného technického díla vede dříve nebo později k narušení výstavby nebo provozu technického díla, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: velká Dopady: velké	Opatření: doplnit tým o odborníky ve spolupráci s investorem a provést nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
	Nezvážení výskytu situací, které mohou vyžadovat vícenáklady (např. zvýšení daňového zatížení, změna podpory ze strany veřejné správy, výskyt živelní či jiné pohromy apod.) vede dříve nebo později k narušení výstavby nebo provozu technického díla, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: velká Dopady: velké	Opatření: doplnit tým o odborníky ve spolupráci s investorem a provést nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
	Chybné rozdělení investičního celku do etap vede dříve nebo později k narušení výstavby nebo provozu technického díla, enormním výdajům, narušení bezpečí občanů a k problémům s veřejnou správou.	Pravděpodobnost: velká Dopady: velké	Opatření: ve spolupráci s investorem a provést nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
			
Živelní pohroma, požár objektu	V důsledku výskytu dojde k narušení práce na projektu, což povede k nedodržení termínu, anebo ke snížení kvality projektu, což naruší další fáze zhotovení technického díla a povede k nedodržení termínu zhotovení a s tím spojenými vícenáklady a vícepracemi (např. údržba a fyzická ochrana zabraného území)	Pravděpodobnost: malá Dopady: střední	Opatření: ve spolupráci s investorem a provést nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
Selhání techniky, havárie, selhání kritických infrastruktur	V důsledku výskytu dojde k narušení práce na projektu, což povede k nedodržení termínu, anebo ke snížení kvality projektu, což naruší další fáze zhotovení technického díla a povede k nedodržení termínu zhotovení a s tím spojenými vícenáklady a vícepracemi (např. údržba a fyzická ochrana zabraného území)	Pravděpodobnost: malá Dopady: velké	Opatření: ve spolupráci s investorem a provést nápravu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
Insider	V důsledku výskytu dojde k chybám v na projektu, což povede k nedodržení termínu, anebo dokonce k narušení dalších fází zhotovení, či dokonce provozu technického díla, což si vyžádá vícenáklady, a způsobí narušení bezpečí, či dokonce újmy na životním prostředí a poškození zdraví zaměstnanců či lidí v okolí technického díla a problémy s veřejnou správou	Pravděpodobnost: malá Dopady: střední až velké	Opatření: budovat kulturu bezpečnosti a motivovat pracovníky k práci zacílené na plnění úkolů Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta

Teroristický útok	V dôsledku výskytu dojde k chybám v na projektu, čo povede k nedodržaniu termínu, alebo ke zníženiu kvality projektu, alebo dokonca k narušeniu ďalších fáz zhotovenia, či dokonca provozu technického diela, čo si vyžaduje vícenáklady, a spôsobí narušenie bezpečia, či dokonca ujmy na životnom prostredí a poškodenie zdravia zamestnancov či ľudí v okolí technického diela a problémy s verejnou správou	Pravdepodobnosť: malá Dopady: strední až veľké	Opatrenia: ve spolupráci s investorm provést nápravu, tj. odevzu a obnovu, a zlepšit fyzickou ochranu a ostrahu pracoviska Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
Finanční krize	V důsledku výskytu dojde k nedostatku financí, což povede k chybám v projektu, zastavení prací na projektu či k nedodržení termínu dokončení projektu, a s tím spojeným narušením dalších fází zhotovení a k opoždění provozu technického diela, což způsobí vícenáklady, a sociální problémy (nezaměstnanost a narušení bezpečia), či dokonca ujmy na životnom prostredí a tím i problémy veřejné správě (náklady na sociální dávky, boj proti kriminalitě apod.)	Pravdepodobnosť: malá Dopady: strední až velké	Opatrenia: ve spolupráci s investorem a veřejnou správou provést ochranná opatření a zjistit přijatelný způsob řešení úkolu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta
Válka	V důsledku výskytu dojde k nedostatku financí, personálu, změně podpory státu apod., což povede k chybám v projektu, zastavení prací na projektu či k nedodržení termínu dokončení projektu, a s tím spojeným narušením dalších fází zhotovení a k opoždění provozu technického diela, což způsobí vícenáklady, a sociální problémy (nezaměstnanost a narušení bezpečia), či dokonca ujmy na životnom prostredí a tím i problémy veřejné správě (náklady na sociální dávky, boj proti kriminalitě apod.)	Pravdepodobnosť: malá Dopady: velké	Opatrenia: ve spolupráci s investorem a veřejnou správou provést ochranná opatření a zjistit přijatelný způsob řešení úkolu Provede: pověřený pracovník projektanta Odpovědnost: ředitel projektanta

