ANALÝZA, ŘÍZENÍ A VYPOŘÁDÁNÍ RIZIK SPOJENÝCH S TECHNICKÝMI DÍLY

Dana Procházková

PRAHA 2018

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Recenzenti:

Prof., Ing. Josef Říha, DrSc.

Doc. Ing. Jiří Lukavský, CSc.

Doc. Ing. Václav Beran, DrSc.

Doc. RNDr. Miroslav Rusko, PhD.

Doc. RNDr. Dana Procházková, DrSc.

ISBN 978-80-01-06480-1

https://doi.org/10.14311/BK.9788001064801

OBSAH

ABSTRAKT

Předložená práce „***Analýza, řízení a vypořádání rizik spojených s technickými díly***“ se zabývá riziky spojenými s technickými díly, a to především složitými technickými díly. Ukazuje způsoby identifikace, analýzy, hodnocení, řízení a vypořádání rizik zacílené na bezpečnost technických děl a jejich okolí, a přitom respektuje současné poznání, že rizika jsou místně a časově specifická. Bezpečnost je chápaná jako vlastnost celého technického díla, kterou určuje kvalita souboru antropogenních opatření a činností zacílených na bezpečné technické dílo, a to i při jeho kritických podmínkách. Proto při jejím vytváření práce navrhuje sledovat aktiva veřejná i aktiva technického díla a zvažovat rozmanitost jejich fyzikálních podstat, zranitelností i proměn v čase; a to znamená průběžně řešit vzniklé konflikty.

Jelikož rizika jsou příčinou kritičnosti technických děl při procesech umísťování, výstavby, provozu i odstranění technických děl s ohledem na veřejná aktiva, tak za cíl je považováno zajištění koexistence technického díla s okolím, tj. s veřejnými aktivy, do kterých patří životy, zdraví a bezpečí lidí, majetek, veřejné blaho, životní prostředí, technologie a infrastruktury. S ohledem na dynamický vývoj světa, je třeba monitorovat všechna prioritní rizika a provádět jejich řízení a vypořádání s ohledem na zvyšování, anebo alespoň udržování bezpečnosti technických děl na přijatelné úrovni. To znamená budování systémů řízení bezpečnosti technických děl, které při práci s riziky respektují proměnnost světa v čase a prostoru, tj. normální, abnormální, kritické a v některých případech technických děl (např. vysoce nebezpečná jaderná zařízení) i extrémní podmínky, a proto mají připraveny postupy pro řízení a zvládnutí kritických situací.

Klíčová slova: pohromy - zdroje rizik; riziko; metody práce s riziky; technická díla; bezpečnost

SUMMARY

Submitted work "***Analysis, management and trade-off with risks connected with technical facilities***" deals with the risks associated with the technical facilities, particularly with the complex technical facilities. It demonstrates the ways of work with risks at risk identification, analysis, assessment, management and putting under control aimed to the safety of both, the technical facilities and their surroundings, and simultaneously respecting the current knowledge that the risks are locally and time-specific. The safety is understood as a property of the whole technical facility, which is determined by the quality of the file of anthropogenic measures and activities aimed at the safe technical facility, and even at its critical conditions. Therefore, at safety make up, the publication proposes to monitor both, the public assets and the technical facility assets, and to consider the diversity of their physical natures, vulnerabilities, and the constituent changes over time; which means continuously to solve emerging conflicts.

Since the risks are the cause of the technical facilities criticalities in the processes of the sitting, construction, operation and removal of technical facilities with regard to public assets, so the considered goal is ensuring the coexistence of technical facility with the surroundings, i.e. with public assets, which include human life, health and security, property, public welfare, the environment, other technologies, and infrastructures. With regard to the dynamic development of the world, it is necessary to monitor all priority risks and to implement their management and bringing under control with regard to improving or at least maintaining the technical facilities safety at an acceptable level. This means building the safety management systems of technical facilities that respect at work with risks the variability of the world in time and space, i.e. normal, abnormal, critical, and in some cases of technical facilities (e.g., highly dangerous nuclear facilities) also extreme conditions, and therefore, they have prepared the procedures for the control and management of critical situations.

Key words: disasters - sources of risks; risk; methods of working with risks; technical facilities; safety

SEZNAM ZKRATEK

Zkratka	Název
ALARA	As Low As Reasonable Achievable
ALARP	As Low As Reasonably Practicable
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
BOZP	Bezpečnost a ochrana zdraví při práci
CBA	Cost Benefit Analysis
ČR	Česká republika
ČSN	Česká technická norma
ČVUT	České vysoké učení technické
DSS	Decission Support Systém
ESRA	European Safety and Reliability Association
ESREL	European Safety and Reliability Conference
EU	European Union
IAEA (MAAE)	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Informační technologie
MSK	Stupnice velikosti zemětřesení podle dopadů na aktiva území.
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
NATO	North Atlantic Treaty Organization
NEA	Nuclear Energy Agency
OECD	Organisation for Economic Co-operation and Development
OSN	Organizace spojených národů
PC	Personal Computer
Sb.	Sbírka zákonů
SIL	Safety Integrity Level
SMS	Safety Management Systém
SoS	System of Systems
SR	Slovenská republika
TQM	Total Quality Management
US NRC	Dozor nad jadernou bezpečností USA

PŘEDMLUVA A PODĚKOVÁNÍ

Lidé od dob historických pro zlepšení kvality svého života vytváří technická díla. Jelikož je pravdou, že jisté skupiny lidí vytváří také technická díla, která mají opačný cíl, tj. pomocí nich chtějí získat území, majetek nebo jiné komodity, které patří jiné skupině lidí, uvádíme, že tato druhá skupina technických děl není v práci sledována. Základním cílem sledovaných technických děl je zajistit existenci, bezpečí a rozvoj lidské společnosti.

S rozvojem poznání a zkušeností lidí roste jak výkonnost, tak i složitost technických děl. V důsledku toho na jedné straně roste kvalita služeb a výrobků, které technická díla zajišťují, a na druhé straně vznikají nouzové situace ohrožující lidi, když technická díla selžou.

Předložená práce je zaměřena na rizika spojená s technickými díly. Vychází ze současného poznání a technická díla chápe jako vzájemně propojené otevřené systémy různé povahy, které jsou umístěny v prostředí, které má též systémovou povahu a je dynamicky proměnné. V důsledku vývoje probíhají procesy jak v technickém díle, tak i v jeho okolí. Výsledkem procesů, které probíhají v obou systémech i procesů napříč rozhraním, jsou jevy, které v řadě případů nejsou pro lidi přijatelné, protože způsobují ztráty, škody a újmy jak lidem, tak aktivům, na kterých jsou lidé závislí. Proto lidé pro zachování své existence musí předmětné jevy řídit a zvládat tak, aby zajistili koexistenci technických děl a okolí, která je pro ně důležitá.

Vzhledem k povaze sledovaných technických děl a jejich okolí, jde o složitou problematiku. Její řešení není jednoduché, a proto nástroje pro její řešení musí být založeny na vícekriteriálních přístupech. Z předmětného důvodu se práce zabývá nástroji, které nabízí inženýrské disciplíny pracující s riziky. Uvádí několik nástrojů, které byly otestované v praxi jako efektivní při řízení rizik zacíleném na bezpečná technická díla i jejich bezpečné okolí, a to po celou dobu životnosti technického díla.

V předložené práci využila autorka výsledky z celoživotního výzkumu a zkušenosti z praxe získané během řešení konkrétních úkolů doma i v zahraničí pro vládní i nevládní subjekty. Z důvodu zachování přiměřeného rozsahu publikace autorka přebírá z dřívějších publikací stejného zaměření jen důležité partie a na ostatní části se odvolává.

Kniha je sepsána v rámci projektu „Řízení rizik a bezpečnost složitých technologických objektů (RIRIZIBE)“ CZ.02.2.69/0.0/0.0/16 _018/0002649. Za projekt i podporu děkuje autorka EU, MŠMT a ČVUT v Praze.

Za pomoc při zpracování vybraných částí děkuje autorka recenzentům panu Prof. Ing. Josefu Říhovi, DrSc., panu Doc. Ing. Jiřímu Lukavskému, CSc., panu Doc. Ing. Václavu Beranovi, DrSc., panu Doc. RNDr. Miroslavu Ruskovi, PhD., kteří práci podrobně přečetli a dodali podnětné připomínky vedoucí k doplnění úplnosti a validitě textů. Rovněž děkuje panu RNDr. Janu Procházkovi, Ph.D. za podklady pro prezentaci výsledků metod, které se používají při práci s riziky v inženýrské praxi.

Předložená verze knihy byla na žádost rektorátu ČVUT a MŠMT v r. 2022 doplněna o údaje spojené s projektem RIRIZIBE a formátově upravena tak, aby bylo dodrženo původní stránkování.

1. ÚVOD DO PROBLEMATIKY

Předložená publikace je věnována technickým dílům, která jsou významným veřejným aktivem:
- zajišťují výrobky a služby, které zkvalitňují život lidí,
- přispívají k: zaměstnanosti; technické vzdělanosti; energetické soběstačnosti; a konkurenceschopnosti státu,
- vytváří zázemí odezvy na kritické situace (každá odezva potřebuje energii, technické prostředky, finance, dopravní prostředky, materiál) apod.,

a proto je třeba dbát o jejich bezpečnost. Zajistit jejich bezpečnost znamená cíleně a proaktivně pracovat s riziky [1-4]; základní a popisné informace o práci s riziky jsou v práci [2], a v předložené práci je předpokládaná jejich znalost.

Cílem lidského snažení je zajistit životy, zdraví, bezpečí a rozvoj lidí. Proto na základě současného poznání [1] lidé musí:
- pečovat o svět, ve kterém žijí, tj. o ***lidský systém*** a jeho základní veřejná aktiva (životy, zdraví a bezpečí lidí; majetek a veřejné blaho; životní prostředí; infrastruktury a technologie),
- své chování uzpůsobit tak, aby byla zachována koexistence základních systémů (environmentálního, sociálního a technologického), které jsou nezbytné pro existenci a život lidí, tj. pro bezpečný lidský systém, který má povahu označovanou jako systém systémů (SoS) [1], o které bude pojednáno podrobněji dále.

Antropogenní řízení lidského systému, zacílené na zajištění bezpečí a rozvoj dle [1] musí pečovat o:
- existenci schopnosti systému udržet rovnováhu,
- efektivnost systému při vyrovnávání se s nedostatkem zdrojů,
- rozmanitost možností systému při zvládání výzev z okolí,
- bezpečí systému, tj. schopnost systému ochránit se před jevy, které mají původ uvnitř i vně systému,
- adaptabilitu systému, tj. schopnost systému přizpůsobit se vnějším změnám,
- koexistenci systému s okolím, tj. schopnost systému měnit své chování tak, aby chování reagovalo na chování a orientaci dalších systémů a aby je neohrožovalo a ony neohrožovaly jeho.

Je pochopitelné, že výše uvedené požadavky jsou kladeny i na technická díla, která jsou základním veřejným aktivem lidského systému z důvodů uvedených výše. Jde především o technická díla, ve kterých jsou tlaková zařízení, zdroje vysoké energie a nebezpečné látky, protože uvedené skutečnosti mají vysoký ničivý potenciál, když se vymknou lidské kontrole.

Na základě současného poznání [1-4] lze bezpečné území a bezpečná technická díla zajistit jen tehdy, když lidé při řízení území, technického díla, státu aj. (dále je používáno obecné označení *entita*):
- zvažují všechna chráněná aktiva: u území jde o základní veřejná aktiva; u technických děl jde o veřejná i privátní aktiva, kterými jsou např.: hmotný majetek; technologie; know-how; prosperita; soulad organizace se státem v místě působení (tj. plnění úkolů, ke kterým byla organizace zřízena), konkurence-schopnost, good will apod. [3],
- používají současné vědecké poznání v kontextu teorie systému,

- řídí své činnosti tak, aby nezpůsobovali jevy, které by vedly k desintegraci až rozpadu lidského systému, tj. lidských komunit.

V souladu se současným poznáním se bezpečnost ve smyslu integrální lidské bezpečnosti [5] neorientuje jen na jedno chráněné aktivum, a to na životy a zdraví lidí či jen životní prostředí nebo jen stát, ale na celý komplex chráněných aktiv, protože hlavní prioritu, kterou jsou životy a zdraví lidí lze ochránit jen tehdy, když životní prostředí a klima lidské společnosti jsou kvalitní a když je k dispozici potenciál k ochraně, tj. majetek, základní technologie a základní infrastruktura. Takto chápaná bezpečnost a udržitelný rozvoj systému, ve kterém žije lidská společnost, se na základě současného poznání vztahuje na lidský systém, tj. životní prostor lidí, který zahrnuje vše, co je nutné pro kvalitní život a rozvoj lidí i celé lidské společnosti.

Z právě uvedeného důvodu se strategické řízení každého státu, území či objektu (tj. i technického díla) zaměřuje na bezpečnost a dlouhodobou udržitelnost [1]. V předmětném smyslu bezpečnost představuje soubor antropogenních opatření a činností, kterými se lidé brání proti škodlivým jevům všeho druhu. V dané souvislosti je v současné době dominantně používán i pojem riziko. V technických disciplínách, na které se zaměřuje předložená práce, ***riziko znamená pravděpodobnou velikost škod, ztrát a újmy na chráněných aktivech, kterou způsobí pohroma o normativně určené velikosti (nazývanou ohrožení), která je normovaná na jednotku plochy a jednotku času***, tj. jde o míru nepřijatelných dopadů způsobených pohromou o velikosti rovné hodnotě ohrožení [2,6].

Riziko je spojeno se složitými podmínkami a mnoha působícími faktory v našem světě:
- nejistá přírodní ohrožení,
- nejistoty, které obsahují výsledky vědy i používané technologie, a jejich působení na zdraví a kvalitu života lidí,
- zranitelnost lidí a nedostatek konzistentního vysvětlení životních strastí a jejich významu,
- lidská hra se strachem, šancemi a možnostmi.

Z uvedených důvodů je riziko inherentní součástí světa, tj. lidského systému, a proto se na něho zaměřuje legislativa, normy a standardy. Např. novelizace mezinárodní normy ISO 9000, vydaná v ČR v r. 2016, vyžaduje analýzu rizik v souvislosti se zajišťováním kvality procesů a produktů ve firmách, které usilují o certifikaci či re certifikaci systému řízení kvality. Předmětná norma odkazuje na další normy: ČSN ISO 31000 Management rizik – principy a směrnice [7]; ČSN EN 31010 Management rizik - Techniky posuzování rizik; ČSN ISO 10006 Směrnice jakosti v managementu projektu (Proces řízení rizik projektu); ČSN EN 61025 Analýza stromu poruchových stavů (FTA); a ČSN EN 60812 Postup analýzy způsobů a důsledků poruch (FMEA) atd.

Aplikace výše uvedených norem v praxi vyžaduje věnovat dostatečnou pozornost pojmům a jejich provázání s logikou vzniku ztrát a škod danou kauzálním vztahem příčina – důsledek; tj. vyžadovat důsledně stejné pojetí označující procesy vzniku škod a ztrát. Norma ISO/IEC 31010 definuje riziko a další spojené pojmy příliš obecně a nezdůrazňuje roli výběru a validace dat a metod, která předurčuje kvalitu určené hodnoty rizika, a tím i kvalitu lidských protiopatření.

Předložená kniha předkládá důkladné vysvětlení problémů, přičemž vychází z dokumentů pro zajištění bezpečí a strategický rozvoj technických děl, které byly vypracované OSN, OECD, NEA, IAEA, EU a dalšími odbornými organizacemi, jako jsou ASME, ASCE, IEEE aj., které definují pro technická díla riziko přesněji, a to tak, jak je

výše uvedeno; v dalším textu budou zmíněné dokumenty citovány na příslušných místech.

Jelikož je skutečností, že mnoho zdrojů rizik nelze odstranit, tak pro bezpečí a rozvoj lidí je třeba, aby riziko bylo přijatelné. Přijatelná úroveň rizika je subjektivní [1,2]. U známých a častých pohrom je lidmi vnímaná úroveň rizika blízká skutečné míře rizika. U málo častých a málo známých pohrom je lidmi vnímaná úroveň rizika jako neskutečná a vzdálená. Vnímání rizika ovlivňují i jiné faktory – např. u činností, které děláme dobrovolně (horolezectví, skoky na lyžích apod.) obvykle předpokládáme zanedbatelnou úroveň rizika.

Přijatelnost rizika je výsledkem porovnávání několika typů přijatelnosti – technická přijatelnost (spolehlivost a složitost technologií, strojů a zařízení), ekonomická přijatelnost (náklady) a socio-politická přijatelnost (vnímání rizik) [2]. Obecně lze tvrdit, že přijatelné riziko se stanovuje na sociálním a znalostním základě a přitom se zvažují nejrůznější sociální, ekonomické a politické faktory. To mimo jiné znamená, že úroveň přijatelného rizika pro bohatá společenství lidí je vyšší než pro chudá, protože redukce rizika něco stojí. Proto také platí, že přijatelná úroveň rizika neznamená bezpečnou úroveň rizika, tj. že pravděpodobná velikost možných ztrát, škod a újmy na chráněných aktivech je malá až zanedbatelná [2].

Protože doposud neexistuje obecná shoda na formulaci problémů udržitelnosti veřejného blaha (blahobytu) lidské společnosti v kontextu se systémovými službami, je každé dosavadní řešení spojené se zvládnutím rizik ve prospěch bezpečnosti dočasné. Neustále se balancuje mezi konkurujícími si zájmy a společenskými cíli (anebo dokonce jen zbožnými přáními politiků). Je obtížné řešit problémy rozhodování jednoznačně vzhledem k měnícímu se charakteru rozhodovacího procesu [1]. V rozhodování se stále řeší dále uvedená dilemata:

- vztah mezi riziky a přínosy (často větší přínos pro lidi znamená zvýšené riziko pro ekosystémy),
- časový konflikt mezi současnými a budoucími potřebami,
- sociální konflikt (vztah potřeb jedince a celku).

Je obtížné řešit inverzní problémy pro složitost systémů. Skutečnost je taková, že když se stanoví a utřídí jisté příznaky spojené s riziky, vynoří se příznaky nové. Z toho vyplývá, že praktický přístup k řízení rizik zacílený na udržitelnost musí být iterační, interaktivní a adaptivní [1,2].

Cílem komplexního řízení entit, které se s ohledem na výše uvedené poznatky soustřeďuje na řízení rizik procesů [4], je za každé situace zajistit ochranu životů, zdraví a bezpečí lidí, majetku a veřejného blaha, životního prostředí, infrastruktur a technologií (tj. základních veřejných aktiv), které jsou nezbytné pro přežití lidí. Proto pro případ nouze je nutné na úrovní státu, území i technického díla vytvářet schopnost zajistit:

- mobilizaci a koordinaci využití národních zdrojů (energie, pracovní síly, výrobní schopnost, potraviny, zemědělství, suroviny, telekomunikace aj.),
- koordinaci činností takových, jako je systém vyrozumění a varování,
- systém záchrany a zdravotnické služby, které snižují dopady pohrom,
- kontinuitu činnosti státní správy a dodržování zákonů.

Typy plánování tvořící základní metodické nástroje jednotlivých vzájemně provázaných typů řízení musí vytvářet základnu, ve které jsou výše uvedené cíle zakotvené [1,2].

Pro cíle lidské společnosti, tj. především pro její udržitelný rozvoj se musí vzájemně kombinovat opatření a činnosti na snižování zranitelnosti a na zvyšování pružné odolnosti (resilience) a schopnosti adaptace, které respektují všechna základní chráněná aktiva v jednotlivostech i celku. Současným nástrojem založeným na znalostech a zkušenostech je na všech úrovních řízení implementovat proaktivní systém řízení bezpečnosti, ve kterém se upraví práce s riziky do takové formy, která respektuje všechna chráněná aktiva a bere v úvahu existující a prokázané vnitřní závislosti. S ohledem na současné poznání je třeba provádět a sledovat výzkum vnitřních závislostí, které zprostředkovávají sekundární a další dopady pohrom na životy, zdraví a bezpečí lidí a další veřejná aktiva včetně technických děl [1,3].

Pro zajištění bezpečí a rozvoj společenství lidí musí správy celků, na které je organizačně roztříděn lidský systém (tj. správci technických děl i správci území, tj. obce, kraje, státy a společenství států) dobře pracovat s riziky. Pro práci s riziky v každé entitě je třeba vymezit:

- koncept entity a jejich částí v systémovém pojetí,
- základní / prioritní či kritická aktiva entit,
- pojmy důležité pro chápání a řízení bezpečnosti entit,
- zdroje rizik, jejich dopady na chráněná aktiva entity,
- metody pro identifikaci, analýzu, hodnocení a posuzování rizik,
- způsoby řízení rizik,
- způsoby inženýrského vypořádání rizik,
- způsoby práce s riziky v čase.

Je skutečností, že existuje velké množství rizik, protože jejich zdrojů je velké množství [1,2]. Stále roste počet propojení v lidském systému i v technických dílech, která jsou významnými příčinami rizik, i když někdy jen za jistých podmínek [4]. Rizika také stále přibývají v důsledku rostoucí zranitelnosti veřejných aktiv, a lidská společnost nemá zdroje, síly a prostředky, aby tomu zabránila, a tak musí cíleně řídit rizika. Aby předmětné řízení bylo úspěšné, tak se musí zaměřit na prioritní rizika a jejich aspekty a na správné určení cílů řízení [2,3]. S ohledem na povahu rizik a schopnosti člověka, člověk de facto s riziky hraje hru „kdo z koho"; v odborné literatuře se používá pojem „vyjednávání s riziky“. Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá v rozdělení vypořádání rizik do kategorií, ve kterých se příslušná část rizika zajistí tak [2], že:

- preventivní opatření sníží nebo odvrátí realizace rizika,
- účelová preventivní (zmírňující) opatření aplikovaná při odezvě a připravené nástroje (varovné systémy a jiná opatření nouzového a krizového řízení) zmírní dopady rizika, tj. sníží nebo odvrátí se nepřijatelné dopady při realizaci rizika,
- pojištění zajistí prostředky na krytí možných ztrát a škod, které vzniknou při realizaci rizika,
- připravené rezervy na odezvu a obnovu a zálohy pro zajištění přežití lidí a kontinuity provozu území, objektu či organizace zajistí schopnost zvládnout odezvy na pohromy,
- příprava realistického plánu odezvy na nepředvídané situace (Contingency Plan) způsobené realizací rizik neřiditelných nebo příliš nákladných, anebo málo častých zajistí potenciál na zvládnutí extrémních situací.

K tomu se rovněž připojuje rozdělení zvládání rizik mezi zúčastněné [1-3]. Rozdělení úkolů ve správním řízení se provádí tak, že se vychází z toho, že za zvládání rizik odpovídají všichni zúčastnění a že zvládání konkrétního rizika se přiděluje subjektu, který je na situaci nejlépe připraven, přičemž ostatní subjekty na přípravu jeho

schopnosti a provedení činností přispívají. Na základě poznání [1-4] předmětné rozdělení je možné jen v organizaci, ve které je kvalifikované projektové a procesní řízení, tj. činnosti a opatření se aplikují na základě znalostí, a to věcných i z oblasti řízení (tj. činnosti jsou vzájemně provázané, nejsou chyby v komunikaci, každý zúčastněný ví, co má dělat a jak to má dělat).

Předložená kniha se opírá o současné poznání. Navazuje na publikace [1-4,8-24], které byly zpracovány na základě kritického vyhodnocení poznatků v dostupných stovkách odborných prací a zkušeností autorky z praxe. Ve zmíněných publikacích jsou sledovány a diskutovány jednotlivé aspekty rizik. Předmětné poznatky jsou dále doplněny znalostmi získanými kritickou analýzou odborných prací, které se zabývají riziky v předních odborných časopisech a knihách. Jde především o práce, které jsou cíleně shromažďované evropskou agenturou ESRA (European Safety and Reliability Association), prezentované na světových konferencích ESREL a následně publikované ve formě tištěných a elektronických knih [25-34], a také na specifických odborných konferencích, z nichž některé byly pořádány nebo spolupořádány i ČVUT a jejich výsledky jsou v recenzovaných sbornících [35-39].

Cílem knihy není opakovat základy, které jsou v pracích [1-4,8-24], ani popisovat akademické diskuse uvedené v odborných článcích mnoha světových časopisů, ale ukázat postupy, kterými lze zvládat rizika technických děl, a to objektových i síťových. Jde o vytváření bezpečných technických děl, bezpečného území, ve kterém jsou technická díla umístěna, a tím i bezpečné lidské společnosti tak, jak to stanovují současné koncepty OSN [5] i EU [40]. Proto v předložené publikaci jsou sledovány pouze osvědčené postupy prací s riziky, které jsou zacílené na bezpečnost technických děl a jsou detailně popsány v pracích [1-4,11,13,17,24]. V práci jsou pochopitelně využity i další recentní poznatky, které jsou v dalších odborných pracích, které budou dále na příslušných místech citovány.

Kromě úvodu a závěru, monografie obsahuje 5 kapitol, které obsahují základní teoretické i praktické poznatky o důležitých postupech práce s riziky spojenými s technickými díly i jejich okolím. Kapitola 2 obsahuje popis používaných struktur a logiky v zájmové oblasti. Je zmíněno systémové pojetí světa a technických děl a za ním následují provázané soubory pojmů, kterými lze popsat dynamicky se vyvíjející svět i technická díla i nástroje pro antropogenní řízení. Kapitola 3 uvádí souhrn poznatků o příčinách rizik spojených s technickými díly a o zajištění bezpečnosti technických děl. Pozornost je věnována rozdílu mezi náhodnou a znalostní nejistotou, který hraje velkou roli při práci s riziky. Kapitola 4 shrnuje recentní poznatky spojené s metodami používanými v inženýrských disciplínách, které pracují s riziky technických děl. Předmětná kapitola je zásadní, protože se zabývá nástroji práce s riziky a věrohodností výsledků získaných jejich aplikací. Kapitola 5 se zabývá způsoby práce s riziky, které ovlivňují koexistencí technického díla a jeho okolí. Kapitola 6 ukazuje alternativy práce s riziky spojenými s technickými díly, jejichž cílem je bezpečné technické dílo i jeho bezpečné okolí po celou dobu životnosti technického díla, které jsou používány v praxi. Upozorňuje na důsledky zanedbání v případech, když jsou použity příliš jednoduché postupy práce s riziky. Ukazuje také, že pouhé dodržení norem nezajistí zvládnutí všech rizik, tj. ani bezpečnost technických děl. Proto je třeba u důležitých technických děl k normám připojit práci s riziky.

Je si třeba uvědomit, že práce s riziky ve prospěch bezpečnosti vyžaduje porozumění problému, jasná pravidla a určené odpovědnosti.

2. POUŽÍVANÉ STRUKTURY, LOGIKY A POJMY

Nauka o rizicích a bezpečnosti území i technických děl jako věda je soustavná, kritická a metodická snaha o pravdivé a obecné poznání rizik a bezpečnosti příslušné entity, tj. v našem případě technického díla a jeho okolí. Jejím cílem je nepřetržitý společenský proces soustavného racionálního poznávání entity s cílem zajistit její žádoucí stav a rozvoj žádoucím směrem. Zahrnuje obecnou teorii rizik a bezpečnosti (v integrálním / komplexním smyslu), teorii *„umění“* řízení rizik a bezpečnosti (tj. způsoby a formy aplikace opatření na jednotlivých stupních), teorii výstavby a provozu systému řízení bezpečnosti (bezpečnostního systému), tj. výstavby, provozu a chování dotčených orgánů a zúčastněných složek pro zajištění bezpečnosti předmětné entity. Jedná se o přípravu, funkčnost a schopnost systému řízení bezpečnosti entity (tj. jejich prvků, vazeb a toků) zajistit bezpečnost a rozvoj entity za podmínek normálních, abnormálních i kritických. Příprava entity na zvládnutí kritických podmínek je nutná z důvodu dynamiky vývoje světa i entity.

Předmětem kapitoly je vymezení odborného zázemí, tj. předmětu zkoumání; zvažovaných souvislostí; a pojmů. Další aspekty jako problematika dat, metod a postupů pro řešení problémů; způsobu rozhodování a struktury řízení a řešení problémů jsou předmětem kapitol dalších. Z důvodu zvoleného cíle je dále zvažována celá šíře problému a je zvolen transparentní postup zvažující fyzikální podstatu sledovaných entit (nehomogenity, anizotropie, anomálie, nelinearity, přechodové jevy, náhlé skoky apod.) [11,17]; proto jsou uvedeny jen nezbytné matematické vzorce a u software často používaných pro potřeby plánování jsou uváděny zjednodušující předpoklady, na kterých jsou založeny. Použité pojetí odpovídá potřebám současného managementu každé entity, jehož cílem je zvládnout problémy a zajistit rozvoj entity, což není možné bez pochopení systémové povahy entity v detailech a jejího chování v souvislostech.

Řízení bezpečnosti v území i v technickém díle [3,4] se prezentuje jako antropogenní řízení, které se opírá o:

- vyhodnocení vlastností a ocenění potenciálu živelních a jiných pohrom působit újmy, škody a ztráty na chráněných aktivech v území i technickém díle,
- identifikaci, analýzu, hodnocení řízení a vypořádání rizik, a to jak v území, tak v technických dílech s tím, že se zvažuje zranitelnost území, technických děl a lidské společnosti,
- kvalifikované stanovení opatření krátkodobých, střednědobých i dlouhodobých, které vedou k růstu bezpečnosti a k udržitelnému rozvoji technického díla i území,
- monitoring bezpečnosti technického díla i území,
- přípravu případných nápravných opatření, kterými se zabezpečí růst bezpečnosti v území i v technických dílech.

Pozornost je soustředěna především na složitá technická díla s tím, že na základě výše uvedených úvah je požadována koexistence technických děl s okolním územím. Území i technická díla tvoří soubory otevřených a vzájemně propojených systémů, které jsou při řešení problémů nahrazeny modely, které znázorňují podstatné vlastnosti požadované řešitelem problému. Podle charakteru parametrů a rozhodovacích proměnných, modely dělíme takto:

1. Deterministické modely jsou modely, v nichž jsou pro všechny parametry na vstupu pevně zadané hodnoty, a v nichž vystupují pouze deterministické veličiny a

vztahy.

2. Stochastické modely jsou modely, v nichž se vyskytuje alespoň jeden parametr, jenž je náhodnou veličinou. Důsledkem je pak výskyt alespoň jedné rozhodovací proměnné v modelu, jež je náhodnou veličinou. Rozdělení pravděpodobnosti náhodných veličin v modelu se pokládá za známé (v praxi se tato rozdělení buďto odvodí z logicko-teoretických úvah, nebo se určí pomocí metod matematické statistiky, anebo se odhadnou pomocí expertních metod).
3. Heuristické modely jsou modely, v nichž se vyskytuje alespoň jeden parametr, jenž je náhodnou veličinou, jejíž rozdělení na rozdíl od stochastických modelů není známé, a nelze je určit ani metodami matematické statistiky (obvykle v důsledku jejich malé četnosti, anebo příliš velkého rozptylu disponibilních dat), ani logicko-teoretickými úvahami; obvykle mluvíme o náhodných a znalostních nejistotách, anebo ve smyslu pojetí známého fyzika Heisenberga o nejistotách a neurčitostech [2,3]. U každého takového parametru známe pouze dolní a horní mez, jichž může nabývat.

Používané pojmy pro práci s riziky jsou sestaveny na základě teorie procesních modelů tak, jak je prosazováno OECD a IAEA a jak je to běžné v dnešních odborných disciplínách, např. v pracích [25-33,41-55].

2.1. Systém a pojetí technických děl

Systém je slovo řeckého původu, které znamená uspořádání rozmanitostí určité dané entity. V daném pojetí je entita množina prvků, které jsou ve vzájemných vztazích a které tvoří určitý celek. Původně ve starověké filosofii znamenal seskupení, sjednocení, celek. Představa o struktuře a hierarchii systému vznikla již v antice a uplatnila se zejména v tehdejších poznatcích o stavbě živého organismu. Novodobě pojem začal široce používat v r. 1948 zakladatel kybernetiky Norbert Wiener. Postupně se pojem ujal v odborných oblastech i v občanském životě.

Systém je neprázdná účelově definovaná množina prvků, vazeb a toků mezi prvky, která vykazuje jako celek určité vlastnosti a chování v čase a prostoru. Vůči okolí vystupuje systém jako celek. Charakteristické znaky systému zůstávají po určitou dobu a v určitém prostoru konstantní, a proto je lze pozorovat a popsat. Vazby jsou přímé, zprostředkované a zpětné. Uzavřené systémy, které by byly oddělené od okolí, v realitě neexistují; cíleně lze pouze vytvořit systémy „částečně“ izolované od okolí. Vztahy systému s okolím jsou rozhodující pro celistvost systému. V současném pojetí je každý systém chápán jako prvek struktury, tj. systému vyššího řádu a každý jeho prvek jako systém nižšího řádu.

Invariantní (neměnné) aspekty systému určují strukturu systému. Hierarchické uspořádání dílčích systémů a mnoho stupňovitost dílčích systémů určují strukturu, morfologii (tvar) a chování systému. Určitá funkčnost dílčích systémů je podmínkou pro určité chování systému. Celková funkčnost systému je výsledkem vzájemného působení všech dílčích systémů, a to na všech úrovních hierarchie. Platí tudíž následující shrnutí:

- každá realita je tvořena hierarchicky uspořádanými segmenty (reálnými systémy) různé úrovně,

- každá vyšší úroveň se vyznačuje novými kvalitami, a proto potřebná informace o systému musí zahrnovat vždy více informací než agregaci informací o prvcích a subsystémech,
- systémy směrem „dolů“ se v této hierarchii jeví jako autonomní celky, ale směrem „nahoru“ jako závislé části,
- každý systém je tedy subsystémem nejblíže vyššího systému v hierarchii, ale jako subsystém je současně samostatným systémem. Tímto způsobem jsou znázorněny prostorová a funkční propojení dílčích struktur a široké spektrum vazeb, procesů a mechanismů v něm možných, např. složky v systému životního prostředí; skupiny v lidské společnosti; technologie a infrastruktury v technologickém celku apod.