Plán řízení rizik při projektování SKFS slouží k ochraně před problémy, které z pohledu správnosti projektu bezpečného technického diela (SKFS) by měly bránit vydání stavebního povolení. Tabulka 1 ukazuje, že velkou roli hraje lidský faktor, a to při plnění kritických úkolů projektování (sestavování zadávacích podmínek, využití znalostí o tvorbě bezpečného projektu atd.), a při dohledu prováděného veřejnou správou, který musí být zaměřen na veřejný zájem.

Plán řízení rizik byl úspěšně testován na šesti středních SKFS [25]; jejich sestavování pro konkrétní místně specifické podmínky je v praxi náročné, pokud jde o znalosti a čas odborníků, a vyžaduje přístup k podrobným dokumentům SKFS a veřejné správy, které jsou spojeny s dodržováním určitých právních předpisů.

6. POSTUP VYTVOŘENÍ PROJEKTU SKFS ZALOŽENÉHO NA ŘÍZENÍ RIZIK

Na základě výše uvedených skutečností a zkušeností z praxe je sestaven postup pro sestavování projektu SKFS založený na řízení rizik, který respektuje platné normy, osvědčené postupy pro projektování a výše uvedené zásady pro řízení rizik. Vzhledem k tomu, že v mnoha případech je nutné při rozhodování o problému vzít v úvahu i protichůdná kritéria, použili jsme jak jednoduché metody při práci s riziky (lineární a stromové), tak nástroj s více kritérii, tj. DSS [12,19,36] pro každou komponentu, propojení komponent, výrobní proces a celé technické dílo.

Při rozhodování o konkrétních položkách je nutno použít jak dílčí rizika kritických komponent a systémů a jejich propojení, tak integrovaná procesní rizika i integrální riziko celku. Je třeba zvážit



všechny zdroje rizik uvedené v kapitole 4 a určit jejich velikosti pro uvedené položky, které mají parametry požadované normami. U všech relevantních zdrojů rizik je třeba určit velikosti dopadů a podle nich navrhnout vhodná opatření, tj. změny vlastností sledované položky vedoucí ke zvýšení bezpečnosti.

Základním úkolem projektanta je rozpoznat všechna možná ohrožení aplikací přístupu All-Hazard-Approach, který byl vysvětlen výše a rozdělit je na přijatelná, podmíněně přijatelná (tolerovatelná ve smyslu ALARP) a nepřijatelná. V případě druhém a třetím musí projektant přemýšlet následujícím způsobem:

- Jak mohu eliminovat dané ohrožení?
- Jak mohu snížit velikost tohoto ohrožení?
- Nemohu navrženými opatřeními na zvládnutí daného ohrožení vytvořit nové ohrožení?
- Jaké technické a řídicí systémy je nutno použít pro řízení ohrožení, které zbylo?

Pro řízení bezpečnosti *SKFS* při provozu podle [12,19] v rámci tvorby projektu je nutné vytvořit:

- podmínky pro utváření kultury bezpečnosti při provozu *SKFS*, které jsou prováděny: dodržováním bezpečnostních pravidel a postupů; odpovědností vedoucích pracovníků; provozováním systémů hlášení na pracovišti; audity na pracovišti; komunikací se zaměstnanci; proaktivními přístupy k řízení rizik; zajištěním bezpečného pracoviště; komunikacemi o bezpečnosti a školeními zaměstnanců,
- správnou politiku prevence ztrát prováděnou řízením bezpečnosti (jde o vyšší prioritu než v případě orientace jen na spolehlivost),
- jasné rozdělení odpovědností (důležitý je soulad mezi pravomocemi a odpovědnostmi),
- rozřídění zařízení, konstrukčních částí a systémů podle kritičnosti,
- provozní předpisy pro normální, abnormální a kritické podmínky,
- správné režimy pro provoz zařízení, součástí a systémů, zejména kritických,
- souhrn kritických aktiv-jejich limity a podmínky a požadavky na kontroly založené na rizicích (risk-based inspections-RBI),
- plán údržby podporující bezpečnost (zvažuje prevenci a prognózy chování kritických zařízení, součástí a systémů),
- plán modernizace a obnovy zařízení, komponentů a systémů, zejména těch kritických,
- program nedestruktivních zkoušek kritických zařízení,
- nouzové (pohotovostní) plány,
- plán kontinuity, který zajišťuje přežití *SKFS* (zejména jeho kritických položek) v kritických i extrémních podmínkách.

Na základě výše uvedených znalostí a zkušeností z praxe shrnutých v pracích [12,14,18,19,25,36,37], navrhuje techniku sestavování návrhu založeného na řízení rizik:

- Vytvořit seznam součástí (prvky, komponenty) a systémů, které splňují normy a budou spojovány do dílčích celků.
- Pro všechny položky v seznamu součástí a systémů (bod 1), které splňují stanovené normy a standardy určit limity a podmínky z hlediska jejich provozu na určitém místě, pokud jde o: a) materiál, ze kterého jsou vyrobeny; požadavky na provozuschopnost; pracovní režim, ve kterém budou pracovat; lidský faktor; a možná další rizika (vnitřní požár nebo výbuch a důležitá vnější rizika).
- Pro všechny položky v seznamu součástí a systémů (bod 1) určit pro zdroje rizik specifické pro lokalitu či místo, ve které je *SKFS* či sledované položky umístěné se zvažováním přístupu All-Hazard-Approach velikosti a charakteristiky dílčích rizik.
- Pro všechny zdroje rizika (bod 3) stanovit scénáře dopadů pro nejméně příznivé podmínky; a pokud některé dopady rizik nejsou přijatelné, je nutné zvýšit požadavky na materiál, ze kterého jsou zhotoveny komponenty či systémy tak, aby tato rizika byla přijatelná. Není-li to

možné, je třeba vložit do projektu *SKFS* opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní kvalitní odezvu na realizaci příslušného rizika při provozu.