Současná úroveň poznání shrnutá v práci [2] ukazuje, že:

1. Žádný systém není dosud poznán dostatečně dobře. Např. je známo, že k popisu atmosféry máme sice dnes již k dispozici více než 500 000 rovnic, a přesto předpovědi počasí nejsou dosud stoprocentně úspěšné.
2. V našem poznání je nejen mnoho nejistého, což lze odstranit aparátem matematické statistiky, máme-li k dispozici vhodná data, ale i mnoho neurčitého, což lze posoudit jen pomocí expertních odhadů, máme-li k dispozici znalostní databáze a zkušené experty z oblastí spojených se sledovaným problémem.
3. Žádný systém není v čase a v prostoru neměnný a každý je lidskou činností zranitelný. Velikost (míra) zranitelnosti a její příčiny jsou pro nás velkou neznámou. Proto kvalita odpovědnosti lidské společnosti se projevuje tím, jak konkrétní lidská společnost přistupuje k různým rizikům, např. tím, že instaluje nebo neinstaluje systémy „hlídající“ nebezpečné činnosti nebo tím, jak přistupuje k podmínkám daným podstatou systému samotného. Ve zmíněných souvislostech lidská společnost často dělá chybu a spoléhá na adaptaci lidského systému a neuvědomuje si, že proces adaptace je proces velmi pomalý, což znamená, že spolehnutí jen na tento proces nezaručuje bezpečnost, a proto nepředstavuje odpovědný přístup.
4. Způsobem, kterým lze zajistit existenci a rozvoj systému, je aplikovat nástroj řízení bezpečnosti, který má v sobě inherentně zahrnut prvek předběžné opatrnosti.

Chápání objektu jako systém je rovno zavedení systému na objekt, což znamená definovat prvky, vazby a toky mezi prvky, vstupy a výstupy. Abychom považovali reálný objekt za systém, je rozhodující náš přístup k tomuto objektu, způsob jeho pojetí, způsob práce s ním, nikoli jeho věcná povaha.

Každý systém má strukturu (skladba, vnitřní uspořádání systému), která se projevuje jako jednota prvků, vazeb a toků, a mechanismus řízení, který určuje jeho chování. Velkou roli hrají zpětné vazby, tj. zpětná působení řízeného procesu na toho, kdo proces řídí. Role je kladná, když vede k synergii a záporná, když oslabuje projevy systému. Chování systému je způsob reakce systému na podněty vnitřní i vnější. Příčiny reakce často označujeme vstupy a výsledky reakce jako výstupy. ***Stav systému*** je množina definovaných podmínek nebo veličin, které lze v daném časovém okamžiku a v daném místě rozpoznat. ***Kritičnost*** je krajní / mezní stav nebo vlastnost systému. Adaptabilita systému je schopnost systému reagovat na své okolí způsobem, který je v určitém smyslu výhodný k tomu, aby systém pokračoval ve své činnosti.

Systém se dynamicky vyvíjí, když se jeho stav v čase mění [2]. Trajektorie dynamického systému je posloupnost stavů systémů v čase; může to být funkce. V dynamických systémech se řeší:
- úlohy o stabilitě systému vůči vlivům zvenku, a to analyticky či heuristicky,
- prognostické úlohy pomocí simulace deterministické, stochastické i heuristické,
- optimalizační úlohy pomocí analytických, numerických metod, simulací i vícekriteriálních nástrojů,
- ostatní úlohy jako chování systémů systémů.

Obecné vlastnosti systému dle [2] jsou:
- koherentnost znamená, že změna v jednom prvku systému vyvolá změnu ve všech prvcích systému,
- samostatnost znamená, že změna v jednom prvku probíhá autonomně, tj. nevyvolá změnu v ostatních prvcích,
- kompatibilita je soubor podmínek, za kterých dva či více systémů může spolupracovat, tj. podílet se na společné činnosti,
- centralizace označuje případ, ve kterém jeden prvek systému má dominantní roli v činnosti systému,
- ekvifinalita znamená schopnost systému dosáhnout daného cíle z různých výchozích stavů systému,
- operabilita je soubor podmínek, za kterých systém je v bezpečný, spolehlivý a funkční.

Vlastnosti systémů (struktur entit) jsou celistvost, rozložitelnost, existence vazeb, existence toků, interakce, dynamičnost. Z hlediska celistvosti se v systému zkoumá a řeší, jak daná funkce ovlivňuje ostatní funkce a které funkce se netýkají celku, ale jen určitého prvku, vazby či toku. Dva systémy jsou podobné, když jsou izomorfní (tj. přiřazení prvků je jednoznačné a oboustranné), anebo homomorfní (přiřazení prvků je jednoznačné a není obousměrné). Podobnost usnadňuje studium rozsáhlých systémů [2].

Cílem poznávání systémů je odhalit podstatu systémů a její proměnnost v čase. Proto sestrojujeme varianty chování systémů a hledáme optimální variantu, a to podle povahy buď stochasticky, nebo heuristicky [2].

Základní postup pro výzkum problému systému spočívá v:
- analýze situace,
- formulaci otázek a cílů na základě věcné znalosti problematiky,
- definování problematiky očekávaného řešení a její zobrazení, tj. modelu, který představuje zjednodušení reality,
- provedení zpracování dat k dané problematice na modelu, které je založené na analýze dat a syntéze poznatků k problematice,
- interpretaci výsledků a v komunikaci se zúčastněnými,
- návrhu řešení, postupu řešení a monitoringu včetně nápravných opatření aplikovaných v případě, jestliže řešení neodpovídá stanoveným cílům.

Systémy dělíme na:
- měkké, které se vyznačují tím, že jsou obtížně strukturovatelné, těžko rozpoznatelné a práce s nimi je značně subjektivní,
- tvrdé systémy, které se vyznačují jasnou strukturou a jasnými pracovními postupy.

Tvrdé systémy jsou uměle vytvořené. Jejich vlastnosti se definují exaktně. Setkáváme se s nimi zejména v exaktních vědách, kde jsou založeny na matematických me-

todách. Mají rozpoznatelnou a explicitně vyjádřenou strukturu. Při použití formálních prostředků modelování jsou výsledky jednoznačné. Vlastnosti reálného objektu vystihují málo.

Měkké systémy se vyznačují tím, že jsou adaptibilní ke změnám okolí a mají určité stálé rysy. Prvky, vazby a toky nebývají neměnné, nedefinují se abstraktně a zpravidla se mění se změnou vlastností okolí. Jsou obtížně strukturovatelné, tj. není možné jasné vymezení struktury. Měkkost může také vyplývat z neurčitosti či neschopnosti analytika vyznat se v reálných systémech (proto i tvrdé systémy se mohou jevit jako měkké). Měkké systémy jsou typické pro sociální a ekonomické systémy. Při práci s nimi je typická subjektivita a mnohdy i neúplnost jejich rozpoznání (formalizované prostředky omezené použití).

Kritérium tvrdosti nebo měkkosti není fyzická podstata systému, ale míra s jakou může být systém objektivně rozpoznán a popsán tvrdými, tj. formalizovanými prostředky. Většina reálných systémů spojených s technickými díly se řadí někam mezi oba uvedené typy. Metodologie tvrdých systémů se vyznačuje přenositelností, objektivitou, algoritmizací a prokazatelností vlastností. Metodologie měkkých systémů se vyznačuje nesnadnou přenositelností, metodickou nehomogenitou, nesnadnou algoritmizací a obtížnou formulací vlastností – je třeba často používat verbální stupnice.

Další důležitá dělení systémů jsou:
- systémy uzavřené a systémy otevřené – podle toho, zda nastává interakce s okolím,
- systémy deterministické a systémy stochastické – podle toho, zda systém vykazuje jednoznačné nebo náhodné (statisticky popsatelné) chování,
- systémy statické a systémy dynamické – podle toho, zda se vyvíjejí v čase,
- systémy spojité a systémy diskrétní – podle toho, zda se hodnoty mění spojitě nebo skokově.

Systém systémů (*dále jen SoS*, což je odvozeno od anglického názvu „System of Systems“ nebo v americké angličtině „Systems Systém“) je systém, který se skládá z několika systémů různé povahy a různého umístění, které jsou vzájemně provázané k tomu, aby zajistily jisté operace a činnosti. Jedná se o specifickou hierarchii rozdělení systému na podsystémy [2]. Příkladem SoS jsou lidské tělo, životní prostředí, technická díla, kritická infrastruktura, lidská společnost aj. Musíme si uvědomit, že při sledování chování SoS pro potřeby řešení jedněch úkolů se musíme zabývat velmi podrobným dělením systémů v několika úrovních a při jiných postačí jen dělení v nejvyšší úrovni (úrovně regionální, obecní, místní atd.). Vzájemná provázanost systémů pochopitelně působí závislost. V daném případě pochopitelně neplatí, že bezpečnost SoS je agregací bezpečnosti dílčích systémů, protože se musí respektovat i průřezová rizika způsobená vazbami a toky napříč SoS. To také znamená, že integrovaná bezpečnost založená na řízení integrovaného rizika není zcela na místě, a proto musí být postupně nahrazována integrální bezpečností, při které se spoléhá i na řízení průřezových rizik [3,4].

Je si třeba uvědomit, že komplexní chování, funkčnost a vývoj systému systémů závisí jak na množství a vlastnostech dílčích systémů, tak na rozmanitostech jejich propojení, tj. jejich vztahů a toků mezi nimi a také napříč nich. Vztahy a toky jdoucí napříč dílčích systémů jsou původci vnitřních závislostí (tzv. interdependences). V lidském systému a ve všech jeho podsystémech, tj. v přírodě, technice i lidské společnosti je řada systémů systémů, jejichž chování je podřízeno dosažení určitého cíle a některé z nich jsou i samoorganizující a schopné během funkčnosti změnit svoji

strukturu a způsob řízení. Mnohé systémy systémů mají na jednotlivých úrovních charakteristické cíle, které nejsou shodné, a proto řízení musí být zacíleno tak, aby se předešlo konfliktům [2].

Typickými vlastnostmi systému systémů jsou např. operační nezávislost a emergentní chování jednotlivých dílčích systémů, kompatibilita a interoperabilita (styková provozuschopnost). Operační nezávislost dílčích systémů spočívá v tom, že při rozložení systému na dílčí systémy, jsou tyto dílčí systémy schopny fungovat nezávisle. Emergentní chování systému systémů znamená, že systém vykonává funkce a uskutečňuje záměry, které nejsou uloženy žádnému z dílčích systémů.

Interoperabilita je schopnost celku, tj. souboru vzájemně propojených rozmanitých systémů a zařízení, fungovat společně efektivním způsobem podle konceptu projektu, který je zaměřen na určitý cíl. Interoperabilita je technická a organizační. Technická interoperabilita se vztahuje k fyzickým a komunikačním spojením mezi zařízeními a systémy a interoperabilita organizační se zabývá vztahy mezi organizacemi a jejich částmi včetně podnikatelských a právních vztahů. Na tomto místě je vhodné konstatovat, že problémům organizační interoperability se začala věnovat v analýze rizik pozornost až po velkých selháních elektroenergetických infrastruktur, které postihly vyspělé státy v posledních letech. Při řešení problémů interoperability si je třeba také uvědomit, že její stinnou stránkou je skutečnost, že zvýšením velikosti a počtu propojení se zvyšuje systémová složitost, takže celkový systém může selhávat složitým a nepředvídatelným způsobem [2,3].

Dílčí systémy i celý systém systémů jsou složité dynamické systémy s určitou úrovní přizpůsobivosti. Pro zajištění bezpečnosti zahrnující funkčnost, provozní spolehlivost a stabilitu se musí znát prahová hodnota – kritičnost, která určuje stav, při kterém systém nezajišťuje očekávané funkce v požadovaném čase, místě a v požadované kvalitě.

Pro odhalení slabin systému systémů se používají metody multikriteriální analýzy: matice kritičnosti (porovnává zranitelnost a důležitost); měkké metody (Soft System Methodology), Strategic Choice Approach, scénáře; či kauzální metody (Causal Loops Analysis) nebo analýza závislostí [2]; další údaje o metodách jsou v kapitole 4.

2.2. Model technických děl a jejich okolí

Technické dílo je dílo vytvořené lidskou činností, které zajišťuje výrobky nebo služby důležité pro život lidi. Architektura technických děl je objektová nebo síťová. Každý typ technického díla má svá specifika; např. významný rozdíl existuje mezi ovládáním stabilních a pohybujících se technických děl. Z důvodu rozsahu publikace, další podrobnosti jsou např. v pracích [3,4,11,17,24] a v pracích, které jsou v nich citovány. Mezi velká technická díla patří: elektrárny, průmyslové objekty, přehrady, letiště, nádraží, sklady, nemocnice, velká obchodní centra, velká kulturní či sportovní centra atd. Náleží do správy různých sektorů a jejich cílem je zajistit kvalitní život lidí. Zahrnují fyzické, kybernetické, organizační a sociální systémy, tj. jednotlivá zařízení, stroje, komponenty, systémy či celé výrobní či obslužné celky.

Velká technická díla jsou víc než jen množina technických částí zařízení a součástek; jde o soubor vzájemně propojených otevřených systémů (tzv. systém systémů –

SoS), který se nachází v dynamicky proměnném světě. Jejich požadované charakteristické rysy jsou:
- velký rozměr,
- velký výkon,
- použití více technologií,
- složení se z několika autonomních částí, které mohou pracovat samostatně a být vyvíjeny nezávisle,
- vysoká bezpečnost, tj. funkčnost a spolehlivost i nízké ohrožení chráněných aktiv vlastních i veřejných, a to za podmínek normálních, abnormálních i kritických.

Proto jde o systémy značně složité. V dané souvislosti rozlišujeme ***zabezpečený systém*** (systém ochráněný před všemi riziky) a ***bezpečný systém*** (systém, který je zabezpečený a při svých kritických podmínkách neohrožuje sebe, ani své okolí) [3].

Na základě současného poznání, shrnutého v pracích [3,4], jsou technická díla složité socio-kyber-technologické systémy, které zahrnují:
- budovy,
- zařízení budov,
- infrastruktury,
- obslužný personál,
- systém řízení technických děl.

Jejich vlastní aktiva tudíž tvoří stavby, jejich prvky, zařízení, obsluha a další personál, konstrukční a kybernetická propojení způsobená vazbami a toky mezi vyjmenovanými položkami, znalosti (know-how), provozní postupy, výrobky, rezervy (materiálové, finanční, lidské a další), smlouvy o spolupráci s veřejnou správou, bezpečnostními složkami, výzkumnými institucemi, veřejností atd. To znamená, že představují otevřený systém skládající se z řady vzájemně se prolínajících otevřených systémů [3].

Žádné technické dílo není v prostoru a čase osamocené. Je umístěno v území a v lidské společnosti, které ho ovlivňují; společně vytváří lidský systém**,** ve kterém se vyskytují pohromy, tj. škodlivé jevy všeho druhu, jejichž velikost se mění v čase a prostoru. Předmětné jevy ohrožují nejen technická díla samotná, ale mohou způsobit domino efekty, tj. poškození technického díla značně zesílí škody na lidech a dalších veřejných aktivech lidského systému, který je modelem našeho světa v okolí [3].

2.3. Soubor pojmů

Z odborného pohledu je pravdou, že každý solidní obor, každá věcná oblast používá obecné pojmy a specifické pojmy. Pro odbornou oblast zabývající se riziky a bezpečností technických byl vytvořen konzistentní soubor pojmů, který vystihuje současné poznání, jeho základ je v pracích [1,2]. Jde o integrální pojmy, které se vztahují k lidskému systému, jeho podsystémům a k jejich řízení, jejichž cílem je zajištění bezpečí a udržitelný rozvoj lidského systému. Protože předmětné pojmy vznikly na základě mnoha oborového a mezioborového pohledu, existují rozdíly oproti jednotlivým oborům. Je všeobecně známo, že komplexní přístup není možný bez generalizace, a proto není možno vyhovět všem zvláštnostem důležitých oborů, které se historicky vyvinuly.

Na základě systémového chápání světa a konceptu, jehož cílem je zajistit koexistenci lidí, životního prostředí a techniky, tj. sociálního systému, systému životního prostředí a technologického systému jsou dále uvedeny provázané systémy pojmů pro inže-

nýrství pracující s riziky s cílem zajistit bezpečný svět. Je rovněž zvážena stále více se rozvíjející automatizace, a proto předmětný systém systémů dle povahy je socio-kyber-fyzický (technický či technologický) systém [4] a pojmy odpovídají této povaze. Ve všech dále uvedených tabulkách pojmů je upřednostněna logická následnost před abecedním pořadím.

Tabulka 1 shrnuje pojmy spojené s řešením problémů v oblasti integrální bezpečnosti. Je logicky uspořádána dle procesu řešení problémů. Použitý pojem entita je zobecněným pojmem pro území, objekt, technické dílo, stát atd. Tabulka 2 shrnuje pojmy spojené se zpracováním dat a je uspořádána dle logiky vzniku položky. Tabulka 3 obsahuje integrální pojmy pro disciplíny, které pracují s riziky tak, že jejich cílem je vytváření bezpečnosti lidského systému. Její uspořádání je založeno na logice uspořádání pojmů jdoucích od cílů státu, modelu světa až po názvy nástrojů používaných při práci s riziky. Pro informovanost čtenářů jsou v tabulkách uvedeny pojmy používané v anglicky psané odborné literatuře.

Tabulka 1. Obecné pojmy spojené s řešením problémů.

Pojem	**Význam (definice) pojmu**	**Anglický ekvivalent**
Metoda	Způsob, jak dosáhnout jistého předem stanoveného cíle prostřednictvím vědomé a plánovité činnosti, tj. označuje záměrný systematický postup.	Method
Kritérium	Hledisko pro srovnání více entit, parametrů nebo jevů.	Criterion
Kritická položka	Bod, místo, objekt, jev, proces, ve kterém dochází k výrazné změně vlastností sledované entity (podrobné vysvětlení je v práci [17]).	Critical Item
Měření	Způsob určování veličiny srovnáním se stanovenou mírou pomocí jistého přístroje.	Measurement
Experiment	Poznávací metoda, při které se za kontrolovaných a řízených podmínek sleduje jistý jev nebo proces (zjišťují se jím nové vlastnosti, ověřují se jím výsledky výpočtů, hypotéz, vztahů apod.).	Experiment
Zpracování dat	Koordinovaný a vzájemně skloubený soubor všech úkonů nutných pro řešení dané úlohy.	Data Processing
Rozhodovací proces	Logicky provázaná posloupnost jistých kroků od zjištění problému až po formulaci rozhodnutí, tj. výběru jedné z variant z možných řešení daného problému.	Process of Decision-Making
Hodnota	Určitá vlastnost entity.	Value
Hodnocení	Proces přiřazení hodnoty určité entitě, jevu či procesu podle určitých pravidel, tj. podle stupnice hodnot / hodnotové stupnice.	Assessment, Judgement, Evaluation
Problém	Rozpor mezi stavem současným a stavem požadovaným, který nemá zřejmé řešení a na nalezení řešení je třeba vynaložit duševní, anebo i	Problem

	fyzickou práci. Může být úspěšně řešen, je-li včas identifikován a správně formulován.	
Řešení problému	Nalezení a provedení postupu, kterým se dosáhne stanovený cíl nebo přesněji zvládne se úkol, u kterého je znám cíl s větší či menší přesností (určitostí) a je třeba zvolit a použít prostředky, které se opírají o algoritmické nebo heuristické postupy. Řešení do značné míry závisí na charakteru úkolu a na schopnosti řešitelů.	Problem Solving
Metodologie řešení problémů	Ucelený soubor poznatků a principů poznání v určité oblasti. Velkého významu nabývá v málo strukturovaných úlohách, u kterých umožňuje pružně řešit různé úrovně problémů.	Problem Solving Methodology

Tabulka 2. Soubor pojmů pro zpracování dat.

Pojem	**Význam (definice) pojmu**	**Anglický ekvivalent**
Děj	Děj je řada vzájemně propojených událostí v prostoru a čase.	Action
Proces	Proces je vzájemné propojení dílčích soustav pochodů (mechanismů), kterými se uskutečňuje a probíhá děj.	Process
Prvek	Prvek je dílčí součást množiny pochodů, které ve svém souhrnu utvářejí proces a jeho jevy.	Element / Component
Jev	Jev je úkaz, který je výsledkem procesu. Je to soubor vlastností, parametrů a souřadnic, které určují proces či stav, který se za stejných (podobných) podmínek vždy (opakovaně) uskuteční.	Phenomena
Scénář / Režim / Chod	Scénář (režim, chod) je časový průběh jevů v daném prostoru.	Scenario / Regime
Veličina	Veličina je pojem pro vše, čím lze měřit a popsat jevy.	Quantity
Měření veličiny	Měření veličiny je technologický postup (způsob) určení hodnoty dané veličiny.	Quantity Measurement
Jednotka veličiny	Jednotka veličiny je odsouhlasený (smluvený, normativní) rozměr pro číselné vyjádření veličiny.	Quantity Unit
Údaj	Údaj je informace o jevu a jeho vlastnostech, získaná měřením či pozorováním.	Reading / Particular
Data	Data jsou zpracované údaje v daném časoprostoru. Význam dat je věcný, legislativní (viz platné zákony a normy) a arbitrážní (odborné a soudní spory, posuzování škod).	Data
Primární data	Primární data jsou údaje získané přímo měřením a vyhodnocením jevu. Pozn. – měření a vyhodnocení se obvykle provádí v měsíčním, ročním či jiném cyklu v dané enti-	Primary Data

	tě.	
Sekundární data	Sekundární data jsou data získaná dalším vyhodnocením primárních dat (tj. jsou odvozená složitějšími postupy z primárních dat). Způsob vyhodnocení je určen účelem, pro který mají být tato data využita.	Secondary Data
Proměnná / Proměnná veličina	Proměnná veličina je veličina, která může nabývat různých hodnot, pokud ji lze číselně vyjádřit, nebo je to symbol (neměřitelný statistický znak), který může mít různé míry.	Variable
Zákonitost	Zákonitost je kvantitativní nebo kvalitativní vztah (závislost).	Relationship
Parametr	Parametr je veličina (zpravidla používaná jako pomocná proměnná), která charakterizuje daný systém či proces.	Parameter
Charakteristika	Charakteristika je soubor veličin, které popisují podstatné (typické) vlastnosti jevů.	Characteristics
Střední hodnota	Střední hodnota je charakteristika úrovně hodnoty statistického znaku nebo náhodné veličiny. Může to být průměr, medián, modus, či jiná charakteristika.	Mean Value
Rozptyl	Rozptyl je charakteristika proměnnosti hodnot kvantitativního statistického znaku nebo náhodné veličiny.	Dispersion
Standardní odchylka	Standardní odchylka (směrodatná odchylka, střední kvadratická odchylka) je druhá odmocnina z rozptylu.	Standard Deviation
Četnost	Četnost je počet případů zahrnutých do určité skupiny (třídy).	Frequency
Model	Model je popis nebo analogie celku, tj. jde o reprodukci charakteristik určitého objektu na jiném objektu většinou speciálně sestrojeném pro jeho výzkum.	Model
Systém	Systém je entita složená z prvků, vazeb mezi prvky a toků mezi prvky,	System
Ukazatel	Ukazatel (indikátor) je charakteristika sloužící k určení vzniku anebo k hodnocení stavu již probíhajícího jevu.	Indicator
Pozorování	Pozorování je soustavné sledování jevů a procesů v čase i prostoru. Provádí se buď měřením hodnot veličin jejich prvků, nebo stanovením měr neměřitelných znaků.	Observation
Pozorovací síť	Pozorovací (observatorní síť) je soustava entit (územních bodů, stanic, profilů, objektů), ve kterých se provádí pozorování.	Observation Network
Monitoring	Monitoring je specifický způsob sledování a vyhodnocování, sloužící pro získání poznatků potřebných pro rozhodnutí o určitém záměru anebo k vydání výstrahy či předpovědi. Monitoring je	Monitoring

	účelově zaměřené pozorování.	
Monitorovací síť	Monitorovací síť je systém územních bodů, stanic, objektů, profilů aj., ve kterých se provádí monitoring.	Monitoring Network
Databáze	Datová báze (databáze) je věcně uspořádaný soubor dat.	Database
Empirická báze	Empirická báze je soubor poznatků, založených na zkušenosti, získaných pokusem nebo měřením, vyjádřených ve formě kvantitativních závislostí a heuristik (i nejisté a neurčité údaje a poznatky) či získaných od expertů.	Empirical Database
Informační systém	Informační systém je programové vybavení (kybernetický nástroj / nástroj informačních technologií) obsluhující datové báze.	Information System
GIS	Geografický informační systém (GIS) je programové vybavení (kybernetický nástroj / nástroj informačních technologií) umožňující zpracování údajů (např. krajinotvorných prvků) v daném území.	Geographic Information System
Geografická databáze	Geografická databáze je soubor dat o území.	Geographic Database
Časoprostor	Časoprostor (prostoročas) je nerozlučné spojení času s prostorem.	Space-time
Geografická databáze v časoprostoru	Geografická databáze v časoprostoru je soubor vybraných časových řad pro určité území.	Geographic Database in Space-Time
Expertní systém	Expertní systém je programové vybavení obsluhující systém datových bází, matematických modelů a bází empirických hodnot veličin a měr statistických znaků. Se znalostní bází pracuje za pomoci speciálních matematických nástrojů, které dodává teorie mlhavých „fuzzy“ množin. Tento způsob vyhodnocování je výsledkem výzkumu umělé inteligence.	Expert System
Náhodný jev	Náhodný jev je jev, který je vyvolán náhodnými (nedeterministickými) vstupy.	Random Phenomena
Nejistota dat	Nejistota v datech vychází z předpokladu, že odchylky v hodnotách veličin jsou způsobeny náhodností jevu.	Random Data Uncertainties
Neurčitost dat	Neurčitost dat vyplývá ze skutečnosti, že data jsou neúplná, nehomogenní (tj. jejich přesnost závisí na jejich velikosti nebo na čase výskytu), anebo nestacionární (tj. jejich velikost závisí na podmínkách). Neurčitá data mají značný rozptyl a jsou zatížená náhodnými a někdy i systematickými chybami, jejichž funkce rozdělení obvykle není možno stanovit. Neurčitosti v datech souvisí s náhlými změnami procesů.	Data Undeterminatess Data Knowledge Uncertainty Data Epistemic Uncertainty

Agregace dat	Agregace dat je seskupení prvků, mezi nimiž neexistují pevnější vazby a spojuje je jen jedna společná vlastnost nebo prostorová blízkost.	Data Aggregation
Významnost	Významnost je věrohodnost výskytu či velikosti jevu či hodnoty veličiny.	Significance / Relevance
Nejlepší odhad	Kvantifikované stanovení hodnoty veličiny / charakteristiky provedené za předpokladů, které se pokud možno co nejvíce přibližují pravděpodobným skutečným hodnotám.	Best Estimate
Odchylka měření	Rozdíl mezi střední hodnotou výsledků měření a dohodnutou referenční hodnotou.	Measure Difference
Výsledek měření	Hodnota určité charakteristiky, získaná použitím konkrétní zkušební metody. Zkušební metoda má specifikovat provedení jednoho nebo více pozorování a jako výsledek zkoušky se uvede jejich aritmeticky průměr nebo jiná vhodná funkce (např. jejich medián nebo výběrová směrodatná odchylka). Může se vyžadovat použití korekcí na normální podmínky, např. korekce objemu plynu na normální teplotu a tlak. Výsledkem zkoušky tedy může být hodnota vypočtená z několika pozorovaných údajů. V jednoduchém případě je výsledkem zkoušky jediná pozorovaná hodnota.	Measure Result
Měřící rozsah	Rozsah definovaný dvěma hodnotami měřené nebo vytvářené veličiny, pro kterou jsou specifikovány meze chyby měřidla. Pozn. - měřidlo může mít několik měřicích rozsahů.	Measure Range
Třídění	Rozdělení údajů, dějů, procesů a jevů do kategorií (tříd) podle zvolených (dle cíle vybraných) kritérií.	Ranking
Analýza	V systémovém pojetí metoda, která se snaží nějaký celek, proces či jev vysvětlit myšlenkovým či faktickým rozborem jeho prvků, složek, vazeb, toků a vnitřních spřažení. V analýze rizik to je metoda používající otázky typu „Co se stane, když…“ k identifikaci zdrojů rizik (zranitelností vůči dané pohromě), kvalitativnímu posuzování existujících ochranných a bezpečnostních opatření a hledání základních scénářů průběhu pohromy. Výsledkem je seznam otázek a odpovědí o procesu, popř. tabulkový seznam nouzových situací doplněný o ochranu před dopady a o návrhy na snížení zranitelnosti, a tím i na snížení rizika.	Analysis
Pravděpodobnostní přístup	Pravděpodobnostní přístup je založen na předpokladu, že výskyt každého jevu má určitou náhodnou nejistotu, tj. možnost výskytu náhodného jevu je odhadnuta určitou hodnotou pravděpodobnosti.	Probabilistic Approach
Deterministický přístup	Deterministický přístup je založen na předpokladu, že každý jev je nutným důsledkem podmínek	Deterministic Approach

	a příčin.	
Konzervativní přístup	Konzervativní přístup je založen na předpokladu, že z důvodu bezpečnosti je nutno při odhadech a výpočtech zvážit právě ty hodnoty základních veličin, které vystihují nejméně příznivý případ a při splnění zajišťují nejvyšší dosažitelnou bezpečnost.	Conservative Approach
Heuristický přístup	Heuristický přístup je založen na tvůrčím myšlení na základě získaných zkušeností. Cílem je vybrat na základě zkušeností řešení problému, které nejlépe vyhovuje stanoveným podmínkám.	Heuristic Approach

Tabulka 3. Integrální pojmy pro disciplíny pracující s rizikem a bezpečností.

Pojem	**Význam (definice) pojmu**	**Anglický ekvivalent**
Základní funkce státu	Základní funkcí státu je zajistit bezpečí chráněných aktiv (zájmů) státu a udržitelný rozvoj státu. Pozn.: Stát je chápán jako útvar, v němž lidé, vládnoucí moc a území spadají pod jednu podstatu (tj. souhrn hlubinných vlastností, vztahů a vnitřních zákonitostí, které určují hlavní rysy a tendence vývoje daného systému).	Fundamental State Functions
Chráněná veřejná aktiva (zájmy) státu či území	Chráněná aktiva (zájmy) státu jsou aktiva státu, které jsou prioritně ochraňovány (životy, zdraví a bezpečí lidí, majetek, životní prostředí, veřejné blaho, technologie, infrastruktura). Pozn. 1: Chráněná aktiva jsou definována v základních právních předpisech / ústavě a jsou předmětem nouzového plánování. V tomto případě se používá i pojem právem chráněné zájmy. Pozn. 2: Chráněná aktiva v ČR jsou dle legislativy ČR životy a zdraví lidí, majetek a životní prostředí. Pozn. 3: Mezi chráněná aktiva se i v ČR postupem doby zařazují také veřejné blaho a kritická infrastruktura, a to přesto, že kritickou infrastrukturu, fyzickou i kybernetickou, lze v mnoha případech považovat za součást majetku. Pozn. 4: Jde o základní chráněná veřejná aktiva, protože nenastala-li nouzová situace tak ochraňujeme a zajišťujeme rozvoj i dalších aktiv jako jsou kulturní a přírodní památky, historické monumenty, kultura, rekreace apod.	Protected Public Assets Human System Assets.
Chráněná aktiva technického díla	Chráněná aktiva technického díla jsou veřejná aktiva a aktiva technického díla, která zajišťují jeho bezpečnost, tj. jeho existenci, spolehlivost, funkčnost a konkurenceschopnost.	Protected Assets of Technological Facility

Lidský systém	Lidský systém je minimální prostor pro život člověka a lidskou společnost, tj. zahrnuje prvky, které tvoří lidé, části životního prostředí nezbytné pro život lidí, části planety Země nezbytné pro život lidí, majetek, technologie, infrastruktury a vazby a toky mezi těmito prvky.	Human System
Chráněné aktiva lidského systému	Chráněná aktiva lidského systému jsou komponenty, vazby a toky v lidském systému, které jsou nutné pro jeho bezpečí a udržitelný rozvoj. Jsou prioritně ochraňovány a zahrnují životy, zdraví a bezpečí lidí, majetek, životní prostředí, veřejné blaho, technologie a infrastruktury. Pozn. 1: V některých konceptech bezpečí je nejvyšší cíl a inherentně zahrnuje udržitelný rozvoj. Pozn. 2: Pro udržitelný rozvoj lidského systému je nutné, aby chráněná aktiva státu byla totožná s chráněnými aktivy lidského systému.	Human System Protected Affairs / Human System Assets
Bezpečí	Bezpečí je stav systému, při kterém vznik újmy na chráněných aktivech má přijatelnou pravděpodobnost (tj. je téměř jisté, že újma nevznikne). Pozn.: Podobně je definováno bezpečí jednotlivého chráněného aktiva či bezpečí technického díla.	Security
Nebezpečí	Nebezpečí je stav systému, při kterém vznik újmy na chráněných aktivech má vysokou pravděpodobnost (tj. je téměř jisté, že újma vznikne). Pozn. 1: Podobně je definováno nebezpečí jednotlivého chráněného aktiva či nebezpečí technického díla. Pozn. 2: Nebezpečí je bezprostřední, když vývoj nezadržitelně směřuje ke vzniku pohromy a tím ke vzniku nouzové situace a je plíživé, když vývoj směřuje ke vzniku pohromy nenápadně a bez zřejmých příznaků.	Jeopardy
Bezpečnost	Bezpečnost je soubor antropogenních opatření a činností k zajištění bezpečí a udržitelného rozvoje systému, tj. k zajištění bezpečí a udržitelného rozvoje chráněných aktiv. Pozn. 1: Bezpečnost v tomto pojetí zahrnuje opatření a činnosti k ochraně aktiv, i k funkčnosti a spolehlivosti infrastruktur a technologií. Pozn. 2: U systémů se měří na úrovni systému, tj. je vlastností celého systému (mírou kvality souboru opatření a činností k zajištění bezpečí a rozvoje systému) a ne jeho dílčích částí.	Safety
Integrita bezpečnosti systému	Integrita bezpečnosti systému je vlastnost systému, která vyjadřuje míru schopnosti systému zajistit svoji bezpečnost.	System Safety Integrity
Úroveň integrity bezpečnosti (SIL)	Úroveň integrity (celistvosti) bezpečnosti entity je míra, s níž je bezpečnost entity zajištěna (použí-	Safety Integrity Level

	vají se 4 stupně).	
Nebezpečnost	Nebezpečnost je soubor vlastností a charakteristik prvků, látek, pohrom, procesů a činností, které na chráněných aktivech působí nebo za jistých podmínek mohou působit újmu (zdroj zranění, škod, ztrát). Je doplňkovou veličinou k bezpečnosti. Při provozu technických děl je nahrazována pojmem kritičnost.	Danger
Kritičnost	Kritičnost je vlastnost systému, která se měří kvalitou souboru opatření a činností s ohledem na bezpečí systému; při menších hodnotách je stav systému bez problému a při vyšších hodnotách je vysoká pravděpodobnost vzniku havárií či selhání systému. Je doplňkovou veličinou k bezpečnosti. Zahrnuje i nefunkčnost a nespolehlivost infrastruktur a technologií.	Criticality
Zabezpečený systém	Zabezpečený systém je systém, který je ochráněn proti pohromám všeho druhu (vnitřním, vnějším, lidskému faktoru).	Secure System
Bezpečný systém	Bezpečný systém je zabezpečený systém, který ani při svých kritických podmínkách neohrozí sebe, ani své okolí.	Safe System
Selhání systému	Selhání systému znamená, že systém neplní požadované úkoly v očekávaný čas, na daném místě a v požadované kvalitě.	System Failure
Systém systémů - SoS	Je soubor otevřených a vzájemně propojených systémů.	System of systems (SoS)
Složitost systému	Vlastnost systému, která způsobuje, že za jistých podmínek se uplatní neočekávaná propojení některých prvků či systémů a dojde k selhání systému nebo jeho části.	System Complexity
Bezpečný systém systémů	Bezpečný systém systémů je ochráněný proti všem pohromám, nežádoucímu působení lidského faktoru i škodlivým propojením a sám neohrožuje ani sebe, ani své okolí, a to ani při svých kritických podmínkách.	Safe system of systems
Lidské bezpečí	Lidské bezpečí je stav lidského systému, při kterém vznik újmy na lidech má přijatelnou pravděpodobnost, a to při zvážení všech prvků, vazeb a toků v lidském systému, které mohou zprostředkovat nebo přispět ke vzniku újmy na lidech.	Human Security
Lidská bezpečnost	Lidská bezpečnost je soubor opatření a činností k zajištění bezpečí a udržitelného rozvoje lidí a lidské společnosti, a to při zvážení všech prvků, vazeb a toků v lidském systému, které mohou zprostředkovat nebo přispět ke vzniku újmy na lidech nebo lidské společnosti. Pozn.: Lidská bezpečnost v tomto pojetí zahrnuje	Human Safety

	opatření a činnosti k ochraně lidí a lidské společnosti.	
Škoda	Škoda je újma na životě, zdraví a bezpečí lidí, majetku, veřejném blahu, životním prostředí, infrastrukturách a technologiích, kterou lze vyjádřit v penězích. Pozn.: Újma je nejobecnější pojem vyjadřující ztrátu nebo poškození chráněného zájmu.	Damage / Harm
Zranitelnost	Zranitelnost je náchylnost (citlivost) chráněného aktiva ke vzniku škody.	Vulnerability
Dopad	Dopad je nepříznivý účinek (působení) jevu v daném místě a čase na chráněná aktiva.	Impact / (Effect)
Nepřípustný / Nepřijatelný dopad	Nepřípustný dopad je dopad, který může způsobit nebo způsobí nepřijatelnou škodu na jednom či více chráněných aktivech.	Inadmissible / Unacceptable (Severe) Impact
Pohroma	Pohroma je jev, který vede nebo může vést k újmě a značné škodě na chráněných zájmech. Tj. je to jev, který vede nebo může vést k nepřijatelnému dopadu na chráněná aktiva. Pozn. 1: V českém jazyce jsou také v definovaném smyslu používány pojmy „porucha, nehoda, havárie, pohroma, kalamita, katastrofa“, mezi kterými jsou významové rozdíly. Pozn. 2: Z pohledu kybernetiky je pohroma jeden z možných stavů systému, který vede nebo může vést ke škodě na jednom či více chráněných aktivech. Pozn. 3: Význačné světové a evropské finanční instituce (Světová banka, Evropská banka, orgány OSN a další) používají pojem pohroma (anglicky „Disaster“) obvykle pro jevy doprovázené malým počtem obětí; je-li počet obětí větší (obvykle více než 25), používají pojem katastrofa (anglicky „Catastrophe“). Pro jevy se značným počtem lidských obětí se mluví o humanitární katastrofě. Pozn. 4: Pro klasifikaci některých pohrom existují stupnice založené na jejich fyzikální velikosti i stupnice založené na ocenění velikosti jejich dopadů podle popisných znaků [17]. Pozn. 5: Projektová pohroma je určitá velikost pohromy, až do které se zajišťuje odolnost chráněných aktiv lidského systému či jiné entity, např. technického díla prevencí. Pozn. 6: Nadprojektová pohroma je určitá velikost pohromy, vůči které se zajišťuje odolnost jen vybraných chráněných aktiv lidského systému.	Disaster In specific cases: Calamity, Catastrophe, Humanitarian Catastrophe Design Disaster Beyond Design Disaster Severe Disaster

Lidský faktor	Vrozené způsoby člověka, kterými reaguje na podněty, tj. podmíněné reakce a cílevědomé vůlí řízené jednání.	Human Factor
Selhání lidského faktoru	Buď špatné provedení úkonu, anebo provedení špatného rozhodnutí.	Human Factor Failure
Organizační havárie	Organizační havárie je havárie nebo selhání entity způsobené špatným rozhodnutím člověka, který rozhodnutí provádí.	Organizational Accident
Kultura bezpečnosti	Soubor pravidel zacílený na tvorbu bezpečného systému entity.	Safety Culture
Ohrožení	Ohrožení spojené s danou pohromou je soubor maximálních dopadů pohromy, které lze očekávat v daném místě za specifikovaný časový interval s pravděpodobností rovnou stanovené hodnotě. Podle norem a standardů je obvykle určeno velikostí pohromy, která se vyskytne s pravděpodobností větší nebo rovné 0.05 s ohledem na četnostní rozdělení pro časový interval sto let. V technické praxi ohrožení spojené s pohromou je normativní velikost pohromy na stanovené hladině věrohodnosti (stoletá, tisíciletá apod.). Pro potřeby praxe se vyjadřuje souborem dopadů na chráněná aktiva. Pozn. 1: V uvedeném případě jde o ohrožení od stoleté pohromy (např. stoleté povodně, stoletého zemětřesení). Pozn. 2: Pro specifické účely (v případech, kde je třeba zajistit vyšší bezpečnost) se používají statistiky založené na četnostním rozložení pro 1 000 a 10 000 let. Pozn. 3: Ohrožení je inherentní vlastnost pohromy určená procesem, který ji vyvolává. Pozn. 4: Pro stanovení ohrožení se používají metody založené na teorii extrémních hodnot a datové soubory, které obsahují i historická data. Jimi se stanoví největší očekávaná velikost pohromy pro vybraný časový interval.	Hazard
Riziko	Riziko je míra nepřijatelných dopadů způsobených pohromou o velikosti rovné hodnotě ohrožení. Riziko je pravděpodobná velikost škod, ztrát a újmy na chráněných aktivech, která odpovídá ohrožení spojené s pohromou, které je normativně stanovené. Pozn. 1: Při definici rizika panuje značná nejednotnost, např. se používá koncept, že riziko je pravděpodobnost, že vznikne nebo může vzniknout událost nebo soubor událostí, které zcela mění žádoucí (původně předpokládaný) stav či	Risk

	vývoj chráněných zájmů státu z hlediska jejich celistvosti a funkce. Pozn. 2: Riziko závisí jak na velikosti dané pohromy, tak na vlastnostech území, které předurčují zranitelnost území vůči pohromě a také na vlastnostech chráněných aktiv v daném území, které rovněž předurčují zranitelnost vůči pohromě. Je určeno ohrožením od pohromy (tj. dopady způsobenými vypočtenou velikostí pohromy) a zranitelností chráněných aktiv v daném místě a v daném časovém intervalu, tj. je místně a časově specifické. Pozn. 3: V praxi je třeba zvažovat technickou zranitelnost, zranitelnost vyvolanou počtem lidí, kybernetickou zranitelnost aj. Pozn. 4: ***V technické praxi*** v kvantitativní analýze rizik používané ve strategickém řízení je riziko rovno velikosti ztrát, škod a újmy na chráněných aktivech při normativní velikosti pohromy normované na jednotku území a jednotku času (obvykle 1 rok). Pozn. 5: Matematicky je míra rizika = míra ohrožení x míra zranitelnosti.	
Hrozba	Hrozba je míra výskytu útoku (teroristického nebo vojenského) v daném místě. Je to pravděpodobnost, že vznikne nebo může vzniknout událost nebo soubor událostí, zcela odlišných od žádoucího stavu či vývoje chráněných aktiv z hlediska jejich celistvosti a funkce. Pozn. 1: Hrozba je určena schopností útočníka, zranitelností chráněných aktiv státu a úmyslem útočníka. Pozn. 2: Matematicky je míra hrozby = míra schopnosti útočníka x míra zranitelnosti x míra úmyslu útočníka.	Threat
Nouzová situace	Nouzová situace je situace, kterou v území či objektu vyvolá vznik pohromy. Pozn.: V české legislativě se pro některé nouzové situace používá označení mimořádná událost, pro jiné zase kalamita nebo selhání atd.	Emergency / Emergency Situation
Kategorie nouzové situace	Kategorie nouzové situace je mírou závažnosti nouzové situace z hlediska jejich dopadů na chráněná aktiva. Pozn. 1: Kategorie nouzové situace závisí na době trvání, intenzitě dopadů pohromy, velikosti oblasti zasažené dopady pohromy a na množství lidí zasažených dopadem pohromy. Pozn. 2: Rozlišují se následující kategorie: 0: zanedbatelné z hlediska života občana, 1: nedůležité z hlediska občana, 2: důležité z hlediska občana,	Emergency Categories

	3: závažné z hlediska společnosti, 4: velmi závažné z hlediska společnosti, 5: ohrožující existenci či podstatu společnosti. Pozn. 3: Kategorie se pro jednoduchost označují barvami (nejvyšší pak posloupností barev – žlutá, oranžová, červená).	
Nástroje entity k zajištění ochrany chráněných aktiv a k zajištění rozvoje entity	Nástroje entity k zajištění bezpečí a udržitelného rozvoje chráněných zájmů jsou: - řízení všech úrovní entity založené na kvalifikovaných datech a správných metodách rozhodování, - výchova a vzdělání občanů či zaměstnanců, - specifická výchova technických a řídících pracovníků, - standardy, normy a předpisy, tj. regulace procesů, které mohou nebo by mohly vést k výskytu (vzniku) pohromy, - inspekce, - výkonné složky ke zvládnutí nouzové situace, - plánování: bezpečnostní / územní / nouzové / krizové. Pozn.: Systém vzdělávání ČR zajišťuje, že každý občan je schopen zvládnout nouzovou situaci kategorie 1 a 2, díky své výchově a přípravě.	Entity Tools for Emergency Planning Objectives Achievement
Bezpečnostní plánování	Je plánování pro potřeby zajištění bezpečného systému / území / objektu a jeho udržitelného rozvoje. Zahrnuje územní plánování, plánování na úseku hygienické služby, plánování rozvoje sektorů sledovaných v kompetenčním zákoně (zákon č. 2/1969 Sb. v platném znění) a zajišťuje jejich soulad a prosazení priorit, které určuje výzkum a zkušenosti.	Security Planning
Územní plánování	Plánování pro potřeby zajištění bezpečného území a udržitelného rozvoje území.	Land-Use Planning
Nouzové plánování	Nouzové plánování je plánování souboru antropogenních opatření a činností pro zmírnění dopadů pohrom, kterým nelze zabránit předem a pro implementaci opatření nutných pro zvládnutí nouzových situací. Je to soubor opatření a činností pro: - předcházení a zabránění výskytu pohrom, kterým zabránit lze, - zmírnění dopadů pohrom, kterým nelze zabránit, - implementaci opatření nutných pro zvládnutí nouzových situací kategorie 2 – 4, - zajištění stabilizace situace, obnovy a dalšího rozvoje. Pozn. 1: Nouzové plánování není v ČR právně definované jako celek. Právem jsou definovány jen vybrané části, např. havarijní plánování ve smyslu zákona č. 239/2000 Sb.; a povodňové	Emergency Planning

	plány. Pozn. 2: Nouzové plánování též obsahuje plánování pro předcházení a zabránění vzniku pohrom či zmírnění jejich dopadů na chráněná aktiva v oblastech jako: ekonomika, informatika, bankovnictví, životní prostředí (epidemie, epizootie, epifytie) aj., tj. zajišťuje i ochranu infrastruktur a technologií. Pozn. 2: Nouzové plánování navazuje na bezpečnostní plánování a používá standardní zdroje, síly a prostředky.	
Krizové plánování	Krizové plánování je plánování souboru opatření a činností pro zmírnění dopadů kritických situací (tj. nouzových situací kategorie 5) na chráněná aktiva státu, kterým nelze zabránit předem a pro implementaci opatření nutných pro zvládnutí kritických situací za přijatelných zdrojů, sil a prostředků. Jde o soubor opatření a činností, kterými se: - sníží na přijatelnou míru výskyt nouzových situací kategorie 5, - umožní situace kategorie 5 zvládnout, - zmírní dopady nouzových situací kategorie 5 na chráněná aktiva, - zajistí obnovu a další rozvoj chráněných aktiv. Pozn. 1: Krizové plánování je základní součástí krizového řízení. Pozn. 2: Krizové plánování navazuje na nouzové plánování a používá standardní i nadstandardní zdroje, síly a prostředky.	Crisis Planning
Hodnocení pohromy Hodnocení ohrožení Hodnocení rizik	Hodnocení pohromy / Hodnocení ohrožení / Hodnocení rizik jsou pracovní metody inženýrských disciplín pracujících s riziky. Podle charakteru pohromy se použijí u: - měřitelných pohrom příslušné (technickými normami nebo obdobnými právními předpisy stanovené) deterministické nebo pravděpodobnostní přístupy, - u neměřitelných pohrom (oblast veřejného pořádku, ekonomiky, peněžnictví, informatiky, terorismu aj.) přístupy založené na agregaci (zásady agregace jsou určené technickými normami nebo obdobnými právními předpisy) statistických znaků.	Disaster Assessment Hazard Assessment Risk Assessment
Scénář pohromy	Scénář pohromy je soubor izolovaných i propojených dopadů pohromy v území či objektu a čase, který vyvolá nebo může vyvolat vznik událostí lišících se od předpokládaného stavu či vývoje systému (objektu), jeho celistvosti a funkce. Pozn. 1: Statický problém - scénář pohromy je	Disaster Scenario

	model zobrazující rozložení dopadů pohromy v území. Pozn. 2: Dynamický problém - scénář pohromy je model zobrazující rozložení dopadů pohromy v území a v čase. Pozn. 3: Pro plánování musí být použita normativní definice, protože rozložení dopadů v prostoru i čase závisí na místních podmínkách, které působí anomálie.	
Relevantní pohroma	Relevantní (významná) pohroma je pohroma, která v daném území má nebo může mít dopady.	Relevant Disaster
Specifická pohroma	Specifická pohroma je relevantní pohroma, která v daném území za určený časový interval (není-li stanoveno jinak, tak 100 let) má nebo může mít nepřípustné (nepřijatelné) dopady.	Specific Disaster
Kritická pohroma	Kritická pohroma je specifická pohroma, která v daném území za určený časový interval (není-li stanoveno jinak, tak 100 let) má nebo může mít nepřípustné (nepřijatelné) dopady takové intenzity nebo rozsahu, které vedou k destabilizaci území či jiné sledované entity. Podle TQM [56] jde o prioritní pohromu, která se monitoruje při řízení bezpečnosti entity.	Critical Disaster
Kritická situace	Kritická situace je nouzová situace vyvolaná výskytem kritické pohromy, tj. nouzová situace kategorie 5.	Critical Situation
Monitoring	Monitoring je specifický způsob sledování a vyhodnocování údajů v čase a území, sloužící pro získání poznatků potřebných pro rozhodnutí o určitém záměru anebo k vydání výstrahy či předpovědi. Pozn. 1: Monitoring je způsob sledování umožňující následné vyhodnocení získaných poznatků pro získání podkladů pro rozhodnutí o určitém záměru anebo k vydání výstrahy či předpovědi. Pozn. 2: Monitoring je specifické pozorování procesů, jevů, prvků apod., které je zaměřené k jistému cíli, tj. sleduje se jen to, co je vybrané. Tím se liší od širšího pojmu „pozorování“.	Monitoring
Opatření	Opatření je antropogenní nástroj k odvrácení a ke zmírnění dopadů pohromy v prostoru a čase (odvrácení, zmírnění či zvládnutí nouzové situace) nebo k zajištění obnovy a rozvoje chráněných aktiv.	Measure
Ochrana	Ochrana je soubor antropogenních opatření a činností pro zachování a udržitelný rozvoj chráněných aktiv. Je založena na principu předběžné opatrnosti. Pozn.: Bezpečnost inherentně zajišťuje ochranu.	Protection
Zvládnutí nouzové	Zvládnutí nouzové situace je dosažení stavu, při	To Put (Bring / De-

situace	kterém škody vzniklé v důsledku výskytu nouzové situace jsou tak nízké, že jsou snadno odstranitelné nebo přijatelné.	feat) Emergency Situation under Control
Odezva	Odezva na nouzovou situaci je provedení souboru antropogenních činností a opatření, který vede ke zvládnutí nouzové situace, tj. ke: - stabilizaci situace v postižené oblasti a jejím okolí, - zamezení či alespoň omezení dalšího rozvoje nouzové situace, - zamezení či alespoň zmírnění dopadů na lidi, majetek, životní prostředí, lidskou společnost, technologie a infrastruktury. U pohrom, které jsou předvídatelné, anebo vznikají pozvolna (např. povodeň) lze stanovit několik vývojových fází (stavů) a dle nich rozdělit odezvu a její přípravu do několika etap: - bdělost – varování, - pohotovost, - vlastní odezva. Pozn. 1: Odezva výkonných složek se obvykle nazývá zásah a je pro potřeby zvládnutí situace rozdělena z pohledu sil a prostředků, jejich materiálního zabezpečení a dalších aspektů. Pozn. 2: V ČR je pro zvládnutí mimořádných událostí kodifikován Integrovaný záchranný systém.	Response
Obnova	Obnova je soubor antropogenních opatření a činností pro zajištění stability území / objektu, likvidaci odstranitelných škod v území / objektu a pro zahájení (nastartování) dalšího rozvoje území / objektu.	Renovation / (Return)
Scénář odezvy	Scénář odezvy je propojený soubor antropogenních opatření a činností v čase a prostoru, který stanovuje postup ke zvládnutí nouzové situace. Pozn. 1: Scénář zásahu je spojen s odezvou prováděnou výkonnými složkami a je součástí scénáře odezvy, který logicky připravuje správce území nebo správce objektu.	Response Scenario
Specifický scénář odezvy	Specifický scénář odezvy je scénář odezvy na specifickou pohromu, který je založen na znalostech podstaty pohromy a jejich dopadů. Připravuje ho výkonná složka, která je odpovědná za zvládnutí této pohromy.	Specific Response Scenario Response Scenario to Specific Disaster
Kritický scénář odezvy	Kritický scénář odezvy je scénář odezvy na kritickou pohromu. S ohledem na charakter kritické pohromy ho na úrovni státu připravují vláda a ústřední správní úřady.	Critical Response Scenario Scenario to Critical Disaster
Scénář obnovy	Scénář obnovy je propojený soubor antropogenních opatření a činností, který vede ke stabilizaci	Renovation Scenario

	situace, k likvidaci odstranitelných škod a k nastartování dalšího rozvoje. Patří do něho plán na prevenci ztrát při obnově.	
Prevence	Prevence je soubor antropogenních opatření a činností pro snížení pravděpodobnosti výskytu pohromy / vzniku nouzové situace a popř. pro provádění opatření na zmírnění dopadů pohromy / nouzové situace předem.	Prevention
Připravenost	Připravenost je: - vypracování příslušných scénářů odezvy, - zajištění příslušných výkonných složek a jejich výcviku, pomůcek, osob, technických prostředků a financí pro realizaci příslušných scénářů odezvy, - zajištění příslušného vzdělání a přípravy veřejné správy, občanů a dalších zúčastněných a jejich případného materiálně technického vybavení.	Preparedness
Výkonná složka	Výkonná složka je zvláště vytvořená, speciálně vzdělaná, vyškolená a vybavená složka určená k provádění zásahu při nouzových a kritických situacích. Pozn.: V ČR jsou těmito složkami Hasičský záchranný sbor ČR (HZS), Policie ČR, zdravotníci, Armáda ČR, vodní záchranáři aj. Jsou spojeny do integrovaného záchranného systému (IZS), který je koordinován HZS.	Effective Force (Units) Force (Units)
Systém odezvy na pohromy¨ Záchranný systém	Provázaný systém spolupráce všech zúčastněných, tj. veřejné správy, výkonných složek, občanů a dalších, kteří provádí odezvu na pohromy. Pozn. 1: V ČR je právem vytvořena jen část systému odezvy, tj. Integrovaný záchranný systém, stanovený v zákoně č. 239/2000 Sb. Pozn. 2: V ČR je systém vycházející od správce území (veřejné správy) vytvořen právně jen pro krizové situace (zákon č. 240/2000 Sb.). Pozn. 3: V ČR chybí právem zřízené specializované týmy připravené k likvidaci pohrom v ekonomice, peněžnictví, informatice apod.; problémy se řeší ad hoc.	Disaster Relief Response Organisation
Řízení	Řízení obecně tvoří soubor postupů a procedur pro hledání a řešení problémů. Skládá se z plánování, vedení a organizace pracovní činnosti lidí, rozdělování prostředků, hodnocení účinnosti postupů, kontroly stavu a v případě potřeby i aplikace nápravných opatření.	Management
Řízení rizika	Řízení rizika je řízení souboru antropogenních opatření a činností tak, aby škody a ztráty na aktivech byly nižší než stanovená úroveň (obvykle stanovené úrovně – ALARP a ALARA).	Risk Management

	Řízení rizika je plánování, organizování, přidělování pracovních úkolů a kontrola zdrojů organizace tak, aby byly minimalizovány ztráty, škody, zranění nebo úmrtí vyvolané různými pohromami, jejichž výskyt je pravděpodobný. Pozn. 1: Rizika se snižují snížením zranitelnosti objektů, populace, životního prostředí, státu atd. (v těchto souvislostech se používá také pojem zmírňování dopadů, které při výskytu pohromy nelze odvrátit). Pozn. 2: Podle většiny technických norem a standardů se při plánování, projektování, výstavbě a provozu technických děl snížení zranitelnosti provádí pro všechna rizika, jejichž pravděpodobnost výskytu je větší nebo rovná 0.05. Pozn. 3: Řízením rizika se vytváří jistá úroveň inherentní bezpečnost lidského systému, tj. tzv. projektové pohromy by měly být zvládnuty projektem, předpisy pro územní plánování a výstavbu, provozními předpisy, předpisy pro zvládnutí nouzové situace a instrukcemi pro zvládnutí kritických situací a jejich výskyt by tudíž neměl ohrozit udržitelný rozvoj.	
Řízení bezpečnosti	Řízení bezpečnosti je řízení souboru antropogenních opatření a činností tak, aby škody a ztráty na aktivech byly přijatelné. Řízení bezpečnosti spočívá v plánování, organizování, přidělování pracovních úkolů a v kontrole využívání zdrojů organizace s cílem dosáhnout požadované úrovně bezpečnosti. Pozn. 1: Zvýšení bezpečnosti se dosáhne využíváním (aplikací, realizací, implementací) technických, právních, organizačních, vzdělávacích aj. ochranných opatření. V úvahu se berou i rizika, jejichž pravděpodobnost výskytu je menší než 0.05, ale dopady s nimi spojené jsou velmi závažné (kruté). Pozn. 2: Řízení bezpečnosti se někdy označuje jako řízení rizik ve prospěch bezpečí, do kterého se zahrnuje i udržitelný rozvoj. Pozn. 3: Řízení bezpečnosti je běžné při plánování, projektování, výstavbě a provozu technických zařízení a objektů jakými jsou elektrárny, přehrady, jaderná zařízení aj. a je tudíž základem jaderné bezpečnosti, radiační ochrany a ochrany před nebezpečnými chemickými látkami, zaváděné direktivou Seveso III. V technickém slangu mluvíme o tom, že v rámci tohoto řízení se zohledňují tzv. nadprojektové havárie. Pozn. 4: Řízením bezpečnosti se vytváří inherentní bezpečnost lidského systému vůči projektovým pohromám a implementací principu před-	Safety Management

	běžné opatrnosti zajišťuje zvýšení odolnosti vůči nepřijatelným dopadům nadprojektových pohrom, jejichž výskyt je tak málo pravděpodobný, že je nepředvídatelný.	
Krizové řízení	Krizové řízení je řízení, jehož cílem je zajistit zvládnutí možných kritických situací v rámci působnosti orgánu krizového řízení a plnění opatření a úkolů uložených vyššími orgány krizového řízení (ke zvládnutí se zpravidla používá právní opatření „vyhlášení krizové situace nebo krizového stavu“, které umožňuje dočasně omezit práva a svobody lidí, použít nadstandardní zdroje apod.), a to včetně zajištění přípravy na zvládnutí možných kritických situací. Pozn. 1: Krizové řízení je nedílnou součástí řízení státu, organizace, správy technického díla či jiné instituce, které mají zájem na svém rozvoji. Jeho cílem je: - identifikovat, rozpoznat a předcházet vzniku možných kritických situací, - zajistit přípravu na zvládnutí možných kritických situací, - zajistit zvládnutí možných kritických situací v rámci působnosti orgánu krizového řízení a plnění opatření a úkolů uložených vyššími orgány krizového řízení (ke zvládnutí se zpravidla používá právní opatření „vyhlášení krizové situace“, které umožňuje dočasně omezit práva lidí a použít nadstandardní zdroje), - nastartovat obnovu a další rozvoj. Pozn. 2: V některých pojetích je krizové řízení součástí řízení bezpečnosti, v jiných zase se krizové řízení používá jen pro případ zvládnutí kritických situací vyvolaných pohromami a pro zvládnutí „běžných“ nouzových situací se používá nouzové řízení. Pozn. 3: Krizové řízení vyvíjí nástroje pro zvládnutí nouzové situace kategorie 5. Pozn. 4: Krizové řízení je nástroj pro zajištění udržitelného rozvoje společnosti, organizace, území a státu.	Crisis Management
Matice odpovědnosti	Matice odpovědnosti určuje pro danou činnost způsob řízení, tj. určuje koordinující resort a resorty, které podporují činnost tohoto resortu dle jeho pokynů. Slouží k zajištění řešení problémů.	Responsibility Matrix
Zázemí státu nutné pro splnění cílů krizového řízení	Zázemí státu nutné pro splnění cílů krizového řízení je tvořeno službami a příslušnou technickou, kybernetickou a organizační infrastrukturou, jejichž správná činnost je nutná pro zajištění ochrany chráněných zájmů státu.	Emergency Support Functions
Kritická infrastruktura	Kritická infrastruktura jsou fyzické, kybernetické	Critical Infrastructu-

	a organizační (obslužné) systémy, které jsou nutné pro zajištění ochrany životů a zdraví lidí a majetku, minimálního chodu ekonomiky a správy státu. Pozn.: Jde o minimální množství funkčních infrastruktur, které zajistí při kritické situaci přežití lidí, stabilizaci situace a umožní nastartování rozvoje.	re
Nouzový plán	Nouzový plán je základní podklad pro implementaci cílů nouzového řízení. Stanovuje postupy pro předcházení pohromám, postupy na zvládnutí nouzových situací s přijatelnými ztrátami a zdroji a postupy na zajištění obnovy a dalšího rozvoje státu.	Emergency Plan
Krizový plán	Krizový plán je základní podklad pro implementaci cílů krizového řízení. Stanovuje postupy pro předcházení velkým pohromám, postupy na zvládnutí kritických situací za přijatelných ztrát a zdrojů a postupy na zajištění obnovy a dalšího rozvoje státu. Pozn. 1: Obvykle se na úrovni správy státu zpracovávají tři druhy plánů, a to: - krizový plán území, - krizový plán úřadu státní správy, - plán ústředního úřadu státní správy (v ČR tzv. soubor typových plánů). Pozn. 2: Každá organizace s rozumným vedením má plán na zvládnutí kritických situací, tj. plán na přežití kritických situací (tzv. contingency) a pro případ, že tento plán selže, má plán krizový.	Crisis Plan / State Response Plan
Plán kontinuity	Plán odezvy, který obsahuje postupy, nástroje a činnosti pro zvládnutí selhání technologií, infrastruktur a služeb s cílem zajistit jejich přežití, tj. minimální bezpečnost, spolehlivost a funkčnost při kritických situacích.	Continuity Plan
Civilní nouzové plánování	Civilní nouzové plánování je nouzové plánování zaměřené na splnění cílů aliance NATO.	Civil Emergency Planning - CNP
Nepravděpodobná událost	Událost, která je neočekávaná na základě provedené analýzy rizik na stanovené hladině věrohodnosti.	Unexpected Event
Nepředvídatelná událost	Nepravděpodobná událost, kterou nelze identifikovat na základě provedené analýzy rizik na stanovené hladině věrohodnosti.	Unforeseen Event
Iniciační událost	Událost, která odstartuje pohromu / řetězec propojených škodlivých jevů.	Initiating Event Trigger Event
Očekávaná událost	Očekávaná událost je událost, jejíž výskyt je očekáván v určitém časovém intervalu na základě provedené analýzy rizik na stanovené hladině věrohodnosti.	Expected Event Anticipated Event
Mimořádná událost	Je škodlivé působení sil a jevů vyvolaných čin-	Extraordinary Event

	ností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací. Pozn.: Pojem zavedený zákonem č. 239/2000 Sb.	
Krizová situace	Je kritická situace, při které je vyhlášen krizový stav (stav nebezpečí, nouzový stav, stav ohrožení státu, válečný stav) k tomu, aby k odezvě bylo možno též aplikovat nadstandardní opatření, zdroje, síly a prostředky. Pozn. 1: Dle § 2 zákona č. 240/2000 Sb. je to mimořádná událost, při níž je vyhlášen stav nebezpečí nebo nouzový stav nebo stav ohrožení státu. Pozn. 2: Krizová situace se vyhlašuje dle odst. 1 § 3 zákona č. 240/2000 Sb.	Crisis Situation
Bezpečný prostor	Bezpečný prostor je prostor, ve kterém je bezpečí na přijatelné úrovni. Pozn. 1: Bezpečím se zpravidla rozumí nejen bezpečí chráněných aktiv, ale i přijatelná úroveň potenciálu jejich udržitelného rozvoje. Pozn. 2: Pod heslem „Evropa - bezpečný prostor“ EU odstartovala v březnu 2004 po událostech v Madridu specifický výzkum zaměřený na bezpečnou Evropu. Pozn. 3: Současná aktivita EU se soustřeďuje především na bezpečí lidí v Evropě.	Safety Space
Pro-aktivní řízení	Pro-aktivní řízení je typ řízení, ve kterém provádíme předem antropogenní opatření a činnosti na odvrácení či alespoň zmírnění některých nežádoucích jevů a zajišťujeme připravenost na zvládnutí očekávaných nežádoucích jevů.	Proactive Management
Reaktivní řízení	Reaktivní řízení je typ řízení, ve kterém řešíme problémy, až když nastanou.	Reactive Management
Indikátor bezpečnosti	Indikátor bezpečnosti je veličina, která je mírou úrovně bezpečnosti v daném podsystému / systému. Obvykle se používají dva typy indikátorů bezpečnosti: - průběžné jako míra trendu bezpečnosti v čase, - cílové jako míra změny bezpečnosti po aplikaci opatření a činností za účelem zvýšení bezpečnosti.	Safety Performance Indicator
Odolnost	Schopnost systému zvládnout dopady dané pohromy, které nepřekročí jistou mez.	Resistance
Pružná odolnost Pružnost	Schopnost systému zvládnout dopady dané pohromy, jejíž velikost působí dopady o velikostech, které jsou kolem meze odolnosti systému.	Resilience