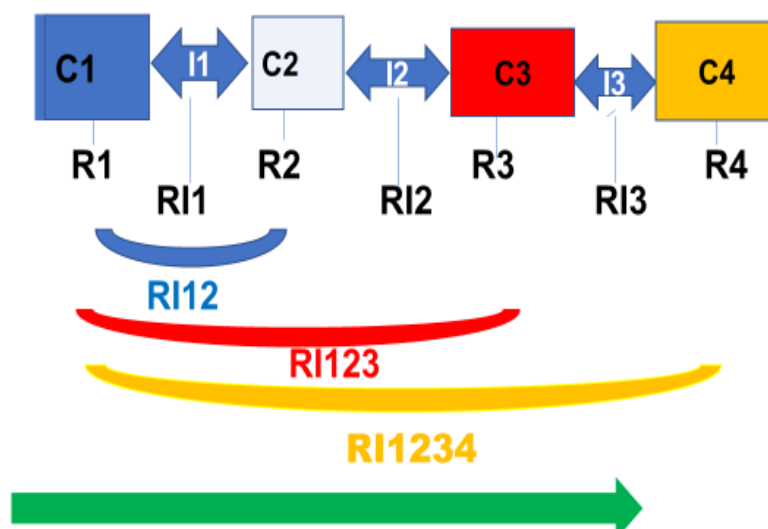
- Vytvořit propojení komponent a model jejich propojení, který splňuje normy a požadavky na inherentní bezpečnost.
- Pro všechna propojení (bod 5) určit limity a podmínky z hlediska jejich materiálového složení, způsobu provedení (volné, těsné nebo složité), metody propojení (svary, šrouby, nýty, lepení atd.) a realizace možných dalších rizik (vnitřní požár nebo výbuch, lidský faktor a vnější rizika).
- Pro zdroje rizik (bod 3) stanovit scénáře dopadů dílčích rizik pro všechna propojení (bod 5) a integrované riziko pro celek, které je vytvořen propojením komponent či systémů; nejsou-li dílčí rizika a integrované riziko přijatelné, je nezbytné zvýšit požadavky na materiál či způsob provedení propojení komponent či systémů tak, aby tato rizika byla přijatelná. Není-li to možné, je třeba vložit do projektu *SKFS* opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní kvalitní odezvu na realizaci příslušného rizika při provozu.
- Pro zdroje rizik (bod 3) určit pro každý výrobní proces scénáře dopadů procesu pro nejméně příznivé podmínky, které ukazují dopady integrovaného rizika (tj. rizika procesu). V případě, že integrované riziko není přijatelné, zvýšit nároky na projekt: komponent výrobního procesu; pracovní režim; a operátory, aby rizika mohla být přijatelná. Není-li to možné, je třeba vložit do projektu *SKFS* opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní kvalitní odezvu na realizaci příslušného rizika při provozu.
- Pro zdroje rizik (bod 3) určit integrální riziko, tj. celkové riziko *SKFS*. Pokud je riziko přijatelné pouze podmíněně (ALARP), provádět změny technologie, které umožní okamžitou reakci s cílem navrátit se do normálního stavu. V případě nepřijatelného rizika je nutné se vrátit k úpravě rizik procesů, dílčích rizik komponentů, systémů a jejich propojení a zavést do projektu *SKFS* opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní realizaci principů jako je “selži bezpečně”, tj. neprováděj nebezpečný úkon, informuj obsluhu a popř. začni provádět stanovené úkony odezvy.
- S ohledem na zdroje rizika (bod 3) určit požadavky na systém řízení, tj. pro I&C i obsluhu za běžných, abnormálních a kritických podmínek. Zde je nutné, aby v každém okamžiku byly pro řízení k dispozici správné informace o stavu zařízení a okamžitých provozních podmínkách hlavně kritických zařízení a kritických procesů.

Příklad procesu projektování je zobrazen na jednoduchém obrázku 7. Nejprve se sestaví pro daný *SKFS* systém pro podporu rozhodování o rizicích jednotlivých komponent a jejich propojení, stanoví se stupnice pro hodnocení míry rizika – tabulka 2; 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 2 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 2 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 2 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 2 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. 7 - Schéma procesu projektování založeného na řízení rizik. Zelená šipka zobrazuje postup vytváření projektu.

Tabulka 2. 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 %

Výše uvedený postup generace projektu *SKFS* založeného na řízení rizik byl úspěšně testován na sedmi středně velkých *SKFS* [25,37]. V současné době je aplikován při sestavení projektu malého modulárního reaktoru [39].

7. ZAVĚR

Kvalita projektu *SKFS* předurčuje bezpečnost *SKFS* po celou dobu provozu. Příklady z praxe ukazují, že některé chyby, jako je podcenění základových podmínek nebo některé chyby v zadávacích podmínkách nelze po dokončení a uvedení technického díla do provozu odstranit. Za určitých podmínek (např. při povodni nebo zemětřesení) představujících nebezpečí a mohou být dopady zmíněných rizik zmírněny pouze organizačními opatřeními, která s sebou nesou dodatečné náklady a nejsou schopny zajistit úroveň bezpečnosti na takové úrovni, jako správná opatření ve fázi projektování [12,13,14,25].

Výše shrnuté znalosti a výsledky studia nehod a poruch *SKFS* ukazují, že základem pro zajištění bezpečnosti technických děl a zařízení v požadovaném životním cyklu jsou znalosti: právních předpisů, norem a standardů; rizik v místě, kde je technické dílo či zařízení umístěno; technického systému, který představuje technické dílo či zařízení; modelů a teorií spojených s haváriemi a selháními; metod analýzy, řízení a vypořádání rizik; a způsobu řízení, který by měl provozovatel používat po uvedení technického díla do provozu (finance, lidské zdroje, organizace, technologie,



inovace...). Kromě toho je nezbytné, aby všichni zúčastnění respektovali veřejný zájem, podíleli se na budování kultury bezpečnosti a aby manažeři motivovali zaměstnance ke kvalitní práci, a to i vlastním příkladem, jak ukazují tzv. zlatá pravidla [29]. Zásady pro jejich provádění musí být vloženy do projektu.