Houževnatost		
Adaptabilita Schopnost adaptace	Schopnost systému zvládnout dopady dané pohromy určitým přizpůsobením, kterým se nezmění vlastnosti systému.	Adaption Capability
Funkčnost	Schopnost systému plnit dané úkoly přesně dle zadání.	Functionality
Spolehlivost	Schopnost systému bezchybně dodržovat stanovené požadavky po stanovenou dobu.	Reliability Dependability Credibility
Limity a podmínky	Limity a podmínky jsou nástroje pro řízení bezpečnosti technologických zařízení. Jejich dodržování zaručuje bezpečný provoz technologického zařízení nebo infrastruktury. Jsou souborem jednoznačně definovaných podmínek, pro které je prokázáno, že provoz technologického zařízení či infrastruktury je bezpečný. Předmětný soubor tvoří údaje o přípustných parametrech, požadavcích na provozuschopnost zařízení, nastavení ochranných systémů, požadavcích na činnost pracovníků a na organizační opatření ke splnění všech definovaných podmínek pro projektované provozní stavy.	Limits and Conditions
Princip předběžné opatrnosti	Princip předběžné opatrnosti je princip, který ukládá v případě nejistých nebo neurčitých dopadů připravovaného rozhodnutí na budoucí vývoj lidského systému toto rozhodnutí neprovést z důvodu neschopnosti zajistit bezpečí nebo ho rozložit na soubor dílčích rozhodnutí, jejichž rizika se hodnotí a důkladně monitorují (tj. proces se i koriguje, když je to třeba s ohledem na velikost rizika).	Precautionary Principle
Průkaz odolnosti / schopnosti	Průkaz odolnosti tvoří soubor výpočtů, testů, analogií, úsudků, kterými lze s jistou spolehlivostí stanovit, že sledované zařízení či jeho části jsou odolné až do stanovené (specifikované) úrovně pohromy. U běžných technických zařízení a objektů se prokazuje odolnost na stoleté pohromy. U důležitých mostů, přehrad pro tisícileté pohromy a pro běžná jaderná zařízení na deseti tisícileté pohromy (pozn. úložiště aktivního plutonia vyžadují prokázání odolnosti na sto tisíciletou pohromu).	Resistance / Capability Demonstration
Hodnocení techniky	Hodnocení techniky je hodnocení, které posuzuje přínos dané technologie pro společnost podle skórování jejích dopadů a užitků na základě kritérií ze všech oblastí života společnosti (technické, ekologické, sociální, společenské, ekonomické, právní).	Technology Assessment
Domino efekt	Proces, ve kterém nehoda u jedné instalace nebo zařízení nebo předmětu vede ke vzniku ná-	Domino Effect

	sledných nehod u sousední instalace nebo zařízení nebo předmětu, čímž je vyvoláno stupňování dopadů nehody v území.	
Analýza příčin a dopadů	Metoda pro vyjádření možných závěrů, které vznikají z logické kombinace zvolených vstupních událostí nebo stavů.	Cause - Consequence Analysis – CCA
Analýza citlivosti	Zkoušky provedené k odhadu různých výsledků stanovení ohrožení nebo nebezpečnosti k možným předpokládaným nejistotám.	Sensitivity Analysis
Analýza systému pomocí kontrolního seznamu	Analýza stavu systému a shody bezpečnostní dokumentace s požadavky legislativy pomocí předem připravených seznamů jednotlivých položek nebo kroků. Výsledkem je doplněný kontrolní seznam odpovědí obecně „ano“ nebo „ne“.	Check List System Analysis
Analýza systému pomocí stromu poruch	Deduktivní metoda, která zpětně analyzuje rozvoj nežádoucího jevu (živelní pohromy, havárie, útoku apod.) pro nalezení řetězu příčin, které mohly vést k havárii či selhání entity. Výsledkem je grafický logický model, který zobrazuje různé kombinace poruch zařízení a lidských chyb, které mohou vyústit ve vrcholovou danou událost. Metoda je použitelná pro identifikaci zdrojů rizika (tj. pohrom všeho druhu a místních zranitelností) a pro oceňování četností iniciačních událostí a pravděpodobností koncových stavů (scénářů). Metoda zobrazuje a hodnotí kombinace různých stavů systému, které vedou ke konkrétnímu závěru (cílová událost).	Fault Tree System Analysis – FTA
Analýza režimů a dopadů poruchy	Proces k identifikaci rizika, ve kterém jsou opakovaně uvažovány všechny známé režimy, poruchy, součásti nebo znaky systému a nežádoucí výsledky jsou zaznamenávány.	Failure Modes and Effect Analysis – FMEA
Analýza režimů a dopadů poruchy a analýza kritičnosti	Proces, ve kterém je uvažována možnost řady poruch a závažnost jejich dopadů k identifikaci nejkritičtějších prvků, funkcí, procesů, jevů nebo znaků.	Failure Modes, Effects and Criticality Analysis – FMECA
Analýza systému pomocí stromu událostí	Induktivní metoda, která ze základní iniciační události (živelní pohroma, porucha zařízení, lidská chyba, útok) konstruuje rozvoj události do možného koncového stavu na základě možnosti „příznivá – nepříznivá“ včetně uvážení odezvy bezpečnostních systémů a operátorů na iniciační událost. Výsledkem jsou scénáře nehody graficky znázorněné pomocí stromu událostí, tj. soubor poruch nebo chyb vedoucích k nehodě. Metoda je vhodná pro analýzu složitých procesů. Metoda ilustruje a hodnotí bezprostřední a konečné výsledky, které mohou vzniknout po výskytu zvolené počáteční události.	Event Tree System Analysis – ETA
Analýza rizika	Metodický nástroj pro zjištění a ocenění rizik.	Risk Analysis
Analýza skutečných	Účetní metoda hodnocení nákladů na odstranění	Cost Benefit Analy-

nákladů a užitků	škod proti nákladům na užitečně vynaložené činnosti spojené se zmírněním dopadů. V oblasti velkých rizik se provádí jako podpora k rozhodnutí, zda je nebo není nutno pokračovat ve snižování zranitelností či jiném zmírňování rizika.	sis
Analýza spolehlivosti	Analýza napomáhající určení spolehlivosti technologických celků nebo systému člověk / stroj.	Reliability Analysis
Kvantitativní analýza rizika procesů	Komplex metod používaný v logickém procesu hodnocení rizika, stanovení míry rizika, která je výsledkem sumarizace rizik všech vybraných poruch. Řešení probíhá po etapách a směřuje k ocenění dopadů a pravděpodobností všech koncových stavů scénářů vybraných poruch. Zároveň obsahuje návrhy ke snížení rizik. Pro kvantifikaci dopadů se používá modelování fyzikálně chemických procesů a jevů (úniky, rozptyly, požáry, výbuchy, zranitelnost příjemce rizika – modely dávek a odezvy: koncentrace, probit funkce, tepelná radiace, přetlak).	Process Risk Quantitative Analysis – PQRA
Analýza lidské spolehlivosti	Samostatná oblast analýzy rizika obsahující kvalitativní i kvantitativní stránku. Do identifikace a hodnocení rizik je zahrnut lidský činitel. Provádí se hodnocení možných lidských chyb, jejich příčin a dopadů. Součástí je identifikace důležitých míst systému, která mohou být lidskými chybami ovlivněna. Obvykle se používá ve spojení s jinými metodami.	Human Reliability Analysis – HRA
Kvantitativní stanovení rizika	Kvantitativní hodnocení pravděpodobnosti vzniku nežádoucích událostí a pravděpodobnosti škody nebo poškození. Pravděpodobnost může být vyjádřena jako pravděpodobnost nebo četnost.	Quantitative Risk Assessment – QRA
Metody kvalitativního hodnocení	Hodnotící postupy, které nevedou k numerickým výsledkům.	Qualitative Assessment Methods
Metody kvantitativního hodnocení	Hodnotící postupy, které vedou k numerickým výsledkům.	Quantitative Assessment Methods
Předběžná analýza ohrožení	Metoda určená pro používání v předběžné fázi vývoje technologického zařízení. Používá se v případech, kdy předcházející zkušenosti poskytují nepatrný nebo žádný pohled na jakékoliv možné bezpečnostní problémy, např. u nového zařízení s novými postupy. Cílem je včasná identifikace ohrožení, aby mohl být konstruktérům poskytnut návod při závěrečné etapě konstrukce zařízení.	Preliminary Hazard Analysis – PHA
Analýza ohrožení a provozuschopnosti	Metoda pro identifikaci ohrožení, tj. zdrojů rizika a provozních problémů metodickou identifikací procesních odchylek technologických systémů a prvků pomocí tzv. klíčových slov aplikovaných na jednotlivé body nebo studijní uzly v procesních schématech. Výsledkem je tabulka, ve které jsou identifiková-	Hazard and Operability Analysis – HAZOP

	na ohrožení, tj. zdroje rizika, provozní problémy a doporučení pro zlepšení daného stavu. Studie prováděná aplikací nebo průvodními rozhovory k identifikaci všech odchylek od konstrukce se zřetelem k nežádoucím dopadům.	
Metoda PSA	Metoda řízení bezpečnosti založená na posouzení příspěvku zranitelností jednotlivých komponent k celkové zranitelnosti systému.	Probabilistic Safety Assessment – PSA
Relativní klasifikace	Klasifikace procesů dle vybraných kritérií.	Relative Ranking – RR
Určení nebezpečnosti látky	Určení nebezpečnosti látky znamená posouzení nebezpečných vlastností látky pomocí stanovených nebo věrohodných údajů z odborné literatury.	Substance Danger Identification
ALARA / ALARP*)	ALARA je princip, který stanovuje zásadu, že z možných hodnot dopadů pohromy je pro společnost přijatelná ta malá hodnota, kterou lze dosáhnout aplikací rozumných zmírňujících technických opatření. (Pozn. – někdy se v odborné literatuře vyskytuje také zkratka ALARP je princip používaný při skórování rizik.	ALARA (as low as reasonably achievable) ALARP (as low as reasonably possible)

*) ***ALARP*** princip vyjadřuje, že riziko by mělo být redukováno na velikost, která je prakticky dosažitelná. To znamená, že by neměly být zvažovány náklady na opatření, kterými se redukce rizika provede. ALARP zdůrazňuje princip předběžné opatrnosti, který je základním principem řízení bezpečnosti s ohledem na obezřetnost. Podle odborníků by princip měl být používán v každé fázi technického díla, od přípravy až do ukončení provozu.

Jelikož v České republice i ve Slovenské republice mají velkou vážnost integrované záchranné systémy, tabulka 4 uvádí hlavní odlišnosti mezi pojmy uvedenými v tabulce 3 a pojmy, které obsahuje legislativa pro Integrovaný záchranný systém.

Tabulka 4. Porovnání pojmů v inženýrských oborech zacílených na celý cyklus budování bezpečnosti entity a v oboru odezvy, prováděné Integrovaným záchranným systémem.

Obsah pojmu	**Pojem používaný v řízení bezpečnosti a anglický ekvivalent**	**Pojem používaný při záchranných a likvidačních pracích v ČR a SR + anglický ekvivalent**
Jev, který vede nebo může vést k újmě a značné škodě na chráněných zájmech. Má věcnou podstatu a je zdrojem rizik pro chráněná aktiva.	Pohroma (anglicky Disaster) *Česká legislativa:* živelní či jiná pohroma	Mimořádná událost (anglicky Extraordinary Event)
Stav, který je vyvolán v území / objektu apod. při výskytu pohromy.	Nouzová situace (anglicky Emergency)	Mimořádná událost (anglicky Extraordinary Event)

Situace v území či v lidské společnosti vyvolaná výskytem pohromy (živelní či jiné pohromy), která v daném území za určený časový interval (není-li stanoveno jinak, tak 100 let) má nebo může mít nepřijatelné dopady takové intenzity nebo rozsahu, které vedou k destabilizaci území a společnosti. Tj. situace je vyvolaná výskytem tzv. nadprojektové pohromy (nadprojektové živelní či jiné pohromy), proti níž nejsou systematicky v územním plánování a v řízení bezpečnosti chráněných zájmů prováděna adekvátní ochranná opatření, nebo jde o případ, při kterém se při odezvě na pohromu provedly závažné chyby, anebo došlo ke kombinaci neočekávaných okolností.	Kritická situace (anglicky Critical Situation)	Mimořádná událost (anglicky Extraordinary Event)
Situace, pro jejíž zvládnutí nestačí běžná opatření prováděná správními úřady a bezpečnostními složkami a je třeba použít nadstandardní zdroje, síly a prostředky ke zvládnutí situace. Je nutno aplikovat právní opatření, tj. vyhlásit krizový stav.	Krizová situace (anglicky Crisis Situation)	Krizová situace (anglicky Crisis Situation)
Plánování, organizování, přidělování pracovních úkolů a kontrola zdrojů organizace tak, aby byly minimalizovány ztráty, škody, újmy, zranění nebo úmrtí vyvolané různými pohromami (živelními či jinými pohromami), jejichž výskyt je pravděpodobný (tj. pravděpodobnost výskytu ve specifikovaném časovém intervalu je větší nebo rovna 0.05).	Řízení rizika (anglicky Risk Management)	Není předmětem
Řízení, které spočívá v plánování, organizování, přidělování pracovních úkolů a v kontrole využívání zdrojů organizace s cílem dosáhnout požadované úrovně bezpečnosti a zahrnuje princip předběžné opatrnosti, tj. dělá systematicky opatření i proti pohromám (živelním či jiným pohromám) a jejich dopadům, jejichž výskyt je velmi málo pravděpodobný, tj. pravděpodobnost výskytu ve specifikovaném časovém intervalu je menší než 0.05.	Řízení bezpečnosti (anglicky Safety Management)	Není předmětem
Řízení bezpečnosti a rozvoje území s ohledem na danou pohromu.	Řízení pohrom (anglicky Disaster Management)	Není předmětem
Řízení, které spočívá v plánování, organizování, přidělování pracovních úkolů a v kontrole využívání zdrojů organizace s cílem zvládnout možné kritické situace, při kterých bude vyhlášena krizový stav s cílem zajistit zvládnutí situace v rámci působnosti orgánu krizového řízení a plnění opatření a úkolů uložených vyššími orgány krizového řízení. Používá dočasné omezení práv lidí a použití nadstandardní zdrojů, sil a prostředků.	Krizové řízení (anglicky Crisis Management)	Krizové řízení (anglicky Crisis Management)

Plán pro zajištění bezpečného území a udržitelného rozvoje území a lidské společnosti.	Územní plán (anglicky Land-use Plan)	Není předmětem
Plán odezvy na nouzové situace, který obsahuje soubor antropogenních opatření a činností pro zmírnění dopadů pohrom (živelních či jiných pohrom), kterým nelze zabránit a opatření nutná pro zvládnutí nouzových situací, která vedou k zajištění stabilizace situace a umožní obnovu a další rozvoj území. Je založen na použití standardních zdrojů, sil a prostředků správních úřadů a bezpečnostních složek.	Nouzový plán (anglicky Emergency Plan)	Havarijní plán (anglicky Accident Plan) Povodňový plán (anglicky Flood Response Plan) Plán pro stav nouze v zásobování elektřinou, ropou, vodou apod. / (anglicky Emergency Plan for Supply of Energy, Oil, Water etc. OR Plan for Emergency Supply of Energy, Oil, Water etc.) Traumatologický plán (anglicky Response Plan to Trauma) *Tj. používají se dílčí názvy plánů a ne integrální název.*
Plán odezvy na krizové situace, který obsahuje soubor antropogenních opatření a činností pro zmírnění dopadů pohrom (živelních či jiných pohrom), kterým nelze zabránit a opatření nutná pro zvládnutí kritických situací, která vedou k zajištění stabilizace situace a umožní obnovu a další rozvoj území. Je založen na použití standardních a nadstandardních zdrojů, sil a prostředků správních úřadů a bezpečnostních složek.	Krizový plán (anglicky Crisis Response Plan OR Response Plan to Crisis)	Krizový plán (anglicky Crisis Plan)

Na závěr je vhodné zopakovat, že pojmy pro ***inženýrství, které pracuje s riziky a je zacílené na bezpečný svět,*** tvoří nadstavbu pojmů v technických vědách, sociálních vědách a environmentalistice. Jsou založeny na konceptu, jehož cílem je zajištění koexistence základních systémů, které člověk potřebuje ke svému životu a rozvoji, tj. systému životního prostředí, sociálního systému a technologického systému. Předmětná koncepce je nadčasová a je založená na komplexním přístupu, který však není možný bez generalizace.

Z pohledu potřeb praxe je vždy důležité si ujasnit pojmy; vztahy mezi pojmy a cíle, které chceme aplikací pojmů dosáhnout. V případě sledovaném v předložené publi-

kaci je cílem zajištění bezpečných technických děl a jejich bezpečného okolí, což vytváří jeden ze základních pilířů, které jsou nutné pro bezpečí a rozvoj lidí.

3. ZDROJE RIZIK A BEZPEČNOST TECHNICKÝCH DĚL

Historie odhadu rizika je velmi dlouhá a srovnatelná s historií bankovnictví a pojišťovnictví. Např. bez znalosti rizika nelze pojišťovat, nelze poskytovat úvěry, bankovní záruky a jiné finanční služby. Pro posuzování rizik byl vyvinut bezpočet pomocných pracovních pomůcek, metodických návodů, uživatelských příruček a software. Jejich struktura je značně diferencována vertikálně a horizontálně, a proto vyčerpávající klasifikace je obtížná. Přehled a posouzení validity často používaných postupů v inženýrských disciplínách budou v další kapitole.

V úvodu bylo uvedeno, že práce s riziky v souvislosti s technickými díly není akademickou záležitostí. Jejím cílem je vytvářet a provozovat technické dílo, které neohrožuje ani sebe, ani své okolí ani za podmínek kritických, se kterými je třeba počítat dnes i v budoucnu, protože svět se dynamicky vyvíjí. Protože technické dílo není osamocené, ale je v určitém území, je třeba zajistit koexistenci technického díla a území po celou dobu existence technického díla, a proto ve všech úvahách o bezpečnosti musí být zvažováno nejen technické dílo, ale i jeho okolí.

3.1. Příčiny rizik technických děl

Každé technické dílo chápeme jako otevřený složitý systém systémů, tj. jako několik otevřených systémů, které se vzájemně prolínají, a jsou propojené s okolím [3,4,17]. Propojení způsobují závislosti, které jsou příčinami specifických zranitelností [17]. Kromě žádoucích propojení vznikají za jistých podmínek i propojení nežádoucí, která vedou k selhání technických děl, která za jistých okolností výrazně poškozují technické dílo i jeho okolí. Proto je třeba technická díla chápat jako otevřené systémy systémů, které mají rozmanitá aktiva a která se v dynamicky proměnném světě mění [3,4,17]. Rozmanitost aktiv způsobuje, že za jistých podmínek jsou požadavky na opatření, která zajišťují bezpečnost jednotlivých aktiv, konfliktní, což znamená, že metody používané k řízení rizik zacílené na bezpečnost technických děl musí být multikriteriální [1-4,17].

Svět se dynamicky vyvíjí, tj. probíhají v něm rozmanité procesy, které jsou mimo jiné i příčinou rizik v lidském systému, tj. území i v technických dílech, které vedou ke škodlivým jevům / pohromám (které zahrnují i havárie a selháním technických systémů) [1]. Cílem lidského snažení je bezpečná lidská společnost, bezpečná komunita, bezpečné území, bezpečná technická díla atd., podrobnosti jsou např. v publikacích [1,5,40]. Všechny sledované systémy jsou složité, a proto je nahrazujeme modely umístěnými do jistého modelu prostředí (okolí systému), které mají určitou hladinu podrobnosti, a tím i jisté meze platnosti; v technické praxi se používá pojem limity a podmínky. Je si třeba proto uvědomit, že mimo těchto mezí jsou závěry získané aplikací použitých modelů neoprávněné a mohou způsobit chybná rozhodnutí vedoucí k iniciaci pohrom či celých řetězců pohrom (v daných souvislostech často mluvíme o organizačních haváriích [3]).

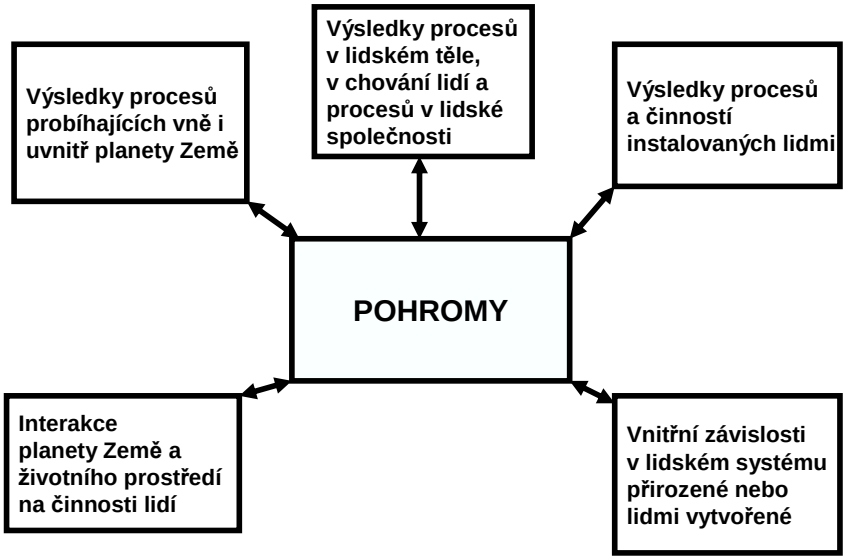
Každé technické dílo je umístěno v území, které je postihováno jistými pohromami, tj. leží v něm zdroje rizik. Jde o vnější zdroje rizik a kromě nich jsou vnitřní zdroje rizik spojené s existencí a provozem technického díla a zdroje rizik spojené s interakcemi technického díla a jeho okolí. V dalších odstavcích je uveden přehled zdrojů rizik a

odkazy na literaturu, ve které jsou pohromy, tj. zdroje rizik sledovány podrobně. Speciální pozornost je věnována zdrojům rizik, jejichž původcem je člověk a jejichž důsledkem jsou tzv. organizační havárie.

Další specifické nové zdroje rizik přináší pokračující robotizace. Zdroje rizik vznikají hlavně na rozhraních: stroj – IT; IT – IT; člověk – IT; např. články v publikaci [34]. V práci [57] je ukázáno, že původcem zdrojů rizik při aplikaci kybernetických technologií je z 84% člověk, jejich tvůrce. Z citované práce vyplývá, že v dané oblasti je podstatné zajistit důvěrnost, integritu a dostupnost kybernetických technologií, když jsou k činnosti technického díla potřeba. Při zajištění uvedených požadavků dochází ke konfliktu mezi bezpečím a soukromím člověka. V zájmu lidské existence a lidského bezpečí je třeba najít rovnováhu. K tomu je nutné pochopit procesy, rozumět předmětné technologii a také rozumět lidem.

3.1.1. Procesy vyvolávající jevy, jež jsou zdroji rizik

Lidem i dalším veřejným aktivům působí ztráty a škody jevy, pro které česká legislativa od r. 1811 používá pojem „pohromy“. Výčet pohrom [1,3,18] ukazuje, že pohromy dle procesu, jehož jsou produktem, mají velmi různou fyzikální, chemickou, ekonomickou, biologickou, sociální či kybernetickou podstatu. Právě tento fakt je rozhodující z hlediska bezpečnosti, protože preventivní opatření musí být zaměřena na povahu pohromy, aby byla účinná [3]. Obrázek 1 ukazuje základní rozdělení zdrojů pohrom podle procesů, které je vyvolávají.



Obr. 1. Zdroje pohrom.

Vlastnosti a charakteristiky pohrom jsou uvedené např. v publikacích [18,58]. Dále se soustředíme na pohromy, jejichž příčiny jsou vnitřní jevy technických děl a technologií, leží v propojení technických děl a jejich okolí a v lidské činnosti.

3.1.2. Havárie technických děl

Havárie technických děl, označované v odborné literatuře jako technologické pohromy, zahrnují poruchy, selhání zařízení, selhání systémů, nehody a havárie. Jde o

průmyslové havárie, havárie při přepravě a skladování nebezpečných látek, dopravní nehody a o jiné jevy, které narušují stabilitu a soudržnost území v důsledku technologií provozovaných člověkem. V praxi speciálně sledujeme:

- průmyslové havárie,
- radiační havárie,
- havárie při přepravě či skladování nebezpečných látek,
- dopravní nehody,
- porušení stability podloží vlivem vibrací, které při činnosti vyvolávají stroje a dopravní prostředky.

Předmětné pohromy jsou výsledky procesů a činností instalovaných lidmi, a proto člověk korekcí svých činností má jistý potenciál ovlivnit jejich výskyt, průběh a četnost výskytu.

Průmyslová havárie je havárie spojená s destrukcí nebo selháním průmyslového komplexu, při nichž dojde k uvolnění nebezpečných látek, požáru, vzniku tlakové vlny a rozletu úlomků. Speciálně se pak sledují chemické a radiační havárie [18].

Havárie při přepravě či skladování nebezpečných látek je výskyt jevu, který je spojen s vlastností nebezpečných látek a který nastane při přepravě či skladování nebezpečných látek a má dopady na životy a zdraví lidí, majetek a životní prostředí.

Dopravní nehoda je výskyt jevu při dopravě, který má dopady na životy a zdraví lidí, majetek a životní prostředí.

Porušení stability podloží vlivem vibrací je narušení soudržnosti podložních vrstev vlivem dlouhodobého působení vibrací, které jsou vyvolány technologickými zařízeními (např. kompresory, buchary používané při těžbě ropy), anebo častými komorovými odstřely používanými jako součást technologie těžby nerostů.

Chemické havárie mají v Evropě vysokou pravděpodobnost výskytu a velikost jejich dopadů může být značná. Příčiny nebezpečí v hlavních technologických zařízeních jsou početné a rozmanité. Průmyslové komplexy se často nacházejí v blízkosti obytných celků. Sekvence událostí vedoucích k havárii může být velmi rychlá a záchranné složky nemají čas na svou organizaci. Nebezpečné látky se rychle uvolňují a okamžitě ohrožují. Je obtížné detekovat a analyzovat uvolněné substance a posoudit jejich dopady. Proto např. záchranné útvary (v České republice Integrovaný záchranný systém) jsou aktivovány i v případě, když podnik má své vlastní záchranné služby. Na velkém území je vysoké nebezpečí otravy lidí a zvířectva, znečištění vod a půdy. Úroda může být zničena a v extrémních případech může být postižené území na určitý čas vyhlášeno jako “zakázaná zóna” [18].

Riziko spojené s haváriemi technických děl je charakterizováno souborem dopadů, které vyvolá samotná havárie a pravděpodobností výskytu samotné havárie. V technické praxi odráží stupeň integrity bezpečnosti vložené do projektu technického díla a kvalitu provozního výkonu technického díla. Jeho míra určená jeho pravděpodobností (četností) výskytu je sice v denním životě méně známá, je však životně důležitá pro technická díla, protože vzbuzuje důvěru ve vysokou integritu bezpečnosti a dobrou provozní praxi [3,4].

Riziko technických děl se obvykle vyjadřuje pomocí očekávaných ztrát za určitou dobu, a to v oblasti úmrtí zaměstnanců a ekonomických ztrát; ve větší šíři pak zahrnuje úmrtí a zranění lidí i ekonomické ztráty v okolí technického díla, újmy na životním prostředí a finanční ztráty veřejné správy a ostatních technických děl v okolí, které byla postižena havárií [3,4].

3.1.3. Selhání obslužnosti technických děl a infrastruktur

Technologie a infrastruktury zajišťují výrobky a služby pro kvalitní lidský život, umožňují ochranu i přežití lidí při kritických situacích. Proto je z hlediska potřeb lidské společnosti nutné zabraňovat narušení provozu nebo selhání technických děl, anebo infrastruktur územních, ekonomických, informačních, komunikačních, společensko-organizačních a nouzových služeb. Jejich příčiny jsou: živelní pohromy; průmyslové havárie spojené s technologií – stárnutí materiálů, nedokonalá propojení mezi komponentami fyzická, územní, kybernetická a logická; sabotáže a teroristické útoky; a válka [11,17]. Předmětná selhání vedou ke ztrátě obslužností území, čímž lidé ztrácí základní potřeby k životu nebo je dostávají v nedostatečném množství. V praxi se sleduje selhání infrastruktur: ekonomických; územních; kybernetických; a v oblasti služeb, zásobování a spojení [10,16,19]. V praxi se zapomíná na infrastruktury vzdělávací, výzkumu a sociálních vztahů [16], které jsou důležité pro zajištění bezpečnosti technických děl.

Rizika a problémy spojené s ochranou technických děl jsou shrnuty v pracích: technická díla – objekty [3]; technická díla – objekty a infrastruktury [11,17,20]; selhání služeb [17]. Posledně jmenovaná publikace rovněž uvádí nedostatky v řízení pohrom z pohledu konceptu „bezpečná komunita“. Z prací [4,17] vyplývá, že se dosud nedostatečně zvažují zdroje rizik ovlivňující provoz technických děl, jakými jsou:

- selhání celé kritické infrastruktury nebo některé z dílčích infrastruktur kritické infrastruktury, anebo základních dodavatelských řetězců,
- nedostatečná kvalita podpory, dohledu a dozoru nad výstavbou a provozem technických děl ze strany státu,
- selhání vzdělávací infrastruktury a infrastruktury výzkumu, které zajišťují výstavbu a provoz technických děl,
- devastace a nehospodárné využívání přírodních zdrojů a surovin,
- nerespektování současného poznání (know-how).

3.1.4. Organizační havárie

Člověk je tvůrce i provozovatel, tj. řídící faktor, technických děl. Svým přístupem a činností proto zásadním způsobem ovlivňuje jejich chování a činnost. Příčiny havárií, které způsobil člověk lze v zásadě rozdělit do dvou skupin, a to: chybné úkony provedené úmyslně či neúmyslně; a tzv. organizační havárie. Lidský faktor jako původce havárií z první skupiny je sledován v pracích autorky [3,19]; a velmi podrobně v článcích uvedených v knihách [25-34].

Organizační havárie je pojem z dnešní technologické praxe. Znamená selhání řízení technického díla v neprospěch veřejného zájmu. K vymezení pojmu došlo v r. 1981 v rámci EU při zavádění směrnice Seveso I do praxe, při kterém byly na základě analýzy závažných havárií identifikovány příčiny závažných havárií. Jednou z oblastí příčin havárií se ukázaly přístupy používané v řízení, a to koncepce řízení a systémy řízení. Analýzy ukázaly, že selhání systému řízení přispělo k příčinám více než 85% nahlášených havárií. Výsledky navázaly na závěry důkladné analýzy havárie jaderné elektrárny Three Mile Islands [59].

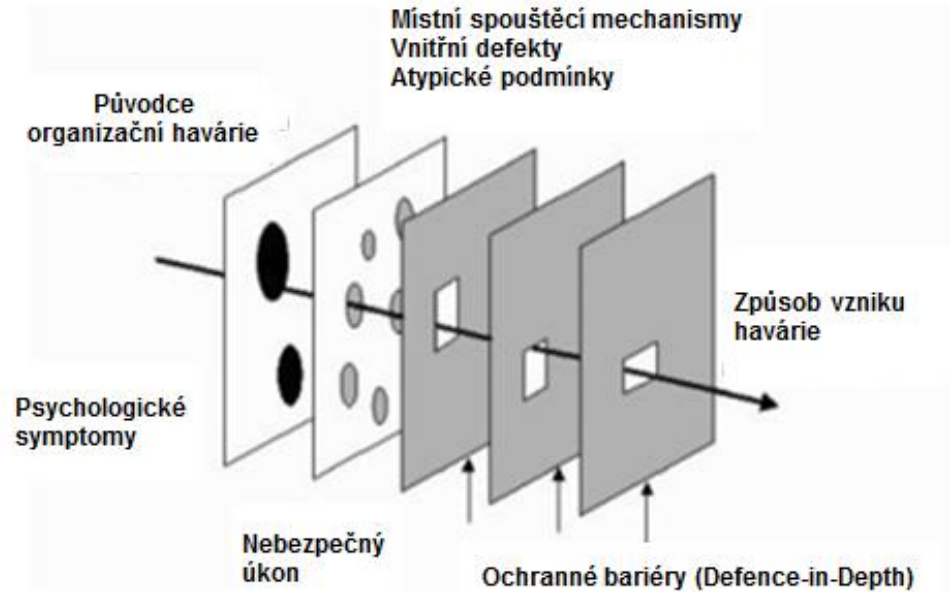
Jak již bylo řečeno, organizační havárie je havárie způsobená chybami člověka, tvůrce a provozovatele technického díla. Původem předmětných chyb jsou jak lidské neznalosti, tak dále uvedené praktiky spojené s řízením technického díla:

- přecenění vlastních rozhodnutí ze strany řídícího pracovníka,
- neznalosti a nezkušenosti řídícího pracovníka,

- neschopnost řídícího pracovníka zajistit včasné a správné předání zásadních informací,
- malá oprávnění (kompetence) řídícího pracovníka pro řešení problémů,
- podcenění závažnosti situace ze strany řídícího pracovníka,
- nerespektování zákonitostí přírodních, technických, ekonomických a sociálních při rozhodování řídícího pracovníka.

Model organizační havárie nazvaný Swiss Cheese byl navržen počátkem 90. let anglickým psychologem Jamese Reasonem jako referenční model pro etiologii a výzkum organizačních havárií ve výrobních systémech s cílem jim zabránit [60]. Jeho přínosem je, že ukazuje složitost reálných procesů a také způsob, jak latentní selhání (chyby) na řídící úrovni vedou za určitých podmínek k fatálním haváriím. Na jeho základě de facto byl postaven koncept ochrany do hloubky [48], o kterém bude pojednáno dále.

Obrázek 2 ukazuje logickou představu vzniku havárie, ke které došlo na základě vzniku procesu, který nastal, když došlo k propojení mezer v ochranných bariérách technického díla v důsledku nedostatků způsobených chybami v návrhu technického díla a v aktech jeho řízení.



Obr. 2. Model organizační havárie s vyznačení základních bariér, které mají zabránit havárii a jsou vytvářeny v rámci řízení bezpečnosti technického díla; zpracováno dle [60].

3.2. Fyzikální podstata průřezových rizik

Průřezová rizika jsou důsledkem propojitelností v systému, kterým je každé technické dílo (složitější jsou pak v systému systémů). ***Propojitelnost*** znamená závislost *mezi aspoň dvěma dílčími systémy. Prostřednictvím propojení se vytváří vazby či spřažení mezi prvky, v jejichž důsledku stav jednoho dílčího elementu či systému ovlivňuje nebo koreluje se stavem jiného dílčího elementu či systému.* Definici propojitelnosti lze ještě rozšířit o podmínku vzájemného sdílení některých fyzických prvků nebo procesů, přičemž prvky nebo procesy mohou být situovány i v různých územních oblas-

tech. Vzájemná závislost v technickém objektu i v území může být proto fyzická, kybernetická, logická a územní [11,17]. Přitom platí:

1. Dílčí elementy či systémy jsou fyzicky vzájemně závislé, jestliže stav jednoho z nich je závislý na materiálním výstupu dílčího elementu či systému druhého.
2. Kybernetická vzájemná závislost znamená, že stav jednoho dílčího elementu či systému závisí na informacích z jiného dílčího elementu či systému. Kybernetická vzájemná závislost předpokládá existenci informačního (dílčího) systému.
3. Dílčí elementy či systémy jsou územně vzájemně závislé, jestliže události v území mohou měnit stavy dílčích elementů či systémů (např., když sítě několika elementů či systémů jsou v jednom kabelovém koridoru).
4. Logická vzájemná závislost znamená, že stav jednoho dílčího elementu či systému závisí na stavu jiného dílčího elementu či systému, přičemž mechanismus propojení není fyzický, kybernetický nebo územní. Jedná se o závislosti přenášené přes toky, kterými jsou předpisy, finance, legislativa apod., např. se může jednat o finanční trhy.