Analýza rozvoje životního prostředí a rozvoje politické, sociální a hospodářské situace ve světě ukazuje, že je třeba se připravit na řešení případů a opatření, která způsobí kritické situace s vyšší intenzitou dopadů, než je dnes. Aby bylo možné řídit realizace rizik, která jsou vlastní současnému světu, za použití odpovídajících sil, zdrojů a prostředků, je třeba mít: zásady pro zvládání nouzových a kritických situací, zejména těch, které jsou velkého rozsahu; zásady pro přidělování zdrojů; rozdělení odpovědností; a plán řízení rizik.

Při projektování složitých SKFS je nutné do projektu vložit racionální řízení každého procesu zacílené na bezpečnost procesu (proces safety management-PSM) a pro řízení celého technického díla vložit systém řízení bezpečnosti (safety management systém-SMS) [13,16,29]. Pro praxi je vytvořeno dvanáct metodik pro veřejnou správu [33], která ve veřejném zájmu provádí dozor nad všemi fázemi životnosti SKFS. Adaptované metodiky lze použít i pro práci s riziky v SKFS v případě externích zdrojů rizik. U interních zdrojů rizik je třeba vždy provádět zvláštní šetření, anebo uplatnit postupy používané v analogických SKFS, pokud jsou splněny podmínky pro přenos technologií [38].

Výsledky [12,36,37] 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 [12,14] 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 [25] odhalila, že dle platných pravidel není vyžadováno sledovat bezpečnost procesů při provozu ve fázi projektování, což občas vede k problémům v provozu [19]. 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. Na základě zkušeností z praxe [25,37] je sestaven postup pro vytváření projektu SKFS založeného na řízení rizik. Metodika byla otestována v několika případech a dále pokračuje její implementace do praxe.

Poděkování

Autorka děkuje podpoře z projektu RIRIZIBE CZ.02.2.69/0.0/0.0/16-018/00026 49.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

- [1] ALE, B., I. PAPAOGLOU and E. ZIO. *Reliability, Risk and Safety*. ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448 p.
- [2] BEER, M. and E. ZIO. *Proceedings of the 29th European Safety and Reliability Conference*. ISBN 978-981-11-2724-3. Singapore: ESRA 2019, e:enquiries@rpsonline.com.sg.
- [3] BÉRENGUER, C., A. GRALL and C. GUEDES SOARES. *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035 p.
- [4] BRIŠ, R., C. GUEDES SOARES and S. MARTORELL. *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362 p.
- [5] CEPIN, M. and R. BRIS. *Safety and Reliability – Theory and Applications*. ISBN 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.
- [6] HAUGEN, S., J. VINNEM, A. BARROS, T. KONGSVIK and A. VAN GULIK. *Safe Societies in a Changing World*. ISBN 978-1-351-17466-4. ISBN 978-1-62276-436-5. London: Taylor & Francis Group 2018, 3234 p.; <https://www.ntnu.edu/esrel2018>.
- [7] IAPSAM. *Probabilistic Safety Assessment and Management Conference*. ISBN: 978-1-62276-436-5. Helsinki: IPSAM & ESRA 2012, 6889 p.
- [8] NOWAKOWSKI, T., M. MLYŃCZAK, A. JODEJKO-PIETRUCZUK and S. WERBIŃSKA-WOJCIECHOWSKA. *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453 p.
- [9] PODOFILLINI, L., B. SUDRET, B. STOJADINOVIC, E. ZIO and W. KRÖGER. *Safety and Reliability of Complex Engineered systems: ESREL 2015*. ISBN 978-1-138-02879-1. London: CRC press 2015, 4560 p.
- [10] STEENBERGEN, R., P. VAN GELDER, S. MIRAGLIA and A. TON VROUWENVELDER. *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387 p.
- [11] WALLS, L., M. REVIE and T. BEDFORD. *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. ISBN 978-1-315-37498-7. London: CRC Press 2016, 2942 p.
- [12] PROCHÁZKOVÁ, D., J. PROCHÁZKA, J. LUKAVSKÝ, V. BERAN a V. SINDLEROVÁ. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 207 p. <http://hdl.handle.net/10467/84466>.
- [13] PROCHÁZKOVÁ, D. *Safety of Complex Technological Facilities*. ISBN 978-3-659-74632-1. Saarbrücken: Lambert Academic Publishing 2015, 244 p.
- [14] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. Praha: ČVUT 2017, 364 p. <http://hdl.handle.net/10467/72582>.
- [15] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. ISBN 978-80-01-06180-0, e-ISBN: 978-80-01-06182-4. Praha: ČVUT 2012, 318 p. ISBN 978-80-01-05103-0.
- [16] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.
- [17] PROCHÁZKOVÁ, D. *Challenges Connected with Critical Infrastructure Safety*. ISBN: 978-3-659-54930-4. Saarbrücken: Lambert Academic Publishing 2014, 218 p.
- [18] PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládnutí*. ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234 p.
- [19] PROCHÁZKOVÁ, D., PROCHÁZKA, J., 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.
- [20] PROCHÁZKOVÁ, D. *Analýza, řízení a vypořádání rizik technických děl*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. <http://hdl.handle.net/10467/78442>.



- [21] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washington: FEMA 1996.
- [22] RAUSAND, M. *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons 2014.
- [23] EPSTEIN, W. Not Losing to the Rain: What I Learned when I Learned about Onagawa. In: *Safety and Reliability of Complex Systems*. London: Taylor & Francis Group 2015, pp. 365-371.
- [24] REASON, J. *Human Error*. Cambridge: University Press 1990.
- [25] ČVUT. *Databáze pohrom, havárií a selhání technických děl, jejich příčin, poučení a opatření odevy*. Praha: ČVUT 2021.
- [26] EU. *Council Directive 82/501/EEC of 24 June 1982 on the Major-Accident Hazards of Certain Industrial Activities*. Brussels: EU 1982.
- [27] IAEA. *Safety Guides and Technical Documents*. Vienna: IAEA 1954–2020. www.ns.iaea.org/standards
- [28] COMAH, *Safety Report Assessment Manual: COMAH*. London: UK – HID CD2 London 2002, 570 p.
- [29] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for Developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191p.
- [30] HEIKKILÄ, A. M. *Inherent Safety in Process Plant Design. An Index-Based Approach*. Helsinki: VIT 1999, 132 p.
- [31] KLETZ, T., *Process Plants: A Handbook for Inherently Safer Design* CRC. London: Taylor&Francis Group 1998.
- [32] INSAG. *Defence in Depth in Nuclear Safety. INSAG-10*. Vienna: IAEA 1996.
- [33] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369 p.
- [34] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd. 1991.
- [35] ISO. *Risk Management – Principles and Guidelines. ISO 31000:2009*.
- [36] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Risk Management at Technical Facilities Designing, Building and Commissioning*. ISBN 978-80-01-06716-1. Praha: ČVUT 2020, 144 p. dspace.cvut.cz. <https://doi.org/10.14311/BK.9788001067161>.
- [37] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Tool for Risk Reduction at Specific Component Aircraft Engine Welding. In: *Proceedings of International European Safety and Reliability Conference, ESREL2018*. ISBN 978-1-351-17466-4. London: Taylor & Francis Group 2018, pp. 3135-3142. <https://www.ntnu.edu/esrel2018>.
- [38] PROCHÁZKOVÁ, D. Šetření podstaty konfliktů technických řešení. *Kontrola MSK ČR 1992*. Praha: MSK ČR, 95 p.
- [39] PROCHÁZKOVÁ, D., PROCHÁZKA, J., DOSTÁL, V. Oblasti důležité pro bezpečnost zdroje elektrické energie na bázi SMR. In: *Řízení rizik procesů a bezpečnost složitých technických děl*. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 319-370. <https://doi.org/10.14311/BK.9788001067864>.