V důsledku vzájemné závislosti porucha či selhání jednoho dílčího systému způsobí poruchu či selhání dílčího systému druhého. Uvedený fakt přispívá ke kritičnosti SoS v objektu / území / státu. Proto nestačí zajišťovat bezpečnost dílčích systémů odděleně, ale je třeba zajišťovat bezpečnost celých SoS, což v praxi znamená hledat řešení problému ***BEZPEČNOST SYSTÉMU SYSTÉMŮ***

3.2.1. Zranitelnosti technických děl vyvolané vzájemnými závislostmi

Systémy systémů mají specifické vlastnosti jako nelinearitu, různé ustálené stavy (atraktory), katastrofické chování, chaotické chování atd., které jsou příčinou průřezových rizik, které narušují bezpečí sledovaného systému systémů i bezpečí okolí systému systémů [11]. Abychom mohli zajistit bezpečné systémy systémů a jejich bezpečné okolí, tak musíme umět vyjednávat s průřezovými riziky, tj. identifikovat je a vhodným způsobem je řídit.

Pro řízení rizik systému systémů platí základní poznání z oblasti řízení rizik [2], tj. nestačí znát velikost rizika, ale je třeba znát jeho konkrétní příčiny, jejich lokalizace v řízeném systému a konkrétní zranitelnosti aktiv v předmětné alokaci. Pro identifikaci, analýzu a hodnocení klasických rizik existuje řada metod, nástrojů a technik. Neznámou jsou nástroje, metody a techniky pro identifikaci, analýzu a řízení průřezových rizik [2,9].

Na základě poznatků shromážděných v [3] v konceptech řízení SoS zvažujeme dva případy, a to realizace rizika probíhá stále stejným způsobem nebo významně odlišnými způsoby. V prvním případě z důvodu bezpečnosti buď zvažujeme nejméně příznivý případ (uvedený přístup nacházíme v normách a standardech založených na deterministickém přístupu pro zajištění bezpečnosti jaderných zařízení) nebo připouštíme náhodné nejistoty, které jsou důsledkem momentálních místních a časových podmínek aktiv a jako reprezentativní veličinu pro řízení rizika používáme střední hodnotu získanou vyhodnocením variant (aritmetický průměr, medián, medián + σ, kde σ je standardní odchylka, pravděpodobnou střední hodnotu). Druhý postup se dnes běžně zvažuje při přípravě podkladů pro strategické řízení (určují se variantní scénáře realizace rizika a pravděpodobnosti jejich výskytu; z nich se jasným ma-

tematickým přístupem určuje střední hodnota a její rozptyl); nacházíme ho v normách a standardech založených na pravděpodobnostním přístupu.

3.2.2. Náhodné a znalostní nejistoty

Na základě poznání z posledních desetiletí [2-4] je nutné při realizaci rizik zvažovat, že kromě náhodných nejistot existují ještě znalostní (epistemické) nejistoty, tj. neurčitosti v datech. Náhodné nejistoty lze ocenit pomocí metod matematické statistiky, když je dostatek dat. Pojem neurčitost je používán ve fyzice od 30. let minulého století [2]. Přiznáním existence neurčitostí de facto připouštíme možnost výskytu významných změn v procesu realizace rizika, které přesahují dopady výskytu jen nahodilých změn.

V posledních letech se proto do praxe pro modelování bezpečnosti a spolehlivosti systematicky začaly zavádět postupy teorie možností, tj. Dempster - Shaferovy teorie [61,62], která vychází z předpokladu, že disponibilní data a naše znalosti mají neurčitosti, tj. obsahují kromě náhodné nejistoty i vědomostní (epistemickou) nejistotu. Pomocí uvedené teorie se modelují varianty odpovídající různým procesům, které jsou možné kvůli vědomostním nedostatkům. Z nich se pak určuje rozmezí, ve kterém jsou očekávané možné varianty. Při výběru variant se používají experti a kombinují se výpočty s praktikami dobré praxe. Praxe ukázala, že nestačí jeden expert, ale je třeba kombinovat znalosti několika expertů. Kombinaci lze zajistit pomocí analytických metod nebo heuristik, např. DELPHI, panelová diskuse [2,9].

Při řízení rizika se odlišuje tolerance a přijatelnost rizika. Při řízení bezpečnosti se nepřipouští tolerovatelné riziko tak, kde jde o životy a zdraví lidí. Při řízení průmyslových rizik je nutno vycházet z předpokladu, že riziko může být redukováno jen do určité míry. Používá se úroveň, která je tak nízká, jak je to prakticky dosažitelné (princip ALARP – As Low As Reasonably Practicable). Aby takto stanovená úroveň zajistila bezpečí a udržitelný rozvoj lidského systému, tak stát, zastoupený veřejnou správou, musí být tak silný, aby zabránil prosazování partikulárních zájmů.

3.3. Riziko a bezpečnost technických děl a jejich okolí

Bezpečnost je dnes v odborných dokumentech a pracích chápaná jako vlastnost celého systému, ne jako vlastnost dílčích částí. U technických děl ji vytváří člověk (tvůrce) svými opatřeními a činnostmi [3-5,31,33,40,43,44,47,54].

Na základě současného poznání riziko a bezpečnost jsou v určitém vztahu, ale nejsou komplementárními veličinami [3,4,17]. Bezpečnost technických děl se zajišťuje cíleným řízením rizik, a to podobně jako spolehlivost, anebo další cíle, kterými je např. zabezpečené technické dílo nebo odolné technické dílo. Rozdíly ve jmenovaných typech řízení jsou vysvětleny v pracích [3,4]. Jelikož řízení bezpečnosti se vztahuje k celému technickému dílu a zahrnuje předběžnou opatrnost, je v současné době upřednostněno [2-4] ve vyspělých zemích i předpisech organizací jako je OECD, IAEA, COMAH aj. [2-4,25-34,40,43,44,47-50,54].

Lidské přání je řídit rizika tak, aby se nerealizovala. Na základě lidského poznání je to možné jen tehdy, když je pochopíme. Velmi důležité je pochopit velké dopady pohrom, které mají velmi nízkou pravděpodobnost výskytu. Vysoce důležité je

v každém systému určit kritická místa a umět klasifikovat znalostní nejistoty, které jsou ve vstupních datech, použitých modelech a hlavně v tom, že reálné systémy jsou složité [3,4].

Podle poznání a zkušeností shrnutých v pracích [1-4,58] pro práci s riziky zacílenou na bezpečnost musí být v každém technickém díle:

- stanovena chráněná aktiva (jde o prioritní či kritické položky, na nichž závisí provoz technického díla) obrázek 3,
- hierarchie pojmů, které jsou důležité pro zajištění bezpečných technických děl i lidí [43,44,47,54],
- stanoveny zdroje rizik a jejich dopady na chráněná aktiva,
- používány validované metody pro analýzu, hodnocení a posuzování rizik,
- používány správné způsoby řízení rizik zacílené na bezpečnost technického díla,
- používány správné způsoby inženýrského vypořádání rizik [58],
- aplikovány správné způsoby práce s riziky v čase.

Obr. 3. Položky důležité pro bezpečné technické dílo.

Jak již bylo řečeno v úvodu, rizik existuje velké množství [1,2,16,18,22] a stále přibývají. Proto je třeba v řízení technických děl správně aplikovat antropogenní opatření a činnosti a mít jasně stanoven cíl, kterým je z pohledu lidí bezpečný lidský systém. Aby řízení rizik bylo úspěšné, tak se musí zaměřit na prioritní rizika a jejich aspekty [3]. Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá v rozdělení vypořádání rizik do kategorií [2], jak bylo řečeno již v úvodu.

V reálné inženýrské praxi zacílené na zajištění bezpečných technických děl je třeba oddělit dvě základní činnosti, které jejich tvůrci musí provést. V rámci první činnosti jde o hodnocení vlastností území, ve kterém je objekt umístěn, a jejím cílem je určit zadávací podmínky pro technické dílo tak, aby bylo zabezpečené vůči všem vnějším pohromám. V rámci druhé činnosti je třeba na základě zadávacích podmínek navrhnout, vystavět a provozovat technické dílo tak, aby neohrožovalo sebe a své okolí, a to ani při svých kritických podmínkách [3].

Podle současného poznání již dnes nestačí řídit rizika jednotlivých pohrom, tj. škodlivých jevů různého druhu, protože svět se dynamicky vyvíjí. Je třeba použít pokrokové zásady řízení procesů pro zajištění bezpečného území, obrázek 4, a pro zajištění

bezpečného technologického i jiného objektu, který je umístěn do území, v čase (obrázek 5) [3,4,35].

Obr. 4. Hierarchický soubor provázaných procesů pro zajištění bezpečného území v čase.

Obrázek 4 ukazuje, že pro zajištění bezpečného území a bezpečných veřejných aktiv je třeba použít hierarchický soubor procesů (super proces), který se skládá z pěti procesů:

1. Proces pro získání dostatečných znalostí o území zahrnuje: stanovení aktiv v území; stanovení parametrů území a charakteristik aktiv v rozsahu územní plánovací dokumentace; a stanovení seznamu pohrom, které mají dopady na území (při jejich identifikaci je třeba vyjít ze seznamu pohrom, uvedeném v [1-4], aby nedošlo k zanedbání nějakého významného zdroje rizik).
2. Proces vyhodnocení rizik a následného řízení rizik zahrnuje: stanovení velikostí ohrožení pro všechny pohromy, které mohou mít dopady v daném území a také period jejich opakování (návratu); stanovení zranitelných míst v území a zranitelnost veřejných aktiv s ohledem na stanovené velikosti ohrožení (způsoby stanovení ohrožení jsou například v [2,3]); stanovení velikostí projektových pohrom (normativně určené velikosti pohrom); stanovení dopadů pohrom na území a jeho sledovaná aktiva (je vhodné určit normativní scénáře dopadů pro projektové pohromy); určení integrálních rizik pro všechny důležité pohromy (tj. zvažovat jak přímé dopady pohrom, tak nepřímé dopady pohrom na aktiva způsobené prostřednictvím vazeb a spřažení mezi aktivy); práce s riziky.
3. Proces vyhodnocení kvality řízení a vypořádání rizik zahrnuje: posouzení úrovně účinnosti prevence, připravenosti, odezvy a obnovy s ohledem na integrální rizika spojená s důležitými pohromami; stanovení kritických bodů v oblasti řízení a vypořádání rizik a určení jejich kritičností s ohledem na integritu a účinnost aplikovaných opatření a činností a způsob jejich řízení (tj. jde o odhalení zdrojů možných organizačních havárií); návrh korekcí pro vysoce kritické body.

4. Proces nastavení řízení bezpečnosti zahrnuje: stanovení opatření a činností pro místa s vysokou kritičností a jejich implementace v rámci krátkodobých, střednědobých a dlouhodobých realizačních plánů, a to včetně odpovědností za příslušné realizace a zdrojů potřebných pro realizace; zavedení kultury bezpečnosti na úrovni aktiv, pravidel pro řízení aktiv a řízení bezpečnosti území (a to od vrcholového managementu až po jednotlivé občany); a stanovení postupů odezvy v případě vzniku nouzové situace s požadavkem, aby při každé odezvě na kritické až extrémní situace byly řešeny otázky jak přežití lidí, tak kontinuita důležitých objektů, zařízení a infrastruktur.
5. Proces udržování (zachování) a zvyšování bezpečnosti zahrnuje: systematické vytváření schopnosti provádět včasné a účinné odezvy na kritické situace a zajistit obnovu a kontinuitu služeb v území; stanovení a realizaci strategického programu pro zvyšování bezpečnosti v čase, a to včetně sledování účinnosti procesů pro řízení a vypořádání rizik; pravidelné detailní hodnocení bezpečnosti území každých 10 let; a bezprostřední hodnocení bezpečnosti území po výskytu kritické situace.

Z důvodu dynamického vývoje je nutné sledovat území a připravovat postupy pro korekce nepříznivých situací. Z ekonomických důvodů je třeba nejprve použít nejlevnější postup, který naznačuje zpětná vazba 1 na obrázku 4; v případě jeho selhání použít postup naznačený zpětnou vazbou 2 atd.; v případě obrovských škod a ztrát ihned použít postup naznačený zpětnou vazbou 4, což znamená změnu koncepce bezpečnosti území. V každém případě označeném zpětnou vazbou se provádí dále uvedené úpravy procesů:

- v případě použití zpětné vazby 1, se provádí změny procesu řízení bezpečnosti území jako: změní pravidla pro řízení bezpečnosti území, změní se rozdělení rolí zúčastněných osob, změní se odpovědnosti osob, změní se priority a jejich řízení atd.,
- v případě použití zpětné vazby 2, se provádí změny v procesu hodnocení kvality řízení a vypořádání rizik jako: změní se způsoby řízení rizik v území, změní se rozdělení úkolů pro zvládání rizik mezi zúčastněnými osobami, změní se priority v oblasti řízení a vypořádání rizik, změní se přidělování prostředků na opatření vedoucí ke snížení rizika – např. přestane se spoléhat jen na odezvu a provedou se i preventivní opatření atd.,
- v případě použití zpětné vazby 3, se provedou změny v procesu hodnocení rizik jako: zavedou se další kritéria pro hodnocení rizik, změní se hodnotové stupnice, zváží se příspěvky k integrálním rizikům od dalších vazeb a spřažení mezi aktivy, a to hlavně ty, které byly odhaleny jako původci obrovských škod, ztrát a újmy na veřejných aktivech atd.,
- v případě použití zpětné vazby 4, se provede změna v procesu poznávání území jako: jsou doplněny a do praxe zavedeny nové poznatky, např. do sady zdrojů rizik jsou přidány další škodlivé jevy, které byly odhaleny jako zdroje obrovských škod, ztrát a újmy na veřejných aktivech, změní se velikosti kritičnosti pohrom, změní se velikosti zranitelností aktiv a k tomu se zavedou příslušná opatření atd.

Obrázek 5 ukazuje, že pro zajištění bezpečného technického díla (technologického objektu nebo zařízení), které se nachází v reálném území, je nutné aplikovat super proces, který se skládá ze čtyř procesů:

Obr. 5. Hierarchický soubor provázaných procesů pro zajištění bezpečného technického díla v čase.

1. Proces umístění, návrhu, výstavby a konstrukce technického díla (budovy, zařízení, sítě) zahrnuje: sběr dat o území a jeho aktivech v rozsahu územně plánovací dokumentace; shromáždění dat o pohromách a jejich dopadech, ohroženích a specifikách v daném území (při identifikaci pohrom je třeba vyjít ze seznamu pohrom, uvedeném v [1,2], aby nedošlo k zanedbání nějakého významného zdroje rizik; způsoby stanovení ohrožení jsou například v [2,3]; stanovení a posouzení integrálních rizik a stanovení zranitelnosti technického díla nebo zařízení s ohledem na možné pohromy všeho druhu, a to i těch, kterými v případě kritických podmínek technické dílo může poškodit území, ve kterém je umístěn; umístění entity, projektování, výstavba a konstrukce objektů a zařízení s ohledem na odhalená rizika s respektováním principu ochrany do hloubky (Defence-In-Depth) [3,4]) a vypořádání rizik spojených s vazbami a spřaženími mezi technickým dílem nebo zařízením a jeho okolím; a stanovení způsobu řízení bezpečnosti technologického celku v průběhu jeho životního cyklu (dokumentace: předběžná bezpečnostní zpráva [3]).
2. Proces přípravy a zahájení trvalého provozu technologického celku (budovy, zařízení, sítě) zahrnuje: zkoušky funkčních schopností jednotlivých budov, vybavení a zařízení a odstranění odhalených zdrojů rizik v oblastech technické a organizační; poloprovoz, během kterého se zjišťují a vypořádávají rizika spojená s vazbami a spřaženími (realizovanými různými toky při provozu), a to uvnitř i vně technického díla; zkušební provoz, během něhož se dále zjišťují a vypořádávají rizika spojená s vazbami a spřaženími (realizovanými různými toky při provozu), a to uvnitř i vně technického díla; realizace návrhu řízení bezpečnosti technického díla (zpracování předprovozní bezpečnostní zpráva a návrh zprávy provozní bezpečnosti [3]); a zahájení trvalého provozu.
3. Proces bezpečného provozu technického díla (budovy, zařízení, sítě během životního cyklu zahrnuje: zavedení provozních postupů pro normální, abnormální a kritické podmínky, kultury bezpečnosti a monitoringu rizik; program pro zvyšování bezpečnosti technického díla v čase a postupy plánu kontinuity pro překonání kri-

tických podmínek (provozní bezpečnostní zpráva [3]); plán optimální údržby budov, vybavení a zařízení a jeho zabezpečení (odpovědnosti, prostředky); plán pro pravidelné prohlídky budov, vybavení a zařízení a pravidel pro provádění včasných oprav zjištěných závad na budovách, vybavení a zařízení, zejména těch, které důležité z bezpečnostních důvodů a jejich zabezpečení, a ve kterých jsou vyznačeny odpovědnosti, postupy a prostředky; plán modernizace budov, vybavení a zařízení a plán pravidelných auditů bezpečnosti technického díla a jeho dopadů na okolí (s vyznačenými odpovědnosti, prostředky), a to včetně posuzování: úrovně kultury bezpečnosti, úrovně realizace opatření pro zvládnutí zjištěných významných rizik, úrovně odstranění zdrojů organizační havárií; a včasné reakce na kritické situace a zajištění kontinuity provozu technického díla po opravě.

4. Proces ukončení činnosti technického díla (budovy, zařízení, sítě) zahrnuje vyřazení z provozu, odstranění budov a zařízení a předání území pro nové použití zahrnuje: stanovení zdrojů a odpovědnosti za opatření a aktivity, které jsou nezbytné pro odstranění technického díla vyřazeného z provozu (budovy, zařízení a sítě) a sanační práce; odstranění budov, zařízení a sítí z území; provedení dekontaminace území. Jde o proces, na který se často zapomíná v praxi, jak ukazuje spousta brownfields show, a proto, je třeba nezapomínat na předmětný úsek během životního cyklu technického díla.

Z důvodu dynamického vývoje je nutné sledovat technické dílo a připravovat postupy pro korekci nepříznivých situací. Je také nutné zvažovat, že každý technologický celek má omezenou životnost, a proto, pro zachování podmínek pro bezpečí a rozvoj lidí je nezbytné předcházet znehodnocení území. Z toho důvodů je třeba připravit postupy a korekce u každého technického díla pro odvrácení nepříznivých situací. Z ekonomických důvodů je třeba nejprve použít nejlevnější postup, který je vyznačený zpětnou vazbou 1 na obrázku 5; v případě jeho selhání použít postup vyznačený zpětnou vazbou 2 atd.; v případě obrovských škod ihned použít zpětnou vazbu 3, která znamená úplnou změnu konceptu bezpečnosti. V každém případě označeném zpětnou vazbou se provádí dále uvedené úpravy procesů:

- v případě použití zpětné vazby 1, se provádí změny v procesu řízení bezpečnosti technického díla jako: změní se požadavky státní správy na provoz technického díla, pravidla pro řízení bezpečnosti technického díla, priority v řízení bezpečnosti technického díla – obrázek 13 ukazuje, že často je nutné vyřešit konflikty mezi bezpečností veřejných aktiv a počet výrobků technického díla atd.),
- v případě použití zpětné vazby 2, se provádí změna procesu přípravy a zahájení trvalého provozu technického díla, např. změní se způsoby řízení a vypořádání rizik a jejich ověření během zkušebního provozu, změní se alokace vypořádaní rizik mezi zaměstnanci, změní se priority v oblasti řízení a vypořádání rizik, změní se systém přidělování prostředků pro opatření vedoucí ke snížení rizika – např. přestane se spoléhat jen na odezvu a provedou se i preventivní opatření atd.,
- v případě použití zpětné vazby 3, se provádí možné změny v umístění stavby, projektování, výstavbě a konstrukci technického díla, např. jsou zváženy další zdroje rizik, použita další kritéria pro hodnocení rizik, změněny hodnotové stupnice, zváženy další příspěvky k integrálnímu riziku spojené s vazbami a spřaženími mezi aktivy, které byly odhaleny jako zdroje velkých ztrát, škody a újmy na veřejných aktivech atd. Pochopitelně v souladu s pravidly uvedenými v [5] se v daném případě nejprve přehodnotí potřebnost technického díla. Je-li předmětné dílo pro

území potřebné, tak se provedou korekční opatření a zavede se monitoring s častějším hodnocením a korigováním rizik.

Dynamický vývoj vyžaduje pravidelně hodnotit v každém území koexistenci území a technických děl, která jsou v něm umístěná, protože je nutné zachovat podmínky v území, které umožní bezpečný život budoucích lidských generací. Při zjištění významných problémů je nezbytné nalézt zdroje, síly a prostředky pro odstranění závažných dopadů na budoucí stav území a budoucí generace. Je nutné určit opatření, zdroje pro jejich realizace a odpovědnost za jejich provádění, v rámci veřejného zájmu je nutné použít všechny prostředky pro provedení nápravy v přijatelném časovém horizontu.

Jelikož nejde o triviální problémy, ale o propojení mnoha oblastí, tak se zpracovává speciální dokumentace. Pro každé technické dílo je třeba na základě dat, měření a výsledků testů i zkušebního provozu zpracovat zprávu, ve které je uveden způsob zajištění bezpečnosti, jak vyžaduje např. [53], atomový zákon (zákon č. 263/2016 Sb.), direktiva SEVESO, a v omezené míře i zákon č. 224/2015 Sb. Na základě srovnání poznatků nejpodrobnější bezpečnostní zpráva má obsah: 1. Úvod. 2. Popis zařízení. 3. Opatření pro řízení bezpečnosti. 4. Hodnocení lokality. 5. Konstrukční aspekty. 6. Popis a konformita systémů s projektem. 7. Analýza bezpečnosti (deterministické a pravděpodobnostní). 8. Uvedení do provozu. 9. Provozní aspekty. 10. Provozní limity a podmínky. 11. Ochrana proti úniku nebezpečných látek. 12. Nouzová připravenost. 13. Aspekty ochrany životního prostředí vně zařízení. 14. Nakládání s odpady. 15. Vyřazení z provozu a ukončení životnosti. Doklady o revizích a aktualizacích. Seznam použitých dokumentů.

Bezpečnostní zpráva dokumentuje, že bylo provedeno hodnocení bezpečnosti technického díla, a že během provozu bude technické dílo bezpečné, což znamená, že byla vypořádána všechna prioritní rizika, nastaven monitoring včetně nápravných opatření při realizaci rizik [3]. Aby se zabránilo chybám při spouštění, tak před zahájením provozu realizuje podrobný audit zprávy o bezpečnosti. Audit je nutné provést ze dvou hledisek:

- jak je objekt zajištěn proti všem pohromám, které jsou možné v daném místě,
- zda objekt neohrožuje sebe a své okolí při svých kritických podmínkách.

Při auditu se požívají inženýrské metody disciplín, které pracují s riziky za účelem posouzení dále uvedených skutečností:

- co by se mohlo stát,
- jak je to pravděpodobné,
- lze si představit důsledky,
- kdo / co je v ohrožení,
- jaký je katastrofický potenciál,
- jaká příčina by mohla odstartovat katastrofické důsledky,
- kontrolovatelnost/dobrovolnost,
- obeznámenost / prodleva,
- jaká je nevratnost důsledků,
- jaká je přijatelnost,
- jaká je míra obav,
- jak spravedlivě budou rozděleny dopady,
- co by se mělo dělat,
- co se musí dělat.

4. RECENTNÍ POZNATKY SPOJENÉ S METODAMI POUŽÍVANÝMI V INŽENÝRSKÝCH DISCIPLÍNÁCH, KTERÉ PRACUJÍ S RIZIKY

Jak bylo ukázáno dříve, tak příčinou rizik jsou procesy v lidském systému, tj. území i v technických dílech. Uvedené procesy vyvolávají škodlivé jevy (pohromy), které zahrnují i havárie a selháním technických systémů v důsledku vazeb a toků mezi prvky (aktivy) systému [1]. Předmětné procesy se v důsledku dynamického vývoje světa vyznačují řadou nejistot a řadou neurčitostí. Jak bylo uvedeno v předchozí kapitole náhodné nejistoty lze ocenit pomocí aparátu matematické statistiky, neurčitosti lze pouze odhadnout na základě důkladné znalosti zdrojového procesu a jevu a pomocí speciálních metod a expertů. Proto se používají rozmanité přístupy a metody identifikace, analýz, třídění a hodnocení. K tomu potom existují různé nástroje pro sběr, zpracování dat, interpretaci výsledků a uložení dat. Nástroje a techniky závisí na kvalitě dat, cílech zpracování, kvalifikovanosti zpracovatelů atd. Výsledky získané aplikací nástrojů závisí nejen na provedení, ale hlavně na kontextu, který nástroj vystihuje [8,9].

4.1. Přístupy používané při práci s riziky

Technická díla jsou složité systémy a tak při řešení jejich problémů spojených s riziky používáme dle povahy problému různé přístupy [3,4]. Základní používané přístupy v inženýrských disciplínách zabývajících se riziky jsou v abecedním pořadí přístupy: analytický, deduktivní, deterministicky, fuzzy, heuristický, induktivní, konzervativní, morfologický, observatorní, pragmatický, pravděpodobnostní, prevence ztrát, sociálně-politický, systémový a vědecko-racionální [9]. Před jejich charakteristikou je třeba upozornit na to, že když se přístupy použijí jen z pohledu jednoho specialisty, tj. ekonoma, sociologa nebo technika, tak výsledky nejsou stejné, protože každý specialista uplatňuje preference spojené s vlastní profesí [3]. Proto při řízení rizik technických děl, podniku, organizace či území musí být přístup víceoborový a mezioborový, tj. musí být použity speciální techniky (např. aplikace DSS – systém pro podporu rozhodování – Decission Support System) a tým expertů z různých oborů, kteří jsou schopni vzájemně chápat problémy jiných oborů a hledat konsensus [3].

Analytický přístup je přístup, který dovoluje přistupovat k řešení problému s využitím obecně přijatých vědních hypotéz, což jsou v našem případě Newtonovy zákony, které odpovídají rovnováze okamžité vnitřní energie v systému. Pro sestavování rovnic dynamického chování musíme velmi pečlivě pochopit mechanismus fyzikálního chování, abychom správně popsali algoritmy zpětných vazeb v systému a tím i příčinnost chování. Pochopení fyzikálního mechanismu a jeho algoritmické vyjádření je velmi obtížné. Proto je tomuto přístupu vytýkána přílišná složitost a zapomíná se na to, že sestavení popisu už znamená obrovský pokrok k pochopení chování dynamického systému. Popis může však jen těžko sestavit ten, kdo neovládá odpovídající vědní obor. Za několik staletí tento problém velmi úspěšně zvládly přírodovědné obory. Chceme-li hovořit o daném oboru jako o vědním, pak kromě specifických znalostí, musíme do teorie zabudovat výstavbu představ či hypotéz o příčinném dynamickém chování systémů tohoto oboru. Z hlediska rozvoje každého oboru je analytický přístup postupem prioritním.

Deduktivní přístup – usuzování se provádí od obecného k jednotlivému, od přijatých výroků (premis) se dospívá k novému důsledku. V deduktivní analýze se předpokládá, že systém nebo proces selhal určitým způsobem. Další činností je stanovit, jakým způsobem systém, složky, chování operátora a organizace přispěly k poruše. Slovní dedukce tvoří ze slov závěr. Typová aplikace je vyšetřování nehody. Deduktivní přístup začíná v jednom časovém bodě (události) na základě faktů a jde zpět v čase k určení předcházející události a stanovuje, které chyby (instrumentální a/nebo lidské) přispěly k nehodě. Příklady deduktivních technik jsou: analýza stromu poruch (FTA); CTM (Causal Tree Method); MORT (Management Oversight and Risk Tree); MCSOII (Multiple-Cause, Systems-Oriented Incident Investigation) [9].

Deterministický přístup je založen na předpokladu, že každý jev je nutným důsledkem podmínek a příčin. Za výsledek se považuje hodnota funkce, která charakterizuje výskyt jevu.

Fuzzy přístup je založen na existenci neurčitostí v datech. Nejsme-li schopni stanovit přesné hranice třídy určené vágním pojmem (např. malý, nízký, zanedbatelný), nahrazujeme rozhodnutí o příslušnosti či nepříslušnosti daného prvku do ní mírou μ vybíranou z nějaké stupnice. Každý prvek má takto přiřazenou míru μ, která vyjadřuje jeho roli a místo v dané třídě. Při použití uspořádané stupnice menší míra μ vyjadřuje, že prvek je blíže k okraji třídy a nejčastěji se k tomuto účelu volí čísla z intervalu <0;1>. Míra μ se nazývá stupněm příslušnosti prvku do dané třídy a třída, v níž každý prvek je charakterizován stupněm příslušnosti do ní se nazývá mlhavou množinou. Rozeznávají se prvky patřící do množiny ($\mu = 1$), prvky nepatřící do množiny ($\mu = 0$) a prvky patřící do množiny se stupněm příslušnosti $\mu = 0.20$, $\mu = 0.50$, $\mu = 0.75$, $\mu = 0.90$, atd. Zavedení verbální proměnné výše uvedeným způsobem umožňuje odstranit rozdíly subjektivního chápání pojmů a vhodně zvolenou množinu slovních výrazů přijatelným způsobem standardizovat.

Heuristický přístup je založen na aplikaci heuristik, tj. na metodickém postupu, který je založený na zkušenosti. Metodický postup je logický a organizovaný a vede k racionálnímu objevování a systematickému shromažďování a úpravě nových poznatků. Hlavní význam spočívá ve schopnosti heuristik získat optimální výsledky v nealgoritmizovaném prostředí.

Induktivní přístup – usuzování se provádí od jednotlivého (jedinečného) k obecným závěrům. Vychází z dílčí chyby nebo počáteční události a určuje jaký vliv má počáteční chyba nebo událost na provoz systému. Pro zkoušení detailů příčinných faktorů je také často nezbytné aplikovat deduktivní analýzu. Příklady induktivních technik jsou: identifikace zdrojů ohrožení a provozuschopnosti (HAZOP); AAM (Accident Anatomy Method); AEA (Action Error Analysis Technique); CELD (Cause-Effect Logic Diagram Technique) [9].

Konzervativní přístup je založen n na předpokladu, že z důvodu bezpečnosti je nutno při odhadech a výpočtech zvážit právě ty hodnoty základních veličin, které vystihují nejméně příznivý případ a při splnění zajišťují nejvyšší dosažitelnou bezpečnost. Na základě toho se při řízení bezpečnosti a jeho součástech používají maximální projektové havárie, nejméně příznivý útlum dopadů pohromy se vzdáleností, maximální očekávané pohromy, scénáře nejhorších havárií, apod., např. direktiva Seveso a práce [43,44,58]. Jsou odborné skupiny, které tvrdí, že tento přístup není na místě, protože existující neurčitosti v datech vedou k finančně a technologicky drahým řešením, která nesplňují mnohdy záměry [6,58].

Morfologický přístup k analytickému vyšetřování nehody je založen na struktuře vyšetřovaného systému. Zaměřuje se přímo na potenciálně nebezpečné prvky (např. výrobní operace, situace). Deduktivní a induktivní přístup je zaměřen na direktivní přístupy podpořené formalistickými symboly a pravidla a řešení poskytujícími algoritmy. Morfologický přístup je více směřován strukturou systému a zkušeností z provozování systému. Záměr je koncentrovat se na faktory, které mají nejvýznamnější vliv na bezpečnost. Když analytik provádí „morfologickou analýzu“, tak v prvé řadě aplikuje své předchozí zkušenosti z vyšetřování nehod. Vyšetřování se spíše soustřeďuje na známé zdroje rizik (např. nebezpečné chemické látky, nahromadění energie), než na to, aby se braly v úvahu všechny možné odchylky s potenciálním dopadem na bezpečnost nebo bez tohoto dopadu. Obvykle je morfologický přístup přizpůsobení deduktivního nebo induktivního přístupu tím, že má vlastní pravidla. Příklady morfologických technik dle [9] jsou: AEB (Accident Evaluation and Barrier Technique); WSA (Work Safety Analysis). Jiné nezařazené techniky pro vyšetřování nehod a havárií dle [3] jsou: Charge Evaluation/Analysis; HPES (Human Performance Enhancement System); MES (Multilinear Events Sequencing); STEP (Sequentially Timed Events Plot); SCAT (Systematic Cause Analysis Technique); TOR (Technique of Operations Review). V odborné literatuře lze najít více než tisíc technik, které původně byly odvozeny pro konkrétní případy a postupem času byly zobecněny.

Observatorní přístup je založen na tom, že se hodnotí příznaky časových řad sledujících požadovaný parametr. Pro vyhodnocení příznaků byly vypracovány statistické matematické metody. V procedurách nazvaných korelační metody je možno určit parametry kmitavého článku, pokud jsme se rozhodli tímto popisem charakterizovat dynamický systém. V tomto případě jde o parametry setrvačnosti a vazební koeficienty. Časové průběhy dynamického chování lze přepočítat do frekvenční oblasti, v níž můžeme snadno sledovat periodické cykly dynamického chování, které jsou výslednicí transformace kinetické a potenciální energie ve všech dynamických systémech.

Pokud nedochází ke změně podmínek při snímání časové řady a tato řada je dostatečně dlouhá a statisticky neměnná, můžeme se obezřetně vyjadřovat k jistému stavu systému do budoucna. Specifickou vlastností observatorního přístupu je, že dává důraz na konkrétní řešení dynamického problému v okamžiku snímání časové řady. Parametry jsou určeny a posteriori a jsou zatíženy předpoklady, které nemusí vždy platit. Nedovolují též určit vnitřní strukturu systému a ztěžují fyzikální výklad příčinného chování. Do této skupiny náleží v současné době vědní disciplíny, jako např. expertní metody, umělá inteligence, fuzzy metody, neuronové sítě atp. Pro získávání základních tvarů matematických modelů z experimentálního pozorování pro dodatečné nasazení počítačů je tento přístup velmi užitečný.

Pragmatický přístup je založen na předpokladu, že nejlepší je takové řešení problému, které se nám na základě zkušeností nejlépe hodí. Ve vyspělých společnostech se při aplikaci v rozhodování a řízení požaduje průkaz znalostí a zkušeností odborníků, kteří pragmatické řešení formulují.

Pravděpodobnostní / stochastický přístup založený na předpokladu, že výskyt každého jevu má určitou nejistotu, tj. možnost výskytu náhodného jevu je odhadnutá s určitou hodnotou pravděpodobnosti výskytu.

Prevence ztrát (Loss Prevention) je systematický přístup k prevenci (předcházení) havárií nebo k minimalizaci jejich dopadů. Zahrnuje prostředky pro eliminaci zdrojů rizik nebo omezení pravděpodobnosti jejich realizace a pro zmírnění dopadů spoje-

ných s touto realizací (preventivní a následná opatření). Dále zahrnuje i identifikaci vhodných kontrolních opatření.

Přístup sociálně - konstruktivistický (sociálně - politický) je založen na tom, že riziko se posuzuje podle vnímání těmi, kteří jim jsou ovlivněni. Řízení se provádí na základě kontrolovatelnosti, dobrovolnosti a obeznámenosti s okolnostmi vzniku rizika.

Systémový přístup je způsob řešení problémů či jednání, při němž jsou jevy chápány komplexně ve svých vnějších i vnitřních souvislostech. Je to uspořádávající princip, který zajišťuje:

- pojmovou jednoznačnost,
- pravidla pro myšlenkové operace analýzy a syntézy daného problému.

Jeho přínosem je skutečnost, že řeší jakékoliv složité problémy - špatně přehledné a slabě strukturované, s bohatou vnitřní členitostí, vhodný pro začátek řešení, jednorázového charakteru a netypické.

Vědecko-racionální (technokratický) přístup chápe riziko jako objektivní koncept, který je nezávislý na vnímání a může se kvantifikovat na základě technologické a vědecké analýzy. Hodnocení a řízení rizika je založeno především na analýze nákladů a přínosů.

4.2. Přehled základních používaných metod při práci s riziky a jejich validita

Na základě logických souvislostí [2] se riziko v inženýrské praxi vyjadřuje vztahem

$$R = H \times Z,$$

ve kterém ***R*** je riziko, ***H*** ohrožení, které představuje pro sledované aktivum nebo objekt sledovaná pohroma a ***Z*** je zranitelnost sledovaného aktiva nebo objektu. U technických děl, která jsou složitými systémy systémů, tento jednoduchý vztah je pouze ideový.

4.2.1. Druhy rizik sledované u technických děl

V praxi rozlišujeme dle počtu zvažovaných chráněných aktiv tři druhy rizik [2]: dílčí, integrované a integrální.

Dílčí riziko je riziko spojené s jedním aktivem a v současné době se používá nejčastěji. Dílčí rizika jsou rozmanitá, např. zdravotní rizika, technologická rizika, riziko požáru atd. Pro výpočet dílčích rizik již existuje řada právních předpisů, norem a standardů a s nimi souvisejících podpůrných software [2]. Na základě údajů v [2] a konkrétních šetření havárií a selhání technických děl [63] ***základní skupiny dílčích rizik zvažovaných v technických projektech a při zajištění bezpečnosti technických děl jsou:***

1. Stavebně-technologická a projekční rizika.

2. Kreditní rizika.
3. Tržní rizika.
4. Vnější rizika.
5. Provozní rizika.
6. Rizika spojená s řízením a rozhodováním.

Stavebně-technologická a projekční rizika spojená s technickým dílem zahrnují:
- stavební a projekční rizika spojená s technickým dílem,
- rizika lokality, ve které je umístěno technické dílo,
- rizika spojená s použitím chybných technologií, sítí a souvisejících služeb u technického díla.

Stavební a projekční rizika zahrnují rizika spojená s:
- projektovou dokumentací technického díla (správná / špatná, chyby),
- konstrukcí a stavbou technického díla,
- překročením stavebních nákladů při výstavbě technického díla,
- znečištěním lokality technického díla a jejího okolí během realizace technického díla, které způsobí veřejná správa špatným povolením a špatným dohledem,
- znečištěním lokality technického díla a jejího okolí během realizace technického díla, které způsobí dodavatel,
- vlivem projektu na životní prostředí během životnosti technického díla, které způsobí veřejná správa špatným rozhodnutím při povolení provozu technického díla a špatným dohledem nad provozem technického díla,
- vlivem projektu na životní prostředí během životnosti technického díla, které způsobí dodavatel a provozovatel.

Rizika lokality, do které je umístěno technické dílo, zahrnují rizika spojená s:
- technickým dílem samotným,
- dostupností lokality,
- vlastnictvím lokality,
- stavem lokality,
- sítěmi nacházejícími se v lokalitě (v místě stavby),
- územním plánem
- stavebním povolením,
- kulturním či archeologickým dědictvím,
- chráněnou krajinnou oblastí.

Rizika spojená s použitím chybných technologiemi, sítí a souvisejících služeb u technického díla zahrnují rizika spojená s:
- vadami vzniklými v průběhu realizace technického díla,
- vadami vzniklými v průběhu provozu technického díla během jeho životnosti,
- použitím chybné technologie v technickém díle,
- technologickou nedostatečností technického díla,
- neočekávaným přerušením dodávky energie, výpadku služeb a podpůrných systémů zajišťovaných soukromým sektorem, které znemožní nebo významně naruší provoz technického díla,
- neočekávaným přerušením dodávky energie, výpadkem služeb a podpůrných systémů zajišťovaných veřejnou správou, které znemožní nebo významně naruší provoz technického díla.

Kreditní rizika spojená s technickým dílem zahrnují rizika spojená s:

- likviditou technického díla,
- nesplněním závazků technického díla

Rizika, která působí nesplnění závazků technického díla, zahrnují rizika spojená s:
- nedodržením závazků soukromým sektorem,
- selháním technického díla, které vede ke ztrátě pro veřejnou správu,
- selháním veřejné správy, která vede ke ztrátě u provozovatele technického díla,
- koncentrací technického díla na jednoho dodavatele,
- koncentrací technického díla na jednoho odběratele,
- ztrátou podpory technického díla ze strany veřejné správy.

Tržní rizika spojená s technickým dílem zahrnují rizika spojená s:
- poptávkou v případě, že dodavatelem je veřejná správa,
- poptávkou v případě, že dodavatelem je soukromý subjekt,
- zvýhodněním konkurence,
- ostatní tržní rizika jako jsou rizika: měnové; inflační; a úrokové.

Vnější rizika spojená s technickým dílem zahrnují rizika spojená s:
- politickou mocí,
- živelními a jinými pohromami,
- ostatní vnější rizika.

Riziko pro technické dílo ze strany politické moci zahrnuje riziko spojené s:
- národní či mezinárodní situací,
- selháním vlády,
- povinnostmi ČR v EU, NATO.

Riziko pro technické dílo spojené s živelními a jinými pohromami zahrnuje riziko spojené s:
- živelní pohromou rozměru katastrofy, tzv. vyšší moc,
- terorismem
- válkou.

Ostatní vnější rizika pro technické dílo zahrnují rizika spojená s:
- legislativou obecnou a hlavně v oblasti daní a s jejími změnami,
- potřebou dodatečných povolení,
- situací v odvětví - ztráta konkurenceschopnosti, stávky apod.

Provozní rizika spojená s technickým dílem zahrnují rizika spojená s:
- technickými zařízením a vybavením technického díla,
- způsobem řízení technického díla,
- zaměstnanci,
- jednáním zaměstnanců.

Rizika technického díla související se zařízením a vybavením technického díla zahrnují rizika spojená s:
- vlastním technickým zařízením a vybavením,
- vstupy, tj. kvalitou a vlastnostmi používaných materiálů,
- údržbou, opravami, modifikacemi a adaptacemi,
- nízkou zůstatkovou hodnotou.

Rizika technického díla spojená se způsobem jeho řízení souvisí s:
- chováním managementu technického díla,
- způsobem rozhodování managementu technického díla,
- zavedenou kulturou bezpečnosti,

- chováním managementu technického díla k zaměstnancům.

Rizika technického díla související se zaměstnanci zahrnují rizika spojená s:
- neodpovídajícími pracovními silami,
- nezastupitelností u kritických činností,
- nedostatkem lidských zdrojů,
- pracovně právními spory,
- selháním lidského faktoru.

Rizika technického díla spojená s jednáním zaměstnanců zahrnují riziko spojené s:
- lidskou spolehlivostí, tj. s náchylností člověka dělat chyby (v technických dílech jde o projektanty, konstruktéry, technology, provozáře, údržbáře, techniky a ostatní personál,
- podvodným jednáním,
- nelegálním jednáním,
- bezpečností technologických systémů,
- poškozením zařízení, krádeží apod..

Rizika spojená s řízením a rozhodováním technického díla zahrnují rizika:
- smluvní,
- ostatní spojená s řízením a rozhodováním.

Smluvní rizika spojená s technickými díly zahrnují riziko spojené s:
- odpovědností třetí straně,
- změnou smlouvy,
- porušením obecně závazných předpisů,
- korupcí.

Ostatní rizika spojená s technickými díly spojená s jejich řízením a rozhodováním zahrnují rizika spojená s:
- koncepcí a strategickým rozhodováním,
- prevencí ztrát a péčí o kritická aktiva,
- kulturou bezpečností,
- reputací.

V oblasti finanční se používají dále uvedená dílčí rizika:

1. Finanční riziko představuje míru snížení hodnoty sledovaného objektu, tj. podniku / majetku / kritické infrastruktury / technologie, které je způsobené živelní či jinou pohromou nebo interakcí možnou v lidském systému. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
2. Kreditní riziko představuje míru snížení hodnoty sledovaného objektu, tj. podniku / majetku / kritické infrastruktury / technologie, které je způsobené tím, že protistrana nesplní existující závazek (nezaplatí úvěr, fakturu, nedodá výrobek apod.). Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
3. Tržní riziko představuje míru snížení hodnoty obchodovatelných finančních nároků, tj. zboží / objektů / majetku / kritické infrastruktury / technologie, které je způsobené změnami na trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
4. Měnové riziko představuje míru snížení hodnoty deviz, které je způsobené změnami na bankovním trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.

5. Kurzovní riziko je druh rizika vznikajícího změnou kurzu jedné měny vůči jiné měně. Když investoři a firmy drží statky či provádějí obchodní operace napříč hranicí měnových oblastí, vystavují se měnovému riziku, proti kterému se však mohou zajistit.
6. Úrokové riziko představuje míru snížení hodnoty majetku, tj. zboží / objektů / budov / kritické infrastruktury / technologie, které je způsobené změnami na finančním trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
7. Akciové riziko představuje míru snížení hodnoty akcií, které je způsobené změnami na burze. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
8. Komoditní riziko představuje míru snížení ceny obchodovatelných komodit, které je způsobené změnami na trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.
9. Likviditní riziko představuje míru ztráty schopnosti realizovat určitý obchod v dané chvíli, což je způsobené: platební neschopností či insolvencí podnikatele (vlastní nelikvidita); neexistencí protistrany pro obchod (nelikvidita trhu); a změnami na trhu. Je vyjádřeno pravděpodobností výskytu snížení hodnoty, které je vyjádřeno penězi.

Integrované riziko – představuje součet nebo jinou agregaci dílčích rizik. Používá se např. v BOZP [2,14].

Integrální riziko je založeno na systémovém pojetí entity a zahrnuje propojení mezi aktivy a komponentami technického díla [3,4,17]. Je dané vztahem

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

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

Integrální čili systémové respektuje i vztahy a toky mezi aktivy a je určováno s větší či menší přesností, jak je dále ukázáno. Je zřejmé, že pro dlouhodobé zajištění bezpečného technického díla je třeba zvažovat integrální riziko. Jelikož ve výše uvedeném vzorci je neznámá ztrátová funkce, tak v pracích [3,4] jsou uvedené postupy používané v praxi.

Je také třeba poznamenat, že určení jednotlivých typů rizik se také liší náročností na data a metody jejich zpracování [2,4,9]; nejméně náročné je určení dílčích rizik, a proto se dílčí rizika nejvíce používají, i když jejich vypovídací schopnost s ohledem na celkovou bezpečnost má velká omezení.

4.2.2. Metody, techniky a nástroje pro práci s riziky používané v praxi

Nástrojů a metod pro identifikaci, analýzu, hodnocení a řízení rizik nepříliš složitých systémů je velké množství; řada z nich je popsána v pracích [2,9,15] a v pracích, které jsou v ní citovány. Z práce [9] vyplývá, že při práci s riziky jde kromě analytických metod hlavně o metody:

Abstrakce; agregace; algoritmizace; analogie; analytical hierarchy proces (AHP); analýza; analýza metodou křížových interakcí; analýza metodou stromu událostí; analýza metodou stromu poruchových stavů; analýza příčin a důsledků; analýza nákladů a efektivity; analýza nákladů a užitků; analýza s cílem stanovit nejmenší náklady; analýza nákladů a přínosů podle užitečnosti; anketa; anketa s tazatelem; aplikace dimenzionální analýzy; aplikace hierarchické analýzy; aplikace kardinální číselné stupnice; aplikace klasifikační analýzy; aplikace myšlenkové mapy; aplikace stromu problému; aplikace obrazových a myšlenkových schémat; aplikace nominální (binární) stupnice; aplikace ordinální bodovací stupnice; aplikace pravidel rozhodování za neurčitosti; aplikace vážené užitnosti; argumentace; audit; automatizace; axiomatická metoda.

Benchmarking; bezprostřední úsudek; bodovací metoda; brainstorming; brainwriting.

Citlivostní analýza a testy citlivosti.

Dedukce; definování; detekce; diagram příčin a následků; diskuse; diskuse 66; dokazování; dotazníkové šetření.

Empirické metody; experiment; expertní metody.

Formalizace; formalizované postupy rozhodování; Fullerova metoda.

Generalizace; genetická metoda; Gordonova metoda.

Heuristika; heuristické metody pro strukturování problémů; hodnocení; hodnocení EIA; hodnocení procesů; hodnocení SEA; hodnocení techniky; hypoteticko-deduktivní metoda.

Identifikace; indukce; inspekce; inspirace; interpretace; interview nestandardizované; interview standardizované; intuice; inženýrský úsudek; Išikavův diagram.

Kauzální analýza; klasifikace; klasifikace entit / pojmů; komparace; komparativní metoda; konstruktivní (genetická) metoda; kontrola; koordinace; kvalifikovaný odhad; kvantifikace; kvantifikace rizika.

Lexikografická metoda; logická analýza; logický postup; logistická metoda.

Marginální analýza; matematické programování; matice odpovědnosti; měření; metafora; metoda alokační; metoda aplikace černé schránky; metody cílového prognózování; metoda delfská (DELPHI); metoda duální ALO-FUL; metoda extrapolace; metoda Eye-Fitting; metoda hlavního článku; metoda hodnocení dosažitelnosti; metoda hodnocení variant; metoda hodnotové analýzy; metoda kauzálního modelu; metodika PPP; metody konkrétních sociologických průzkumů; metody kvalitativního hodnocení; metody kvantitativního hodnocení; metody semi kvantitativního hodnocení; metoda mezních odhadů; metoda mlhavých množin; metoda Monte Carlo; metoda nekompetence; metoda orientovaná na cíle; metoda známkovací; metoda párového hodnocení; metoda párového srovnávání kritérií; metoda PESTE; metoda pokusů a omylů; metoda porovnání investiční akce podle míry návratnosti investic; metoda pořadí; metody operační analýzy; metoda použití případové studie; metody pro multikriteriální hodnocení; metody otevřené skupinové komunikace; metody pro podporu rozhodování; metody pro stanovení vah; metody pro zlepšení práce s informacemi a

pro strukturování problému; metoda rentability investic; metody sběru dat; metody síťové analýzy; metody srovnávání nesouměřitelných jevů; metoda založená na dílčí funkci užitku; metoda stanovení vah kritérií z daného souboru kritérií; metoda stanovení vzorových / mezních hodnot kritérií; metoda stromu významnosti; metoda tvorby soustavy kritérií pro hodnocení; metoda týmového expertního hodnocení; metoda váženého součtu bodů; metoda váženého součtu pořadí; metoda výběru nejvhodnější varianty; metody výběru priorit; metoda založená na dílčí funkci užitku; metody získávání dat; metody získávání expertních odhadů; metoda známkování; metody zpracování expertních odhadů; metoda zpracování a použití scénáře při rozhodování; modelování; modely vícekriteriálního (multikriteriálního) rozhodování; monitoring; morfologická analýza; myšlenková mapa.

Obsahová analýza dokumentace; ocenění majetku; ochrana dat; operační výzkum; operační systémová analýza.

Panelová diskuse; popis; preferenční metody; proaktivní řízení; procesní řízení; prognostická metoda; programové řízení; projektování; projektové řízení; připravenost.

Reaktivní řízení; redukce; rozhodování; rozhodovací proces; rozhodovací strom; rozhovor.

Řízení; řízení problémů; řízení znalostí.

Saatyho metoda; scénář; scénář řízení; scoping; screening; simulace; sociologická metoda obsahové analýzy; stanovení četnostního grafu; stanovení útlumu; strategické plánování; strategické řízení; strukturalizace; strukturálně funkční analýza; SWOT analýza; syntéza; systémová analýza; systémové inženýrství; systémové metody; systémové modelování; systém řízení bezpečnosti.

Šestislovný graf.

Taxonomie pojmů; technika aplikace DSS; technika bazické varianty; technika cíleného vhledu; technika diagramu proč – proč; technika diagramu rybí kosti; technika stanovení vah kritérií; technika inspirativního generování; technika strukturování problému; teorie her; terminologický slovník; týmové expertní hodnocení; třídění; typová analýza.

Verifikace; vícekriteriální hodnocení; vícekriteriální metody hodnocení variant; vícekriteriální rozhodovací analýza; výběr jevů; vyrovnávací počet; vývojový diagram.

Zobecnění; zobrazení dat nad územím; způsoby rozhodování a rozhodovací procesy.

4.2.3. Metody používané pro analýzu a hodnocení rizik

Běžné metody pro analýzu a hodnocení rizik používané v praxi dle poznatků shrnutých v pracích [2,9,13] jsou:

1. Check list (kontrolní seznam).
2. Safety audit (bezpečnostní kontrola).
3. What – If Analysis (analýza toho, co se stane když).
4. Preliminary Hazard Analysis – PHA (předběžná analýza ohrožení).
5. Quantitative Risk Analysis – QRA (analýza kvantitativních rizik procesu).
6. Failure Mode, Effect and Criticality Analysis – FMECA (analýza dopadů selhání a jejich kritičnosti).
7. Hazard Operation Process - HAZOP (analýza ohrožení a provozuschopnosti).

8. Event Tree Analysis – ETA (analýza stromu událostí).
9. Failure Mode and Effect Analysis – FMEA (analýza selhání a jejich dopadů)
10. Fault Tree Analysis – FTA (analýza stromu poruch).
11. Human Reliability Analysis – HRA (analýza lidské spolehlivosti).
12. Fuzzy Set and Verbal Verdict Method – FL-VV (metoda mlhavé logiky verbálních výroků).
13. Relative Ranking – RR (relativní klasifikace).
14. Causes and Consequences Analysis - CCA (analýza příčin a následků)
15. Probabilistic Safety Assessment – PSA (metoda pravděpodobnostního hodnocení bezpečnosti).

Při aplikaci metod v praxi si je třeba uvědomit, že výše uvedené jednotlivé metody byly stanoveny pro konkrétní případy: FMEA 1949; HAZOP 1960; FTA 1961; HRA – 1979 po Three Mail Islands; FMECA 1980. Základní chyba v praxi je, když se metody použijí tam, kam se nehodí, tj. sledovaný proces má jiný procesní model nebo je v jiném prostředí než pro jaké byla metodika odvozena, tj. nejsou splněny podmínky transferu technologií [3,64].

Z kritické analýzy logiky výše uvedených metod vyplývá, že kromě metody What, If, ostatní metody závisí na procesu realizace rizika – základní formální postup je sice stejný, ale konkrétní dopady a kritéria rozhodování jsou dané procesem. Procesy realizace rizika závisí na konkrétních místních podmínkách, např.:
- jak jsou uspořádané činnosti v zařízení,
- jak jsou umístěné tlakové nádoby,
- jak je dlouhé potrubí, které se poruší,
- jakou odolnost má most,
- jakou konstrukci má vysoký dům,
- jak je ukotven tunel v geologickém prostředí,
- jaké je podloží (skalnaté, zemité…),
- jaká skupina lidí je v místě (děti, senioři, handicapovaní, nemobilní….) atd.

V praxi jsou používány procesní modely lineární, stromové, síťové a nestrukturované [2,9]:

1. Na lineárních modelech jsou založeny metody: Check list (kontrolní seznam); Safety audit (bezpečnostní kontrola); Human Reliability Analysis – HRA (analýza lidské spolehlivosti).
2. Na stromových modelech jsou založeny metody: Preliminary Hazard Analysis – PHA; Quantitative Risk Analysis – QRA; Hazard Operation Process – HAZOP; Event Tree Analysis – ETA; Failure Mode and Effect Analysis – FMEA; Failure Mode, Effect and Criticality Analysis – FMECA; Fault Tree Analysis – FTA; Probabilistic Safety Assessment – PSA).
3. Na síťových modelech s použitím metod operační analýzy jsou založeny metody: PERT, GERT, Petriho sítě, Baysovské sítě atd.
4. Pro nestrukturované procesy je třeba použít více kritérií, aby se postihlo více nesourodých aktiv, vnitřních vazeb a spřažení. Pro jejich použití v praxi se vytváří systémy pro podporu rozhodování (DSS – Decision Support System). Při jejich tvorbě a aplikaci se používají:

- poznatky a data od expertů, kteří znají technické parametry, limity a podmínky technického díla a místní zranitelnosti,
- princip teorie maximálního užitku [65], tj. „čím větší, tím lepší“, anebo „čím větší, tím horší“.

Z pohledu logiky metod je zřejmé, že hlavní nevýhoda stromových modelů je ve skutečnosti, že zdroj poruchy, nehody či havárie vychází z jednoho bodu, což pochopitelně neplatí v případě externích nebo úmyslných zdrojů rizik. Použití každé specifické metody je možné jen tehdy, když se ověřením zjistí, že jsou splněny podmínky transferu technologií [3,17,64]. Jinak se metoda musí přizpůsobit místním podmínkám. Je třeba si uvědomit, že přizpůsobení metody na konkrétní podmínky nemohou udělat specialisté z oblasti informačních technologií, ale techničtí experti, kteří znají technické parametry, limity a podmínky technického díla a místní zranitelnosti.

4.2.3.1. Stručná charakteristika vybraných tradičních metod

K údajům uvedeným v [9,15,66] připojujeme dále další poznatky. Analýza toho, co se stane, když, ***What, If*** je postup na hledání možných dopadů vybraných provozních situací. Technika „Co se stane, když …“ je přístup spontánní diskuse a hledání důsledků. Skupina zkušených lidí dobře obeznámených s procesem klade otázky nebo vyslovuje úvahy o možných nežádoucích událostech. Není to vnitřně strukturovaná technika jako některé jiné (např. HAZOP a FMEA). Namísto toho po analytikovi požaduje, aby přizpůsobil základní koncept určitému účelu. Dosud bylo publikováno málo teoretických údajů a informací o metodě „Co se stane, když …“ a jejím použití. Přesto je v průmyslu často používána v téměř každém stádiu průběhu procesů a má dobrý zvuk mezi ostatními technikami. Analýza „Co se stane, když …“ povzbuzuje tým hledající zdroje rizika k přemýšlení nad otázkami, které jsou uvedeny vazbou „*co se stane,*“:

- když se čerpadlo A zastaví při najíždění,
- když operátor otevře ventil A místo ventilu B.

Může však být vyslovena jakákoliv úvaha, i když to není otázka; např. lze uvažovat o možném dodání nesprávné látky nebo nesprávného množství látky do probíhajícího technologického procesu.

Zapisovatel obvykle zaznamenává všechny otázky. Potom jsou otázky rozděleny podle jednotlivých zkoumaných oblastí (vztahujících se obvykle k příslušným dopadům), jako jsou elektrická bezpečnost, požární ochrana nebo bezpečnost personálu. Každá oblast je následně zkoumána jedním nebo více odborníky. Otázky jsou formulovány na základě zkušeností a aplikovány na existující nákresy a popisy procesů. U sledovaného procesu mohou vyšetřování zahrnovat i rozhovory s personálem, který není zastoupen v týmu pro hodnocení zdrojů rizika (nepřijatelných dopadů). Není stanoven žádný pevný vzor, nebo pořadí pro takové otázky, ledaže vedoucí týmu provede logické rozdělení procesu do funkčních částí. Otázky se mohou týkat jakýchkoli zvláštních podmínek vztahujících se k procesu, tj. nejen selhání komponent nebo odchylek procesu.

Účelem analýzy „Co se stane, když …“ je identifikovat zdroje rizika, nebezpečné situace nebo určité nehodové události, které mohou způsobit nežádoucí dopady. Zkušený tým lidí odhaluje možné nehodové situace, jejich dopady a existující bezpečnostní opatření. Poté navrhuje alternativy na snížení rizika. Metoda může zahrnovat vyšetřování možných odchylek od projektu, realizace stavby, modifikace nebo

provozního záměru. Vyžaduje základní porozumění účelu procesu a schopnost rozumně kombinovat možné odchylky od zamýšleného účelu, které mohou vést k nehodě. Pokud je personál zkušený, je to účinná procedura. Jinak ale výsledky budou pravděpodobně neúplné.

Ve své nejjednodušší formě se při použití techniky „Co se stane, když …“ vytváří seznam otázek a odpovědí spojených s procesem. Může také vést k tabulkovému seznamu nebezpečných situací (bez nějakého řazení nebo kvantitativních dopadů odhalených možných nehodových scénářů), k seznamu jejich ochrany proti dopadům a k seznamu možných návrhů na snížení rizika. Protože analýza „Co se stane, když …“ je přizpůsobivá, může být prováděna s využitím libovolných informací a znalostí o procesu v jakékoliv fázi jeho života. K provedení analýzy jsou pro každou oblast procesu přiděleni dva až tři lidé, ale větší tým je lepší. Větší skupina se hodí pro složitý proces. Pokud se proces rozdělí na menší části, pak lze menší skupinu po delší dobu využít pro celý proces. Doba a náklady pro analýzu „Co se stane, když …“ jsou úměrné složitosti procesu a počtu analyzovaných oblastí [9].

Standardní model pro identifikaci dopadů pohrom, tj. důsledků realizace rizik ve vybraném technickém díle, objektu či území metodou What, If spojených s pohromou se provádí vyplněním tabulky 5, která byla úspěšně odzkoušena v praxi [15,63]. Pro technické dílo je předmětný standardní model doplněn o prioritní / kritická aktiva technického díla. Vyplnění tabulky provádí expertně; výjimečně jeden expert, obvykle více expertů s použitím metod brainstorming, brainwriting, panelová diskuse, delfská metoda či vícestupňová delfská metoda [9,15].

Tabulka 5. Standardní model pro aplikaci metody What, If pro potřeby řízen bezpečnosti entit.

Aktivum		**Možné dopady pohromy na aktivum**
Životy a zdraví lidí		
Bezpečí lidí		
Majetek		
Veřejné blaho		
Životní prostředí		
Infrastruktury a technologie		
	Dodávky energií	
	Dodávky vody	
	Kanalizace	
	Přepravní síť	
	Komunikační a informační sítě	
	Bankovní a finanční sektor	
	Nouzové služby	
	Základní služby v území (průmysl, zemědělství, zásobování, zdravotnictví, likvidace odpadů, sociální služby, pohřební služby)	
	Státní správa a samospráva	

Prioritní zařízení, komponenty, vazby a toky v technickém díle ……	

Jelikož při aplikaci metody „Co se stane, když …“ se často používá brainstorming a k němu software (např. program *Mind Manager*), který lze volně stáhnout z internetu, tak si je třeba uvědomit, že každý problém má svá specifika a ta počítačový program, který byl odvozen pro jisté podmínky, nemusí respektovat; viz požadavky na transfer technologií [64].

Kvantitativní analýza rizik ***QRA*** je založena na skutečnosti, že je znám stromový model procesu vzniku havárie a prostředí, ve kterém jsou dopady [9]. Aplikace v oblasti chemických technologií je prosazovaná v souvislosti s direktivou EU Seveso zahrnuje následující kroky: definice QRA; popis analyzovaného systému; identifikace a popis zdrojů ohrožení; identifikace scénářů nehod / havárií; výběr reprezentativních scénářů nehod / havárií; sestavení modelu QRA; odhad dopadů nehod / havárií; odhad pravděpodobností výskytů nehod / havárií; odhad velikosti ohrožení a s ním související velikost rizika; hodnocení a prezentace rizika. Jednotlivé kroky znamenají:

1. Definice QRA převádí požadavky uživatele analýzy ohrožení na cíle studie a na její naplánování. Rozsah opatření plynoucí z analýzy rizika a formáty prezentace rizika se vyberou po určení celkového rozsahu činností pro QRA. Následuje stanovení hloubky studie založené na definovaných cílech a na dostupných zdrojích. Rovněž jsou uvažovány potřeby pro specifické studie v rámci QRA (např. zhodnocení domino efektů, poruchy či selhání výpočetního systému, poruchy ochranného systému apod.). Definování QRA končí stanovením specifických informačních požadavků studie tak, aby mohla být vytvářena databáze údajů pro analýzu. Zde je třeba připojit velmi důležitou poznámku. Žádná bezpečnostní šetření na jakékoli úrovni (kvalitativní, semikvantitativní nebo kvantitativní, klasifikační nebo velmi podrobná) nejsou zbytečná, pokud se všechna potřebná data zaznamenají do vytvořené a neustále doplňované databáze. Všechny informace z jakýchkoliv dostupných databází o chemických látkách, technologických zařízeních a jejich spolehlivosti, měřeních a regulacích, haváriích (jejich příčinách, průběhu a výsledcích jejich vyšetřování), údaje geografické, hydrologické a klimatologické atd. jsou dobré; všechny ty informace, které shromáždí provozovatel, konzultant nebo bezpečnostní analytik do databáze pro analýzu konkrétního zařízení a jeho vlivu na okolí jsou nejlepší.
2. Popis analyzovaného systému je shromáždění informací o analyzovaném procesu a/nebo podniku potřebných pro analýzu ohrožení a identifikaci s ním spojených rizik. Např. informace o lokalitě, o přírodních poměrech, počasí a podnebí, diagramy procesních toků, diagramy potrubí a instrumentace (P&ID), nákresy rozvržení zařízení, instrukce pro provoz a údržbu, technologická dokumentace, chemismus procesu, látková a enthalpická bilance procesu apod. Tyto informace se shromažďují do databáze analýzy pro pozdější použití při vlastní analýze ohrožení a s ním souvisejícího rizika.
3. Identifikace a popis jednotlivých ohrožení je první rozhodující krok QRA. Vynechaný zdroj rizika nemůže být analyzován. Existuje mnoho pomůcek pro určení zdrojů ohrožení, např. využití zkušeností, inženýrských klasifikací, kontrolních seznamů, detailních znalostí o procesu, zkušeností s poruchami zařízení. Existují

indexové techniky pro klasifikaci zdrojů ohrožení (DOW indexy), analýza „Co se stane, když …“ (v originálu „What…,if…“), technika identifikace zdrojů ohrožení a provozuschopnosti (HAZOP), analýza způsobů poruch a jejich dopadů (FMEA), předběžná analýza zdrojů ohrožení (PHA).

4. Identifikace scénářů nehodových událostí je identifikace a tabulková úprava všech možných nehodových událostí bez ohledu na jejich důležitost nebo iniciační událost. Je to druhý rozhodující krok, protože vynechaná nehodová událost nemůže být analyzována.
5. Výběr reprezentativních scénářů nehodových událostí je proces, pomocí kterého se podobné nehodové události sdruží do jednoho zástupce, který reprezentuje skupinu podobných nehodových událostí. V tomto kroku se také určí koncové stavy scénářů a rovněž fyzikální projevy koncových stavů scénářů.
6. Sestavení modelu QRA zahrnuje výběr vhodných modelů dopadů, metod odhadu četností a pravděpodobností a jejich integraci do souhrnného algoritmu tak, aby byl získán a prezentován odhad rizika studovaného systému.
7. Odhad dopadů je metodologie používaná pro stanovení možných škod od jednotlivých nehodových událostí. Jednotlivá nehodová událost (např. prasknutí tanku s hořlavým plynem zkapalněným tlakem) může mít více odlišných koncových stavů (např. exploze neohraničeného mraku par (UVCE), exploze rozpínajících se par vroucí kapaliny (BLEVE), pomalejší vyhoření apod.). Tyto koncové stavy jsou analyzovány užitím zdrojových a rozptylových modelů a modelů explozí a požárů. Modely dopadů jsou následně použity pro stanovení dopadů na lidi, zvířata, majetek a životní prostředí. Činnosti jako ukrytí nebo evakuace mohou snížit rozsah dopadů a proto se též zahrnují do analýzy.
8. Odhad pravděpodobností je metodologie používaná pro odhad četnosti nebo pravděpodobnosti výskytu nehodové události. Odhady mohou být získány z historických dat o četnostech poruch nebo z historických dat o četnostech nehodových událostí. Pomocnými nástroji zde jsou stromy poruch (FTA) a stromy událostí (ETA). Ve většině systémů se musí uvažovat faktory poruch se společnou příčinou (jediný faktor vedoucí k současnému selhání více než jednoho systému, např. výpadek dodávky medií nebo energií, lidská chyba, externí události).
9. Odhad ohrožení kombinuje ocenění dopadů a pravděpodobností všech koncových stavů scénářů všech vybraných nehodových událostí pro stanovení míry rizika. Ohrožení všech vybraných nehodových událostí jsou jednotlivě odhadnuta a sumarizována za účelem obdržení výsledné míry ohrožení a s ním souvisejícího rizika analyzovaného provozu. Měly by se vyhodnotit citlivosti a neurčitosti odhadů rizika a důležitosti různých přispívajících nehodových událostí.
10. Zhodnocení a prezentace ohrožení je proces, pomocí kterého se využijí výsledky analýzy ohrožení s cílem učinit rozhodnutí o opatřeních ať už relativním srovnáním strategií snižování rizika, nebo srovnáním specifických cílů.

Metoda má 4 hlavní fáze: identifikace jevu, který znamená ohrožení; odhad četnosti výskytu tohoto jevu; vyhodnocení dopadů havárie; výpočet individuálního a společenského rizika.

Analýza poruch a jejich dopadů ***FMEA*** je postup založený na rozboru způsobů vzniku poruch a jejich důsledků, který umožňuje hledání dopadů a příčin na základě systematicky a strukturovaně vymezených poruch zařízení. Metoda je vyvinuta pro analý-

zu poruch a jejich dopadů. Slouží ke kontrole jednotlivých prvků projektového návrhu systému a jeho provozu. Představuje procesní model tvrdého, určitého typu [8], kde se předpokládá kvantitativní přístup řešení. Využívá se především pro vážná rizika a zdůvodněné případy. Vyžaduje aplikaci počítačové techniky, speciální výpočetní program, náročnou a cíleně zaměřenou databázi. Zkušenosti s metodou FMEA jsou největší v různých ekonomických sektorech včetně leteckého a automobilového průmyslu, v sektoru obrany apod. Metoda FMEA formálně vyžaduje adaptaci pro konkrétní požadavky a odvětví (úpravu softwaru a vybavení databáze).

Při analýze FMEA je vytvářena tabulka způsobů poruch zařízení a jejich dopadů na systém nebo podnik. Poruchový stav popisuje, jak zařízení selže (v otevřené poloze, zavřené poloze, v chodu, ve vypnutém stavu, únik, atd.). Dopad způsobené poruchy je určen reakcí systému na selhání zařízení. FMEA identifikuje jednoduché způsoby poruchy, které buď přímo vedou k nehodě, nebo k ní významně přispějí. Chyby člověka-operátora obvykle nejsou vyšetřovány přímo pomocí FMEA, nicméně dopady špatné funkce jako výsledek lidské chyby jsou obvykle indikovány nějakým způsobem poruchou zařízení. FMEA není účinná pro identifikování vyčerpávajícího seznamu kombinací poruch zařízení, které vedou k nehodám.

Účelem FMEA je identifikovat způsoby poruch jednotlivého zařízení a systému a potenciální dopad nebo dopady každého způsobu poruchy na systém nebo podnik. Tato analýza typicky vytváří doporučení pro zvýšení spolehlivosti zařízení a tím také pro zlepšení bezpečnosti procesu. FMEA vytváří kvalitativní, systematický seznam odkazů na zařízení, způsoby jeho poruch a jejich dopadů. Součástí je i vyhodnocení dopadů nejhoršího případu plynoucího z jednotlivých poruch. FMEA může být snadno aktualizována po změnách v projektu nebo systému podniku. Výsledky FMEA jsou obvykle dokumentovány v tabulkové podobě. Analytik obyčejně uvede návrhy pro zlepšení bezpečnosti u příslušných položek v tabulce. Analýza FMEA vyžaduje následující zdroje dat a informací:

- seznam zařízení systému nebo podniku nebo P&ID,
- znalost funkcí zařízení a způsobů poruch,
- znalost funkcí systému nebo podniku,
- znalost odezev na selhání zařízení.

Analýzy FMEA mohou být prováděny jedním analytikem, ale takové analýzy by měly být revidovány dalšími odborníky, aby byla zajištěna úplnost. Požadavky na personál se mohou různit podle velikosti a složitosti položek zařízení, které se mají analyzovat. Všichni analytikové zapojení do FMEA by měli být obeznámeni s funkcemi zařízení a způsoby poruch a s tím, jak mohou poruchy ovlivnit ostatní části systému nebo podniku. Doba a náklady analýzy FMEA jsou úměrné velikosti procesu a počtu analyzovaných komponent. V průměru je jedna hodina dostatečná doba pro analýzu dvou až čtyř položek zařízení. Stejně jako při jakékoli studii hodnocení zdrojů rizika systémů s podobným zařízením, které vykonává podobné funkce, je potřebná doba výrazně zkrácena díky opakující se povaze těchto hodnocení [9].

Analýza dopadů selhání a jejich kritičnosti ***FMECA*** je základním nástrojem pro hodnocení návrhu systému v počátečním stádiu tvorby s ohledem na spolehlivost [8]. Skládá se z: popisu systému, tj. jsou identifikovány komponenty systému vystavené selhání; identifikace módů selhání, tj. v pozorovatelném způsobu, kterým je identifikovaná komponenta, která selhala; určení příčin selhání či určení pravděpodobné příčiny selhání; hodnocení dopadů selhání, tj. je hodnocen dopad každého selhání na provoz systému; klasifikace závažnosti dopadů, tj. stupeň závažnosti je přiřazen

ke každému módu selhání – obvykle se používají 4 stupně - katastrofický, kritický, mezní a zanedbatelný; odhad pravděpodobnosti výskytu selhání, stanovení indexu kritičnosti, tj. kvantitativní míry kritičnosti módu selhání, ve které se kombinuje pravděpodobnost výskytu módu selhání a jeho změna krutosti a určení korekčních činností – korekční akce jsou určeny a oklasifikovány dle důležitosti v závislosti na módech selhání s největšími hodnotami indexu kritičnosti a třídy krutosti. Úplnost analýzy a hodnocení závisí na tom, jaké zdroje selhání připustíme, zda jen vnitřní nebo také vnější, zda a jak lidský faktor a na schopnosti rozlišovat detaily v případě zvolené hodnotové stupnice.

Kontrolní seznamy jsou základním nástrojem řídících pracovníků, protože přehledným způsobem odhalují rizika v oblastech, které jsou dobře poznané a pro které jsou během vývoje poznání a zkušenostmi stanovené mantinely jednotlivých činností, dějů, chování apod. Je zřejmé, že pro zajištění bezpečnosti a rozvoje je třeba odstranit bezprostřední, zřejmá a poznatelná rizika, pro jejichž identifikaci dobře poslouží kontrolní seznamy a pak věnovat úsilí rizikům, která jsou skrytá v řetězcích možných událostí, v čase zpožděná či bez použití specifických prediktivních metod a specifických a kvalifikovaných datových souborů téměř nezjistitelná.

Analýza kontrolním seznamem je proměnlivá metoda. Typ ohodnocení takto získaný se může měnit: technika může být rychle použita pro jednoduchá vyhodnocení nebo pro nákladnější podrobnější výsledky. Je to úsporný způsob jak identifikovat tradičně rozpoznatelné zdroje rizika.

Pozornost je soustředěna na všechny úseky řízení bezpečnosti, tj. prevenci, připravenost, odezvu a obnovu. Kvůli potřebám krizového řízení, které vyžaduje dobře vzdělané a vycvičené výkonné složky, je řada kontrolních seznamů zaměřena na kontrolu, zda byly dodrženy metodiky zásahů či jiné instrukce, které jsou pro zásah důležité. Dle [66] jsou kontrolní seznamy pro:

- zjišťování kritičnosti u položek spojených s majetkem v území,
- pro úroveň zajištění obnovy majetku v území,
- zjišťování nedostatků, které musí být odstraněny z důvodu zajištění bezpečnosti při provozu či při obnově majetku po živelních či jiných pohromách,
- zjišťování stavu řízení pohrom v území ze strany správce území (veřejné správy),
- hodnocení stavu nakládání s nebezpečnými látkami,
- zjišťování úrovně podpory direktivy Seveso,
- ocenění ztrát v území po pohromě,
- úroveň zajištění bezpečnosti a udržitelného rozvoje území,
- kontrolu kompletnosti nouzových plánů obcí – pohled na problém 1,
- kontrolu kompletnosti nouzových plánů obcí – pohled na problém 2,
- zjišťování stavu nouzové připravenosti v území,
- zjišťování souladu nouzové připravenosti s požadavky legislativy,
- posouzení úrovně ochrany proti požáru,
- posouzení úrovně bezpečnosti provozů s nebezpečnými látkami,
- posouzní úrovně práce výkonných složek,
- posouzení bezpečnosti na staveništích,
- posouzení úrovně souladu zájmů veřejného a soukromého sektoru u PPP projektů.

Pravděpodobnostní hodnocení bezpečnosti ***PSA*** (Probabilisdtic Safety Assessment), někdy též PRA (Probabilistic Risk Assessment) zjišťuje a propojuje události, které vedou k vážné havárii, určuje jejich pravděpodobnost výskytu a stanovuje jejich následky. Poté stanovuje pořadí předmětných kombinací událostí dle závažnosti. Prv-

ním krokem je analýza technického díla a sběr relevantních dat o chování technického díla. Poté identifikuje iniciační události (možné pohromy) a s nimi spojené stavy poškození zařízení technického díla. Poté se pomocí stromu událostí modeluje řetězec událostí a jejich důsledků pro zařízení a komponenty technického díla. Výsledkem jsou údaje dokumentující spolehlivost systémů a komponent. Je si třeba uvědomit, že vychází z předpokladu, že to, co je spolehlivé, to je bezpečné. Tím je v rozporu s premisou této publikace, založené na současném poznání; podrobné vysvětlení je v práci [4].

4.2.3.2. Tradiční metody a jejich použitelnost při práci s riziky technických děl

Při stanovení rizik je základní aktivitou určení ohrožení, které představuje pohroma / škodlivý jev pro technické dílo. V případě technických děl se často používají k danému cíli techniky HAZOP, FMECA, FTA, ROA (Recursive Operability Analysis, která je méně časově náročná než FTA) [9]. V uvedených případech jde o strukturované procedury – organizované přes výrobní proces. Při identifikaci rizik se vyhodnocení škod provádí deterministicky a odhad četnosti výskytu pravděpodobnostně. Právě zaměření na sledování výrobního procesu nedovoluje postihnout selhání na více místech z jedné příčiny [43,44,63]. Práce [67] na základě studia rizik v energetickém sektoru ukázala, že právě chyby v modelech při stanovení rizik technických děl vedou k selhání technických děl daleko častěji než chyby ve vstupních datech.

Jelikož většinu rizik nelze odstranit při provozu, leží tíha ochrany technického díla na způsobu řízení bezpečnosti technického díla. Zavádí se pokyny pro provoz při abnormálních situacích: zvážit proměnlivost procesu, tj. odchylky od normálního provozu; příčiny proměnlivosti procesu; důsledky způsobené selháními bezpečnostních funkcí; a ochrana prováděná pomocí: alarmů; zásahu obsluhy; automatickými systémy pro bezpečnost [3].

Dle [68] existuje více než 60 metodik pro analýzu rizik, které umožňují řízení aspektů bezpečnosti průmyslových objektů. Jsou však místně specifické, a proto vždy před jejich použitím je třeba ověřit, zda jsou pro daný případ vhodné. Analýzy havárií [3,4,63] ukazují, že při výskytu vnější pohromy nebo chyby lidského činitele může dojít k poškozením na několika místech objektu současně, což stromy událostí založené na výrobním procesu neodhalí.

V práci [69] byly porovnány výše sledované nástroje a byla stanovena vhodnost postupů při práci s riziky v závislosti na cíli, který je v technickém díle požadován. Výsledek je v tabulce 6. Z tabulky vyplývá, že vždy jsou použitelné metody kontrolní seznam, What, If a jejich kombinace. Ostatní metody lze použít jen v určitých fázích řízení rizik zacíleného na bezpečnost technických děl.

Tabulka 6. Použitelnost nástrojů při práci s riziky technického díla.

Fáze navrhování a provozu	**Kontrolní seznam**	**What If**	**Kombinace What, If a kontrolního seznamu**	**HAZOP**	**FMEA**	**FTA**
Výzkum		X				
Projekt	X	X	X			

Zkušební provoz technického díla	X	X	X	X	X	X
Detailní inženýrské práce	X	X	X	X	X	X
Konstrukce + zahájení provozu	X	X	X			
Rutinní provoz	X	X	X	X	X	X
Modifikace	X	X	X	X	X	X
Vyšetřování nehod a havárií		X		X	X	X
Odstavení z provozu	X	X	X			

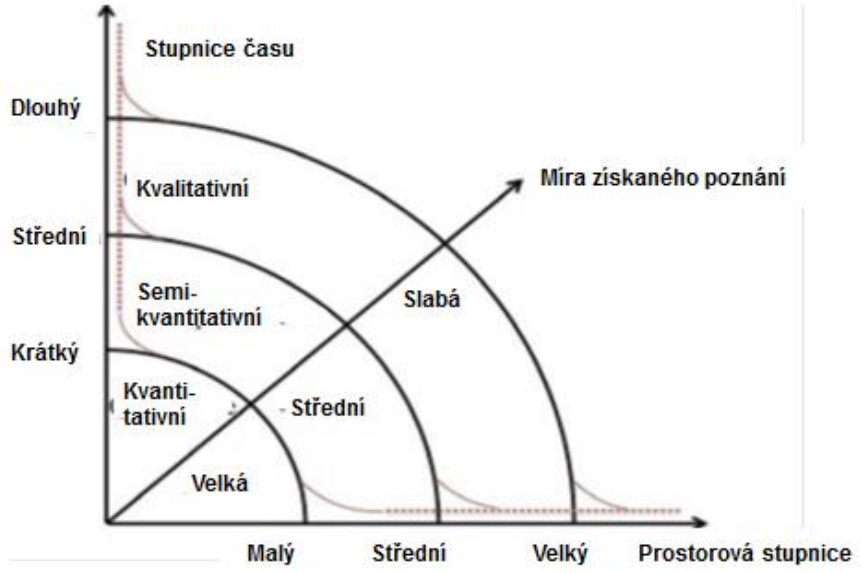
O problémech, které jsou spojené s aplikací stromových modelů, pojednává také práce [70]. Předmětná práce ukazuje, velkým nedostatkem aplikace stromových modelů v bezpečnostních a spolehlivostních studiích technických děl je, že technická díla pokládáme za hierarchicky uspořádaná a neuvědomujeme si předpoklady, které používáme při vytváření struktury modelů (tj. to, co zanedbáváme). Jde o předpoklady:

1. Všechny komponenty jsou vzájemně nezávislé. Zanedbávají se vzájemná propojení trvalá i občasná.
2. Systém má strukturu složenou z několika vrstev, které jsou znázorněny jako strom. Zanedbává se, že každý subsystém či komponenta může mít více stavů.
3. Každá úroveň provozu odpovídá jedné konstelaci podmínek. Zanedbává se, že každá úroveň provozu (od perfektního výkonu po totální selhání) je výsledkem složité kombinace konstelací komponent při reakci na momentální podmínky.
4. Oprava poruchy komponenty je okamžitá. Zanedbává se čas potřebný k identifikaci poruchy a k provedení nápravy.

Z důvodu tohoto zanedbání se pak musí v praxi u technického díla používat zálohy.

Když chceme řídit a vypořádat rizika u inženýrských systémů, musíme pochopit jejich složitost. Jde o spřažené / propojené komponenty (systémy), ve kterých jsou zpětné vazby, smyčky a mnoho činitelů. Jejich chování závisí na podmínkách, které jsou rozmanité, a proto nepředvídatelné. Proto jednoduché modely chování těchto systémů, pro které jsou software, nemají schopnost identifikovat všechna rizika, a to hlavně ta, která jsou málo pravděpodobná.

Práce [71] ukazuje, že míra získaného poznání na základě zpracování dat výsledek hodnocení významně závisí na kvalitě dat, obrázek 6. Předmětný obrázek ukazuje, že pravděpodobnostní hodnocení rizika (PRA) u komplexních systémů není příliš spolehlivé v případech, ve kterých jsou vysoké nejistoty, a to hlavně znalostní (tj. neurčitosti), tabulka 7.



Obr. 6. Pravidla pro výběr metody hodnocení; zpracováno dle [71].

Tabulka 7. Příklad vyjádření nejistot na vstupech; zpracováno dle [71].

Nejistá vstupní veličina	**Výsledek hodnocení**	**Předpoklad**
Perioda opakování povodně	50 let	Srážky vzrostou o 15%
Pravděpodobnost selhání protipovodňových stěn	0.15	Odhad inženýrů
Vyhodnocení rizika	Ztráty 500-600 mil. USD	Podle historických odhadů.
Náklady na obnovu	Podle log-normálního rozdělení jsou v intervalu 7 – 45 USD	Ceny materiálů budou mít dnešní hodnotu.

4.2.3.3. Doplňující údaje k tradičním nástrojům práce s riziky

Specifické metody pro kvantitativní analýzu rizik dle práce [9] jsou např. CRAMM; Metodika @RISK; Metodika RiskPAC; RiskWatch; ETBA; DMEA; ECFC; EEA; THERP; STEP; RBCA; PSHA; FRAP. Software používaná v ČR při analýze a hodnocení rizik jsou souvislosti s nebezpečnými látkami ROZEX; ALOHA; WHAZAN; EFECT; TerEx.

Pro projektování budov, technických děl a infrastruktur existuje v praxi dle [9] mnoho dalších nástrojů, které mají obvykle softwarovou podporu, např. RMPlanner (ABS Group Inc.), HazardReview (ABS Group Inc.), Risk Radar (American Systems Corporation), FaultrEASE (Arthur D. Little, Inc.), Cegis FaultrEASE (Arthur D. Little, Inc.), AgRisk (Ohio State University), SiteSafe (BMS Solutions Pty Ltd), BOSS (BOSS International), DNV Risk Management Software, EquIS – Environmental Quality Information System (USA, UK, Austrálie), RBCA (Groundwaterservices Inc.), MARS 1 (Holandsko, Kanada), ISEC (ISEC Inc.), LABTECH (LABTECH Ltd.), HACCP (M-Tech International, Inc.), HAZMAN (PLG Inc.), RISKMAN (PLG Inc.), PSM (Prima-

tech Inc.), RAC (US Dept. Of Defense), PRISM (US Dept. of Defence), HIRApac (Risiko Pty Ltd.), RiskAdvisory (RiskAdvisory Software Inc.), PHA-Pro (Riska, Reliability, and Safety Engineering Inc.), RiskTrak a RiskManage (Risk Services and Technology), RiskwarePro (Sekmart Ltd.), Risk Monitor (Lawrence Livermoore Lab.), DDMT (RMRI Ltd.), POTW (Sabre Systems Inc.), CHAMPS (SPS Ltd.), SAPHIRE (US INEL), SCIENTECH (SCIENTECH Inc.), CERT a OCTAVE (Carnegie Mellon University), SSESCO (SSESCO Inc.), SRI (Subterranean Research Inc.), FRAC-EXPLORE (US Dept. of Energy), GEMS a UCSS (US EPA), SADA (University of Tennessee) atd.

4.3. Rizika SoS a jejich řízení

Problém výběru metod nastává u SoS. V praxi sice je testována řada metod, jak uvádí např. práce [17,20]. Z metodického pohledu řízení rizik SoS představuje koordinaci řady nesourodých procesů, které probíhají současně v různých oblastech a některé jejich výsledky se vzájemně podmiňují, tj. procesy jsou jistým způsobem na sobě závislé, tj. zvládnutí úkolů spojených se zajištěním bezpečnosti je určováno usměrněním opatření a činností v různých částech SoS. Z pohledu daného cíle je nutné, aby každý řídící orgán SoS chápal každý problém v existujících souvislostech a hledal jeho efektivní řešení v daných podmínkách s ohledem na další systémy, přitom postupoval racionálně a s ohledem na náklady a dostupné zdroje v příslušných oblastech. Uvedené požadavky jsou základním principem SMS pro SoS.

Na základě recentních poznatků a dlouholetých zkušeností s řešením složitých praktických úkolů, při kterých bylo nutno použít praktiky dobré inženýrské praxe, autorka sestavila návrh nástroje na identifikaci a řízení rizik SoS a pro podporu jeho aplikace v praxi jsou uvedeny výsledky testů na reálných datech. Proto na základě znalostí a zkušeností s navrhováním systémů pro podporu rozhodování [2,7,9] byl logickou syntézou údajů a zkušeností navržen komplexní nástroj pro identifikaci, analýzu, hodnocení a řízení rizik, včetně průřezových, který zaručuje přežití či kontinuitu aktiv při kritických pohromách. Z důvodu důležitosti je popis předmětného nástroje uveden v kapitole 5.

Na základě zkušeností z praxe [63] při práci s rizikem a zranitelností, a to především při hodnocení u technických děl, existují omezení:

- metody jsou příliš obtížné při užívání a chápání,
- pojmy a koncepty nejsou jednotné a často se překrývají,
- podpory informačních technologií jsou špatně strukturované,
- uživatelé mají omezené znalosti a schopnosti pracovat např. s informačními technologiemi,
- provedení hodnocení je časově náročné a je i náročné na data,
- procesy hodnocení na sebe nenavazují,
- vedení technických děl se neřídí výsledky hodnocení rizik.

Vzhledem k povaze SoS, kterou mají technická díla, dále uvádíme principy rozhodování i postupy používané v praxi.

4.3.1. Rozhodování složitých problémů

Na základě údajů uvedených v [9] při strategickém řízení se při rozhodování obvykle používá teorie užitku (utility), která je založená na hodnocení variant podle kritérií. Při střednědobém rozhodování se obvykle používají kvantitativně orientované teorie rozhodování založené na aplikaci matematických modelů a metod, především z operační analýzy, teorie her a rozhodovací analýzy (vytváří se DSS). Při krátkodobém rozhodování (zásahy záchranářů, reakce na nehody apod.) se používají postupy založené na dobré praxi, aby se odstranily rozdíly ve znalostech, schopnostech a zkušenostech rozhodujících subjektů. Pro řešení úkolů praxe spojené s řízením rizik je nejúčinnější oblast první, a proto se ji budeme více věnovat.

Rozhodovací proces dále chápeme jako proces řešení rozhodovacích problémů, tj. problémů s více variantami řešení, a proto hlavním úkolem je posuzování variant a výběr optimální varianty. Problém, který de facto řešíme, spočívá v tom, že existuje odchylka mezi žádoucím a skutečným stavem. Při řešení musíme zvažovat stupeň naléhavosti, reakci na existující ohrožení a na momentální příležitosti a také prevenci, abychom nezpůsobili zbytečné, a hlavně nenapravitelné škody, ztráty a újmy ani dnes, ani v budoucnosti.

Postupy a nástroje rozhodování závisí na: subjektu rozhodování, tj. jednotlivec nebo skupina; času, tj. statické či dynamické, spojité či diskrétní; počtu kritérií - jsou nástroje jedno kriteriální nebo vícekriteriální; míře určitosti, tj. rozhodování za jistoty, nejistoty, nejistoty a neurčitosti; úrovni a závažnosti, tj. strategické, taktické či operativní; dopadech variant řešení a jejich důsledcích; systémové struktuře problému, tj. dobře či špatně strukturovaný; a na možnosti algoritmizace řešení problému. Strukturu rozhodovacích procesů tvoří osm dále uvedených kroků:

1. Identifikace problému, tj. sběr dat; analýza a vyhodnocování informací a znalostí; a identifikace situací, které vyžadují řešení.
2. Analýza a formulace problému, tj. stanovení základních prvků pro rozhodnutí; a určení příčin vzniku problému a cílů jeho řešení.
3. Stanovení kritérií hodnocení pro posuzování a hodnocení variant řešení.
4. Tvorba variant řešení, tj. nalezení a formulace činností vedoucích k řešení.
5. Stanovení dopadů a užitků variant z hlediska vybraných kritérií.
6. Hodnocení variant a výběr varianty určené k realizaci (optimální) nebo preferenční uspořádání variant.
7. Realizace rozhodnutí, tj. implementace vybrané varianty.
8. Monitorování realizace rozhodnutí s ohledem na cíle, tj. stanovení odchylek vzhledem ke stanoveným cílům, příprava a realizace nápravných opatření, korekce cílů, pokud nebyly stanoveny realisticky.

Cíle, ke kterým se vztahuje rozhodování, nemusí být vždy komplementární, tj. vzájemně se doplňující a podporující, ale konfliktní. Zkušenosti z praxe ukazují, že druhý případ je ve sledované oblasti velmi častý; např. kvůli bezpečí a udržitelnému rozvoji nelze zvolit bez náležitých, a to většinou nákladných opatření a činností některé postupy, které mají veliká bezprostřední rizika anebo rizika, která nelze řádně pochopit a ocenit.

Podpora nástrojů informačních technologií pro proces rozhodování je v tom, že pomocí informačních technologií lze uchovávat, třídit, aktualizovat a vyvolávat data,

informace a existující znalosti; a že lze vytvářet DSS, tj. systémy pro podporu rozhodování, což jsou interaktivní aplikace matematických modelů. DSS dělíme na speciální, které jsou šité na míru, tj. poskytují podporu pro řešení specifických problémů; a na obecné, tj. založené na adaptivních a pružných modelech rozhodovacího procesu. V obou případech platí, že nenahrazují subjekt, který rozhoduje, tj. jen poskytují podporu, jako např. generují soubor variant řešení, provádí rozšíření souboru variant, zajišťují urychlení a zpřesnění výpočtu užitků a dopadů variant, kvantifikací rizika atd.

Analýza problému začíná soustředěním informací o problému a jeho specifikací z hlediska 5 základních charakteristik:

CO? – jde o identifikaci objektu, který je nositelem problému: na jakém objektu byla zjištěna odchylka od žádoucího stavu, v čem spočívá?,

KDE? – jde o lokalizaci objektu nebo jeho části, ve které se nachází odchylka,

KDY? - jde o časové určení: kdy byla porucha zjištěna, v jaké fázi životního cyklu, projevuje se stále nebo jen občas, kdy se neprojevuje?,

KDO? – jde o zjištění, jakých osob se problém týká?,

KOLIK? – jde o stanovení rozsahu: jaká část objektu nebo kolik objektů je vadných, jaký je trend?

Poté je třeba zvážit shodné a odlišné rysy problémů, protože shodné problémy lze řešit podobně a opačně. Pro identifikaci odlišných problémů byly vyvinuty speciální nástroje, a to gap analýza a analýza rozdílů [9].

Pro identifikaci neznámých příčin se používají: metoda pokusů a omylů, která není příliš efektivní; postupy, které se osvědčily při řešení podobných problémů v minulosti; a kauzální analýza [9]. Důležité je si uvědomit, že problém lze vyřešit jen tak, že nalezneme příčiny a ty odstraníme nebo alespoň zmírníme jejich dopady a že ho nelze vyřešit, když budeme působit na příznaky, tj. projev problému ve sledovaném subjektu. V tomto případě je třeba srovnat opatření řízení rizik, zásadní je prevence zaměřená na pohromy, která je zaměřená na příčiny a není reakcí na nouzové situace.

V praxi se v kauzální analýze používají dílčí metody jako: diagram příčin a následků (metoda rybí kosti, Ishikawův diagram, Cause-Efect diagram); diagram silového pole (Force Field Analysis, Impact Analysis – šestislovný graf); paretova analýza (pravidlo 80:20); a rozhodovací analýza založená na variantách [9].

Je si třeba uvědomit, že skupinové rozhodování má své přednosti i úskalí. Mezi přednosti při atmosféře spolupráce patří: více informací a znalostí; kombinace různých přístupů a dovedností; širší spektrum přístupů k řešení problému; lepší pochopení problému; vyšší přijatelnost řešení; a stimulace myšlení. Mezi úskalí patří: vyšší časová náročnost; dominance některých členů skupiny a podřízenost jiných členů; prosazování preferované varianty; zamlčování nesouhlasu a preference konsensu, tj. místo hledání nejlepší varianty snaha dosáhnout shody; skupinové myšlení, tj. nadměrná loajalita a cenzurování; možnost „nákazy“ chybami jiných členů skupiny; možnost vyloučení inovativních řešení hlasováním; a zvýšený sklon k riziku. Proto již dnes existují postupy, jak tento způsob rozhodování provádět (Fiedlerův kontingenční model, model Vertical Dyad Linkage – VDL, model Vrooma a Yettona atd.) [9].

V praxi se používají při rozhodování dále uvedené nástroje: rozhodovací matice; pravidla – očekávaná hodnota, pravidla minimax, maximax, Laplace, Hurwicz, Savage;

pravděpodobnostní stromy; a rozhodovací stromy [9]. Speciální problematiku tvoří více etapové rozhodovací procesy, ve kterých je základním krokem vymezení etap rozhodovacího procesu a zachování provázanosti opatření a činností během celého procesu.

V případě rozhodování v praxi je obvykle třeba uplatnit více kritérií, která jsou různorodá. Zřídka existuje jedna varianta, která je nejlepší podle všech kritérií. Častěji některé varianty jsou lepší z některých hledisek, z jiných horší (konfliktní kritéria, např. ekonomická efektivnost vs. dopady na životní prostředí). Někdy je možný postup, že se provede převod všech kritérií na stejnou měrnou jednotku (nejčastěji peníze), za možnosti aditivity převedeme vícekriteriální hodnocení na jedno kriteriální hodnocení. Někdy to však nejde, a pak je třeba použít vícekriteriální hodnocení, jehož cílem je preferenční uspořádání variant, které vychází ze stanovení vah jednotlivých kritérií a z vícekriteriálního hodnocení variant. Ke stanovení vah kritérií se používají: bodová stupnice; alokace 100 bodů; preferenční uspořádání kritérií podle významnosti kritérií; párové srovnávání; Saatyho metoda; postupný rozvrh vah; a kompenzační metoda [9].

Metody hodnocení variant jsou: vícekriteriální funkce utility (MUT); jednoduché metody stanovení utility variant (např. metoda váženého pořadí, lineární dílčí funkce užitku, metoda bazické varianty, metoda PATTERN – modifikace metody bazické varianty); párové srovnávání variant (Saatyho metoda, metody založené na prazích citlivosti); kompenzační metoda (nevyužívá vah kritérií; je založena na iteračním procesu od nejhorší varianty k nejlepší); a praktické uplatnění metod vícekriteriálního hodnocení.

Pro správné rozhodování je nutný správný proces rozhodování. Pokud je pravidel příliš mnoho, může se proces zhroutit pod vlastní vahou. Pokud dojde ke zpomalení procesu, lze často najít jednu z následujících tří příčin: nejasné stanovení rozhodovací pravomoci; pokud si myslí více lidí, že odpovídají za určité řešení, dojde mezi nimi k přetahování; stejně škodlivý je opačný případ, kdy za důležitá rozhodnutí není nikdo odpovědný; pokud má příliš mnoho lidí schvalovací pravomoc (právo veta), pak to obvykle znamená, že rozhodnutí nemohou být prosazena do dostatečné hloubky; a pokud je „poradců“ příliš mnoho, znamená to obvykle, že příspěvek alespoň některých z nich není důležitý.

Pro rozhodování a výkonnost subjektu je zásadní schopnost přijímat správná rozhodnutí a rychle je realizovat. Proto je nutné aplikovat následující principy:

- některá rozhodnutí jsou důležitější než jiná (nejdůležitější jsou ta rozhodnutí, která jsou zásadní pro vytváření hodnot. Mohou to být důležitá strategická rozhodnutí, ale také kritická provozní rozhodnutí důležitá pro každodenní efektivní chod subjektu),
- cílem každého rozhodnutí je činnost /akce. Dobré rozhodování nekončí přijetím rozhodnutí, ale jeho realizací. Cílem by neměl být konsensus, který se často stává překážkou akce, ale získání lidí k činnosti / akci,
- nejednoznačnost rozhodnutí je nežádoucí. Je nutné určit jasnou odpovědnost (kdo zajišťuje vstupy, kdo rozhoduje a kdo rozhodnutí provede? Pokud není odpovědnost jasně stanovena, je pravděpodobným výsledkem zaseknutí procesu nebo zpoždění),
- důležitá je rychlost a adaptabilita. Organizace, která rozhoduje rychle, může rychleji reagovat na příležitosti a překonávat překážky. Nejlepší rozhodovatelé vytvářejí prostředí, v němž lidé společně přijímají rychlá a účinná řešení; rozhodovací role jsou důležitější než organizační schéma. Žádná organizační struktura není

dokonalá pro všechna rozhodnutí. Klíčové je zapojit ve správný čas správné lidi na správných místech v organizaci,
- jasné stanovení rolí je kritické, ale není postačující. Pokud organizace neprosazuje správné přístupy k rozhodování prostřednictvím motivačních systémů, informačních toků a kulturou, pak se správné rozhodovací postupy nestanou normou,
- zapojení lidí je důležitější než kázání. Zapojte ty, kteří budou řešení realizovat, do jeho návrhu. Pokud se účastní vypracování řešení, budou motivováni k jeho realizaci; je třeba objektivně stanovit, kde se vytváří hodnota, a podle toho přiřadit rozhodovací role. Pro eliminaci sporů mezi funkcemi je důležitější než přesun odpovědností mezi útvary zajištění toho, aby lidé s důležitými informacemi je mohli sdílet; a rozhodovatel je samozřejmě důležitý, ale mnohem důležitější je vybudování systému, který efektivní rozhodování podporuje a dělá z něj pravidlo. Příčiny špatných rozhodnutí jsou chyby v myšlení, které tkví v přehánění či v přeceňování určitých stránek problému; chyby vedení, tj. špatné řízení, špatná motivace a realizace rozhodnutí; a chyby kultury, tj. v organizačním prostředí.

Z formálního hlediska jsou dva typy rozhodování:
- empiricko-intuitivní, které se opírá o odborné znalosti, zkušenosti a logický úsudek subjektu provádějícího rozhodnutí,
- exaktní, které je založeno na využití matematických modelů a algoritmů a vyžaduje formalizaci celého rozhodovacího procesu.

Zásady racionálního rozhodování jsou: hodnocení situace; identifikace kritických problémů; specifikace řešení; rozhodnutí; implementace rozhodnutí; monitorování a zpětné vazby pro poučení pro příště. V nových případech je často nejasná situace, tj. chybí jasné a uspořádané situace. Proto je třeba kombinovat racionální přístup s intuitivním. Racionální přístup stanoví rámec činností, tj. zajistí, že: na nic nezapomeneme; se vyhneme příčinám špatných rozhodnutí; a používáme nejvhodnější techniky. Intuitivní přístup přináší inspiraci, vhled a instinkt, které jsou potřebné k identifikaci optimálních řešení

Rozhodování v zájmu věci rozhodování, které se provádí v rámci řízení věcí veřejných, musí být objektivní a kvalifikované. Rozhodování lze rozdělit do několika typů podle míry informovanosti o tzv. základních prvcích rozhodování na:
- rozhodování za jistoty (jsou známy všechny základní prvky rozhodování),
- rozhodování za nejistoty, při kterém jsou známy jen alternativy možného řešení, jejich užitnost a rozložení pravděpodobnosti výskytu jednotlivých stavů okolí,
- rozhodování za neurčitosti, při kterém není známo rozložení pravděpodobnosti výskytu jednotlivých stavů okolí.

Rozhodování za jistoty - je vše známo, a tudíž výsledek je znám, tzv. standardní rozhodování.

Rozhodování za nejistoty – problém je dobře strukturovaný (je jasná a kvantitativně popsaná struktura problému), lze použít optimalizační metody. Sestavují se varianty možných řešení a z nich se vybere optimální varianta. K vytvoření variant se dnes používají metody založené buď na odhadu, nebo na matematickém modelování. Při výběru metod je nutno respektovat povahu řešeného problému, stanovené cíle řešení, kritéria řešení a možnosti shromáždění potřebných vstupních informací. Do první skupiny patří metoda analogie, brainstorming, brainwriting, panelová diskuse, delfská metoda, synektika (Gordonova metoda, tj. technika tvůrčího myšlení), aplikace teorie mlhavých množin, aplikace zkušenostních databází, aplikace teorie fraktálů aj. Metody založené na matematickém modelování vychází ze zpracování časových řad. Pří-

lišná exaktnost při konstrukci exaktních modelů vede často k přecenění teoretických hledisek a k nerespektování reálných potřeb a možností budoucích uživatelů. Pragmatický přístup opírající se o rozbor reálné situace a o vytvoření modelu vhodného právě pro ni je závislý na metodice sestavení modelu - objektivita, nezaujatost, komplexnost údajů, schopnosti a kompetentnost odborníků. K výběru optimální varianty se používají metody, např. srovnávací, bodového hodnocení či váhového hodnocení.

Obecně při vysokém až nekonečném počtu událostí se určí medián, horní a dolní kvantil. Medián se ohraničí shora a zdola a postupné se zužuje jeho intervalu a totéž se dělá pro kvantily. Lépe je vycházet z předpokladu, že rozdělení pravděpodobností výskytu události má tvar některého ze známých teoretických rozdělení. Obvykle se vybírá z dále uvedených rozdělení:

1. Rovnoměrné rozdělení - všechny hodnoty v daném intervalu mají stejnou pravděpodobnost výskytu.
2. Normální rozdělení - jinak také Gaussovo – rozdělení spojité náhodné veličiny, je nejpoužívanější.
3. Log-normální rozdělení - přirozený logaritmus počtu událostí má normální rozdělení, tj. hodnoty jsou pozitivně vychýleny (ceny akcií, hodnota nemovitostí); graf je přímka v logaritmické stupnici.
4. Trojúhelníkové rozdělení lze použít, jsme-li schopni odhadnout dolní a horní mez a nejpravděpodobnější hodnotu (velikost prodejů, prodejní ceny,…).
5. Exponenciální rozdělení - rozdělení délky času mezi dvěma výskyty jevu (poruchy, vstup klientů žádajících daný typ obsluhy).
6. Beta rozdělení - vystihuje variabilitu výskytu jevu v určitém časovém intervalu (používá např. metoda PERT – pravděpodobnostní popis doby trvání činností v metodě kritické cesty).
7. Poissonovo rozdělení – diskrétní náhodná veličina - rozdělení málo pravděpodobných (řídkých) jevů,- počet událostí na jednotku (počet hovorů/min., počet klientů/hod., počet chyb/stranu dokumentu)
8. Binomické rozdělení - diskrétní náhodná veličina - počet výskytů jevu v pevném počtu pokusů (počet zákazníků, kteří preferují naše výrobky před konkurenčními).
9. Geometrické rozdělení – speciální případ negativního binomického rozdělení - počet pokusů, který je třeba k dosažení prvního úspěšného výskytu určitého jevu (stanovení počtu zkušebních vrtů, které je třeba provést, než se narazí na naftu)
10. Hypergeometrické rozdělení – diskrétní rozdělení - počet výskytů jevu v pevném počtu pokusů, na rozdíl od binomického se pravděpodobnost v každém následujícím pokusu mění (pravděpodobnost výběru vadné součástky bez vracení).

Postup spočívá v tom, že se volí typ rozdělení a odhadují se jeho základní číselné charakteristiky (střední hodnota, medián, rozptyl, dolní a horní meze).

Rozhodování za nejistoty a neurčitosti, když je problém slabě strukturovaný – lze použít metody systémové analýzy, které spojují exaktní matematické metody s normalizovanými kvantitativními úvahami (tj. heuristické metody). Heuristické metody rozhodování se obvykle dělí na: metody rozhodovací analýzy (maticová forma); a větvené rozhodování (rozhodovací strom).

Rozhodování za nejistoty a neurčitosti, když je problém nestrukturovaný – tj. u řady kroků jsou neurčitosti. Zde lze použít buď expertní metody, nebo metodiku případové studie. Expertní metody napodobují myšlenkové postupy specialistů. Opírají se o scénář procesu, ve kterém je řešitel dané úlohy veden k postupnému řešení dílčích problémů rozhodování v určitém logickém sledu úvah a činností, spojených s vytvářením a hodnocením různých variant řešení daného problému. Expertní metody jsou diagnostické a generativní (projekční).

Případové studie využívají kvalitativní i kvantitativní data způsobem, který umožňuje získat představu o častém řešení problému, tj. na základě zkušeností se vyhledává uspokojivé (a v jistém směru i optimální) místně a časově specifické řešení. Případová studie je založena na zkoumání procesu, ve kterém může z důvodů uvnitř i vně systému dojít v mezních bodech ke vzniku několika alternativ (variant) dalšího průběhu procesu. Na rozdíl od delfské metody (DELPHI), která je základem pravděpodobnostních modelů se nepředpokládá náhodné rozdělení alternativ, ale vydělení alternativ na základě dostupných informací. Dělí se na vyhledávání:

- extrémních nebo disparitních případů,
- kritických případů (zde je strategická důležitost s ohledem na obecný problém),
- paradigmatických (vzorových) případů.

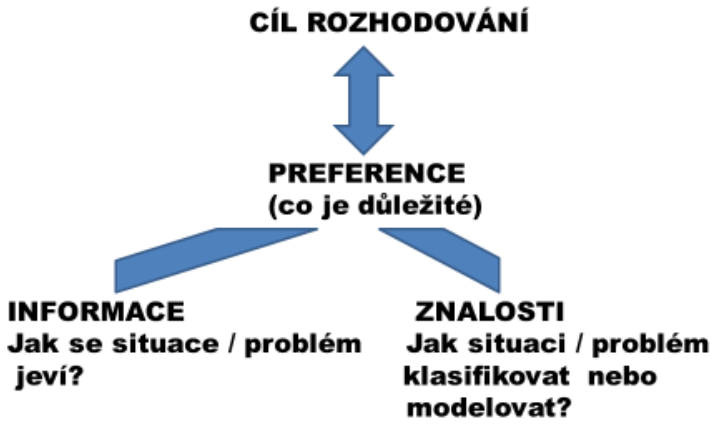
V tomto případě je rozhodovací subjekt aktivním prvkem rozhodovacího procesu, protože jeho znalosti, intuice a zkušenosti ovlivňují chápání problému, poznání neurčitostí, nejistot a preferencí a významně ovlivňují postup i výsledky řešení. Jde vlastně o skloubení exaktních postupů a modelových nástrojů se znalostmi a zkušenostmi řešitele nebo řešitelů.

Při výběru metod rozhodování je nutno respektovat povahu řešeného problému, stanovené cíle řešení, kritéria řešení a možnosti shromáždění potřebných vstupních informací. Pro modelování rozhodovacích procesů se používají:

- modely deskriptivní (popisující dosavadní průběh procesu),
- modely prediktivní (popisující pravděpodobný budoucí průběh procesu),
- modely normativní (popisující požadovaný budoucí průběh rozhodovacího procesu.

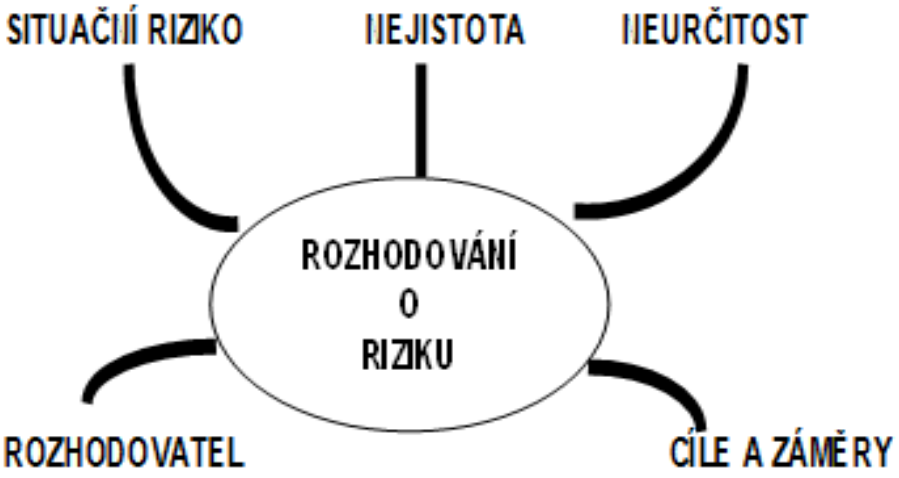
V praxi se používá teorie užitku [65], která respektuje postoj rozhodovacího subjektu k riziku, tj. odlišuje averzi k riziku, při které rozhodovací subjekt vyhledává málo rizikové varianty; sklon k riziku, při kterém rozhodovací subjekt vyhledává značně rizikové varianty, je-li tam vidina velkého užitku; a neutrální postoj k riziku. V prvním případě je funkce užitku v závislosti na kritériu funkce konkávní, v druhém konvexní a ve třetím lineární [9].

Proces stanovení rizika se může strukturovat jako více cílový (důsledky se mohou popsat více atributy) kompenzační rozhodovací problém. Více atributová analýza napomáhá při hodnocení alternativ, když cíle jsou konfliktní a výsledky jsou nejisté až neurčité. Nadto více atributová analýza může do rozhodování začlenit postoje – averze k riziku, hledání rizika. Je si třeba uvědomit, že v rámci inženýrství, které pracuje s riziky, existují dva procesy rozhodování, a to inženýrský a manažerský. Každý z těchto procesů rozhodování, které jsou formálně stejné – obrázek 7, vychází z jiného pohledu na situaci.



Obr. 7. Formální postup pro stanovení cíle rozhodování.

Je také skutečností, že i o riziku se rozhoduje s *rizikem* (technická záležitost − přesnost procesu měření a získávání dat), *nejistotou* (metodologická záležitost − spolehlivost teoretických východisek, identifikace a měření proměnných) a *neurčitosti* (konceptuální záležitost − rozpoznání a identifikace problému), obrázek 8.



Obr. 8. Rizika spojená s rozhodováním o riziku.

Nejistota obecně je odchylka mezi modelem a realitou. Náhodnou nejistotu lze popsat metodami matematické statistiky, když máme k dispozici dostatečné množství dat. Znalostní nejistoty způsobené nedostatkem kvalitních dat nebo důsledky náhlých změn podmínek v technickém díle či jeho okolí lze postihnout jen specifickými postupy, založenými na metodách operační analýzy nebo expertními odhady, o kterých bude pojednáno dále.

Ke zvýšení „nebezpečnosti / kritičnosti“ rozhodnutí obecně přispívají *složitost a rozmanitost cílů* (často jsou konfliktní), *citlivost rozhodnutí na změny, neurčitost klíčových proměnných a rozdílné pohledy na situaci.*

4.3.2. Určení kritických / prioritních aktiv, prvků a jiných položek technického díla

Je zřejmé, že pro technické dílo nemají prvky, zařízení, komponenty a systémy stejnou důležitost z hlediska jeho bezpečnosti. Jestliže chceme řídit bezpečnost technického díla, tak musíme znát prioritní aspekty, na nichž závisí dosažení cíle a na které musíme soustředit pozornost, tj. opatření a činnosti. Jejich výběr závisí na použitých kritériích [17]. ***Kritérium*** je pojem vymezující určitou vlastnost, která se připisuje hodnocenému objektu, a která může nabývat různých hodnot a různé míry přijatelnosti. Proto je nutné vyjasnit odpovědi na základní otázky:

1. Jaký je cíl a koncept, na jehož základě se určují kritické prvky, kritické komponenty, kritické systémy, kritické procesy, kritické funkce, kritická infrastruktura a kritické technologie?
2. Jak se provádí určování kritických prvků, kritických procesů, kritických funkcí, kritické infrastruktury a kritických technologií a komu slouží?
3. Jaké jsou nároky (data / vybavení / intelektuální potenciál apod.) potřebné pro určování kritických prvků, kritických procesů, kritických funkcí, kritické infrastruktury a kritických technologií?
4. Kdo provádí určování kritických prvků, kritických procesů, kritických funkcí, kritické infrastruktury a kritických technologií?
5. Jaké jsou výhody a nevýhody, slabá místa při určování kritických prvků, kritických procesů, kritických funkcí, kritické infrastruktury a kritických technologií?
6. Jaké je základní know-how (tj. popis a zdůvodnění procesu) spojené s vymezením kritických prvků, kritických procesů, kritických funkcí, kritické infrastruktury a kritických technologií?

Potřebám sledovaného konceptu integrální bezpečnosti [17] vyhovuje:

- kritické aktivum (zájem) je aktivům, které je důležité pro existenci a bezpečnost systému, tj. v konceptu integrální bezpečnosti jsou to u technologických systémů veřejná aktiva a aktiva spojená s existencí a provozem samotného technologického systému (obvykle jde o stroje, zařízení, personál, procesy a technologie),
- kritický majetek je majetek, který zajišťuje funkčnost systému, tj. objektu, infrastruktury, podniku, území, a při námi sledovaném konceptu integrální bezpečnosti i pro přežití lidí,
- kritický prvek ve sledovaném systému (objektu, infrastruktury, podniku, území) je prvek, který je důležitý pro funkčnost systému a při námi sledovaném konceptu integrální bezpečnosti i pro přežití lidí. Vyznačuje se vyšší zranitelností, nízkou odolností a zároveň nezastupitelnou funkcí,
- kritická místa v technologickém systému (objektu, infrastruktury, podniku, území) jsou místa, kde probíhají základní technologické procesy a pro která platí specifické předpisy zajišťující bezpečnost za normálních, abnormálních a kritických podmínek (např. jednoúrovňové křížení železnice a silnice v obci),
- kritická místa v objektu jsou schodiště, dveře, východy, výtahy, telefonní a komunikační centrály, elektrické přípojky, topení, bojlery, kamna, sklady, sklady odpadků, střechy. Ze systémů jsou to vnitřní a vnější osvětlení, systémy HVAC (ventilace a klimatizace, tj. rozvody zajišťující dodávky základních (životodárných) produktů), požární a nouzové detektory včetně sprchových systémů, varovacích a oznamovacích systémů, nouzových elektrických generátorů a bezpečnostních systémů včetně zámků, poplašných zařízení a řídicích systémů. Všechny uvede-

né položky a systémy se proto hodnotí z hlediska jejich dostupnosti, přístupu a spolehlivosti při pohromě předem a také se hodnotí dopady jejich selhání na zaměstnance a na provoz při a po pohromě,

- kritický stav prvku nebo zařízení je stav, ve kterém je možné závažné poškození nebo zničení prvku či zařízení,
- kritická vazba v systému je vazba, která je zranitelná pohromou. Je to vzájemný vztah mezi prvky, který se vyznačuje snadnou zranitelností, nízkou odolností a zároveň nezastupitelnou funkcí,
- kritický tok v systému je tok hmoty, energie, informace apod., který se vyznačuje snadnou zranitelností, nízkou odolností a zároveň nezastupitelnou funkcí. Při pohromě může dojít ke vzniku toků, které vytvoří spřažení mezi prvky systému, která vyvolají poškození prvků systému anebo kaskádu selhání dalších prvků, a tím naruší očekávané chování systému,
- kritická cesta je cesta / způsob propojení v systému, která způsobí poškození nebo zničení kritických prvků systému,
- kritický proces v technologickém systému (objektu, infrastruktury, podniku, území) je proces, který je vysoce důležitý pro funkčnost systému a zároveň je vysoce zranitelný při změně podmínek nebo výskytu pohrom,
- kritická pohroma znamená pohromu, která má vysoce závažný dopad na funkčnost systému (objektu, infrastruktury, podniku, území), a při námi sledovaném konceptu integrální bezpečnosti i na přežití lidí
- kritické služby (energie, voda apod.), provozy a výrobky při výskytu pohrom souvisí s problematikou bezpečností, zdraví, detekce a prevence ohrožení, nouzovým plánováním včetně uvědomění a přemístění, obnovou majetku a výrobků, telekomunikacemi, obnovou výroby, zvládnutím nouzové situace, bezpečím, prevencí a dokumentací ztrát, předcházením nouzovým situacím a s plánováním řízení likvidace škod,
- kritické funkce jsou funkce, které jsou vysoce důležité pro entitu a při námi sledovaném konceptu integrální bezpečnosti i přežití lidí,
- kritická funkce nouzového řízení (používá se hlavně v USA) označuje funkci, která je nezbytná pro kvalitní odezvu na nouzovou situaci. Při jejich výběru se posuzují systémy:
    - nasměrování, řízení a koordinace odezvy a obnovy v území postiženém živelnou a jinou pohromou s efektivním a účinným využitím dostupných zdrojů,
    - zajištění předávání informací a zpětné vazby a zálohování informací,
    - varování, tj. publikování časových předpovědí vývoje všech ohrožení a údajů o protiopatřeních, která má veřejnost použít, aby se vyhnula obětem na životech, zraněním a škodám na majetku,
    - zajištění předávání přesných, včasných a užitečných informací a instrukcí veřejnosti,
    - evakuace, tj. přesunu lidí na bezpečné místo,
    - péče o lidi, tj. ochrana evakuovaných a dalších obětí pohromy před dalšími (sekundárními, terciárními atd.) dopady pohromy, ve kterém je zahrnuto poskytnutí ukrytí, jídla, zdravotní péče, oděvů a dalších životně důležitých potřeb,
    - zdravotnictví, které zahrnují služby nemocnic, veřejného zdravotnictví, psychiatrie, péče o životní prostředí a pohřebnictví, tj. léčení, převoz a evakuace zraněných, márnice, kontroly nákaz, ošetření a izolace nakažených, zajištění nezávadné vody a potravin,

- řízení zdrojů, které jsou zacíleny tak, aby lidé, organizace i podniky splnili své úkoly.

Na základě uvedených kritérií jsou kritickými funkcemi nouzového řízení v území položky doprava, komunikace, infrastruktura, veřejné práce a inženýrství, hašení požárů, zajištění informací a plánování, péče o veřejnost, zajištění zdrojů, zdravotnictví, pátrání a záchrana, nakládání s nebezpečnými látkami, zajištění jídla a energií, obnova,

- kritická infrastruktura je soubor infrastruktur, jejichž selhání má závažný dopad na bezpečnost a rozvoj území včetně bezpečí a rozvoje lidí. Každá položka kritické infrastruktury se skládá z několika odlišných položek, které jsou podstatné pro její funkčnost. Jsou to: kritické liniové stavby, kritické objekty, kritické stroje a výrobní zařízení, kritické materiály a kritický personál. Infrastruktura je kritická kvůli své poloze ve složitém systému infrastruktur a území. V praxi se posuzuje: co naruší schopnost infrastruktury plnit požadované funkce v území; a jak dopady jejího selhání naruší bezpečí a rozvoj území včetně bezpečí a rozvoje lidí. Pro určení jejich kritických položek se posuzuje:
  - rozsah území, které je postižené ztrátou obslužnosti (vnitrostátní, mezinárodní, regionální nebo místní),
  - závažnost selhání, tj. stupeň ztráty obslužnosti (žádný, minimální, mírný nebo velký). Mezi kritéria, která lze pro hodnocení velikosti použít, patří zejména: dopad na obyvatele (počet zasažených obyvatel, ztráty na životech, onemocnění, vážné zranění, nutnost evakuace); hospodářský dopad (vliv na HDP, závažnost hospodářských ztrát nebo zhoršení kvality výrobků nebo služeb); životní prostředí (rozsah poškození, ovlivněné složky životního prostředí); synergické jevy (mezi jinými prvky kritické infrastruktury); a politické dopady,
  - časové faktory, tj. závažnost dopadů na jednotlivé subjekty v území v závislosti na čase (tj. okamžitě, za 24, 48 hod, za týden, později),
- kritická místa v infrastruktuře jsou místa, na jejichž funkčnosti závisí funkčnost více větví sítě (jde o místa, která při poruše vyvolají kaskády selhání),
- kritické služby jsou služby důležité pro obslužnost území, a při námi sledovaném konceptu integrální bezpečnosti i pro přežití lidí,
- kritické rozhodnutí v námi sledovaném konceptu je rozhodnutí o zbytkovém, přijatelném, sdíleném nebo vnuceném riziku. Přitom se podstatně projevuje vzdělanost a kultura rozhodovacích subjektů, hodnoty dané společnosti (hodnotový systém, morální úroveň) a obavy o existenci,
- kritické řízení v námi sledovaném konceptu je řízení kritických situací s cílem stabilizovat situaci, obnovit funkce systému a nastartovat další rozvoj systému za dostupných zdrojů, sil a prostředků v přijatelném čase s ohledem na přežití lidí.

Z výše uvedeného vyplývá, že: používaný význam slova kritický označuje určitou prahovou hodnotu pro sledovaný systém s tím, že jsou-li hodnoty pod tímto prahem, tak je stav žádoucí (podkritický) a opačně; máme dva typy kritických položek, a to:

- položky, které pouze způsobují eskalaci dopadů pohrom, buď všech, nebo jen některých, které jsou možné v daném místě,
- položky, které zaručují funkčnost systému, tj. bezpečnost a rozvoj chráněných aktiv. Jejich selhání způsobená nějakou pohromou nebo provozními aspekty vedou k závažným dopadům na chráněná aktiva.

U prvního typu se při obnově provádí zodolnění položky vůči pohromám, které v daném případě vyvolaly nebo mohou vyvolat nepřijatelné dopady. Provádění jejich obnovy nemá žádnou prioritu z pohledu funkčnosti území / objektu / státu apod.

U druhého typu se již v územním plánování, projektování, výstavbě i provozování provádí opatření, která vedou ke zvýšení technické spolehlivosti. Používají se různá opatření i zálohování činností jinými položkami, která vedou k vyšší odolnosti vůči možným pohromám. Proto při obnově je třeba provést opatření jak v oblasti zálohování, tak v oblasti zodolnění. Protože předmětné položky jsou životadárné pro území / objekt / infrastrukturu / stát apod., existují priority v obnově, přičemž je třeba, aby veřejný zájem byl upřednostněn před soukromými zájmy.

Určování kritických položek obecně je determinováno:
- způsobem hodnocení (přijímání) rizika, posuzování a zvládání rizika,
- metodologií rizikové analýzy a operačního výzkumu,
- nástroji řízení bezpečnosti včetně nástrojů krizového managementu,
- specifickými zvláštnostmi kybernetické infrastruktury,
- existujícími ohroženími od všech možných pohrom,
- způsobem určování priorit zranitelnosti systému,
- podvědomím obyvatelstva a vlastnostmi post-moderní společnosti.

Důvody, proč se určují kritické položky, jsou dány požadavkem na snížení rizik pro lidský systém z pohledu jeho bezpečnosti a rozvoje v nejširším slova smyslu. Jde o snížení míry zranitelnosti (zvýšení odolnosti) klíčových elementů lidského systému, které jsou zásadní pro existenci společnosti na všech úrovních organizace a státní správy, zajištění funkčnosti životodárných systémů a racionální ochranu kritické infrastruktury. Určování kritických položek se realizuje metodami exaktními, intuitivními a heuristickými. Nejlepší řešení dávají aplikace sofistikovaných DSS založené na multikriteriálním hodnocení [2-4,17]. Cílem je:
- identifikace, zvládnutí, odstranění nebo minimalizace nepředvídatelných událostí, které mají nežádoucí dopady na kritické prvky, kritické komponenty, kritické procesy, kritické funkce, kritickou infrastrukturu a kritické technologie v technickém díle,
- proces porovnávání odhadovaných rizik proti přínosu a/nebo ceně možných protiopatření a stanovení implementační strategie v rámci integrální (systémové, celkové) bezpečnosti,
- určení, kterým pohromám (škodlivým událostem) je technické dílo vystaveno, jaká jsou rizika od jednotlivých škodlivých událostí, jaké škody mohou vzniknout, která opatření výskyt škodlivých události odstraní nebo minimalizují,
- procedura spočívá v postupu:
  - vymezí se aktiva a stanoví se požadavky na jejich bezpečnost,
  - určí se zranitelná místa, možné dopady a rizika,
  - odhadne se: výše potenciálně způsobených škod; a cena vhodných bezpečnostních opatření,
  - provede se volba adekvátních bezpečnostních opatření.

Pro kritické položky se určí mezní hodnoty (limity), jejichž dodržení zajistí přijatelné bezpečí. To znamená, že úkolem jejich řízení je zajistit dodržování limitů, a proto základem je důkladný monitoring a kvalifikovaný DSS.

Na základě [17] se při hodnocení kritičnosti technických děl používají otázky:

1. Jak technické dílo reaguje na určité typy pohrom?
2. Jak je technické dílo masivní, odolné a pružné?
3. Jak se chování technického díla může zlepšit?
4. Jaké jsou vhodné mechanizmy kontroly?

5. Jaká pravidla se mohou využít pro samoregulaci nebo pro přípustné odchylky?
6. Které části technického díla jsou kritické?

Odpovědi na tyto otázky se hledají v dále specifikovaných krocích:

Krok 1 - Modelování problémové situace. Správný popis problémové situace podmiňuje úspěšnost řešení. Je důležité znát souvislosti, vztahy a interakce mezi částmi, které se mají analyzovat a hodnotit. Popis technického díla má čtyři hierarchické úrovně, které mají dále uvedené funkce:

- úroveň 1 představuje „Systém systémů“, což je celé hospodářství, nebo mezinárodní společenství (jako EU) nebo soustava veřejné správy. Cílovou funkcí této úrovně je funkční schopnost technického díla,
- úroveň 2 představuje komunitu, tj. okolí technického díla, s nimiž jsou spojeny různé zájmové skupiny (držitelé zájmů – stakeholders). Cílovou funkcí je minimalizace rizika nefunkčnosti technického díla,
- úroveň 3 je systémovou úrovní. Každý systém technického díla má určitou hodnotu a je třeba systémy seřadit dle této hodnoty,
- úroveň 4 je úrovní technických složek a prvků technického díla a cílovou funkcí je technická funkcionalita.

Současně se určují složky technického díla, mezi něž patří aktivní činitel (například provozovatel / operátor / obsluha), řiditelné faktory (například počítač, sítě, přepínače apod.), kritéria nebo ukazatel naplňování cílů (integrita, bezpečnost, spolehlivost apod.). A mezi těmito složkami jsou tyto vztahy:

1. Aktivní činitel řídí a kontroluje řiditelné faktory.
2. Řiditelné faktory ovlivňují chování aktivního činitele.
3. Řiditelné faktory určují ukazatele.
4. Ukazatelé regulují řiditelné faktory.

Technické dílo však není izolované (vzájemná závislost), proto se specifikují neřiditelné faktory ovlivňující systémy technického díla a působící na aktivního činitele a řiditelné faktory. Jedná se například o mezinárodní standardy.

Na ukazatele však mají také vliv vnější a vnitřní faktory, které určují hodnotu cílové funkce, jež dovoluje aktivnímu činiteli měnit řiditelné faktory, pakliže hodnota cílové funkce leží mimo normální hodnoty.

Krok 2 - Analýza příčinnosti. Analyzují se vrstvy technického díla: fyzická vrstva, vrstva regulace a řízení, vrstva organizace a managementu a vrstva strategického řízení správce technického díla. Analyzuje se také vzájemné působení prvků, a prvky se dělí na aktivní (řídící), pasivní (řízené), kritické a vyrovnávací prvky takto:

1. Aktivní prvky silně působí na jiné, samy však nejsou ovlivňovány.
2. Pasivní prvky působí slabě na jiné prvky, kdežto samy jsou silně ovlivňovány.
3. Kritické prvky působí na jiné a reagují velmi intenzivně.
4. Prvky, které neovlivňují jiné a ani nereagují s jinými, jsou prvky vyrovnávací.

Krok 3 - Návrh scénářů. Scénář se navrhuje následujícím postupem:

1. Stanovení časového rámce.
2. Identifikace faktorů ovlivňujících chování kritické infrastruktury.

3. Volba relevantní oblasti kritické infrastruktury pro scénář.
4. Návrh základního / výchozího scénáře.
5. Návrh alternativních scénářů.
6. Interpretace scénářů.

Krok 4 - Analýza dopadů. Cílem analýzy dopadů je zvýšení funkční schopnosti kritické infrastruktury, přičemž se vychází z faktu, že funkční schopnost sice závisí na systémové udržitelnosti a technické provozuschopnosti, avšak tyto ukazatelé nejsou přímo řiditelní.

Krok 5 - Plánování opatření.

Krok 6 - Realizace robustního a adaptabilního řešení

Na závěr je třeba poznamenat, že pro každé hodnocení musí být jasně stanovena hodnotová stupnice [16]. Pro hodnocení, tj. určení míry rizika (a následně i míry bezpečnosti) se používají:

- alfabetické stupnice (např. podle velikosti dopadu je riziko: zanedbatelné, malé, střední, velké, extrémní; nebo podle četnosti výskytu je riziko: nepravděpodobné, možné, časté, velmi časté, jisté),
- indikátory (číselné hodnoty pravděpodobnosti výskytu dopadu při realizaci rizika nebo číselné hodnoty velikosti dopadu při realizaci rizika), které jsou jistým způsobem vázané na uvedenou alfabetickou stupnici (např. pro pravděpodobnost výskytu dopadu při realizaci rizika: 1 – výskyt je vyloučený, 2 – výskyt je nepravděpodobný, 3 – výskyt je možný, 4 – výskyt je velmi pravděpodobný, 5 – výskyt je téměř jistý; pro velikost dopadu při realizaci rizika: 1 – škody a ztráty jsou zanedbatelné, 2 - škody a ztráty jsou nízké, 3 - škody a ztráty jsou střední, 4 - škody a ztráty jsou vysoké, 5 - škody a ztráty jsou extrémní). Závažnost (významnost) rizik měřených indikátory se obvykle určuje pomocí rozhodovacích matic, ve kterých se skóruje pravděpodobnost výskytu dopadů a velikost ztráty způsobené dopady nebo pomocí prostého součinu indikátoru vyjadřujícího výši pravděpodobnosti výskytu dopadu a indikátoru vyjadřujícího velikost ztrát (např. v uvedené souvislosti jsou možnosti 1 až 25 a lze použít klasifikaci: je-li součin menší než 5, je riziko nevýznamné; je-li součin mezi 6a 10, je riziko malé; je-li součin mezi 11 a 15 je riziko střední; je-li součin mezi 16 a 20 je riziko velké; je-li součin na 20, je riziko extrémně velké),
- výsledky přesného stanovení nebo změření konkrétních škod a ztrát [2,3,16] (pro potřeby vyjednávání s riziky jsou zjištěné hodnoty srovnávané s prahovými hodnotami, např. přijatelné - škoda menší než 0.01 měsíčního rozpočtu, nepřijatelné – škoda větší nebo rovna 0.1 měsíčního rozpočtu a podmíněně přijatelné, když hodnoty jsou v mezi limitami (místo peněz lze použít hodnoty koncentrace škodlivých látek, množství odpadu, stupeň neplnění požadavků apod.).

Pro řízení bezpečnosti technického díla, tj. pro řízení rizik zacílené na bezpečí a rozvoj technického díla však potřebujeme hodnoty, které mají zcela určitý význam. Protože velikost integrálního rizika spojeného se systémem závisí na celé řadě aspektů (dopady na jednotlivé komponenty, vazby a toky), je třeba mít sestavené hodnotové stupnice, aby se zajistila objektivita hodnocení. To znamená, že výsledky musí být správné (tj. opakovatelné, srovnatelné, ověřitelné a nezávislé na zpracovateli) a validované, tj. mít vypovídací schopnost k cíli řešeného úkolu. Přehled nejčastěji používaných stupnic je v [17].

4.3.3. Problémy řešené při práci s riziky technických děl

Hlavní typy problémů, které se rozhodují při řízení rizik:

1. Výběr prioritních rizik – jde o stanovení rizik, která jsou nejdůležitější.
2. Skórování rizik – jde o rozdělení rizik do kategorií podle konkrétních znaků / vlastností.
3. Třídění rizik – jde o uspořádání rizik podle velikosti nebo podle jejich zdroje na základě jistých pravidel.
4. Popis rizik – jde o kvalitativní popis rizik podle jejich možných dopadů.
5. Eliminování rizik – jde o rozdělení rizik do dvou skupin, a to na zvladatelná a nezvladatelná dostupnými zdroji, silami a prostředky.
6. Určení opatření na zvládnutí rizik v projektu / návrhu entity – jde o určení opatření na snížení rizik, což omezí ztráty, škody a újmy na chráněných aktivech po realizaci.
7. Stanovení podkladů pro sledování rizik – jde o určení dat nutných pro určení, výběr a vypořádání rizik během životnosti entity (projektu).

Jelikož mezi opatřeními pro řízení a zvládnutí rizik jsou i konflikty, je nutné použít multikriteriální rozhodování. Přitom je nutné zvažovat neurčitosti spojené s:
- tím, jak potenciální porucha způsobí významné důsledky,
- úrovní dopadů vyvolaných scénářem havárie, který je dobře definován,
- chováním staveb, systémů a komponent za různých podmínek,
- mnoha dalšími aspekty.

Řízení nejistot, a to hlavně těch, kterým říkáme neurčitosti, je základem pro zvládnutí rizik a zajištění bezpečnosti technických děl.

Kvůli složitosti technických děl je třeba používat multikriteriální rozhodovací metody, které z důvodu objektivnosti se v praxi opírají o příčinné (kauzální) vazby, tj. jejich závěry odrážejí vztah mezi příčinou a následkem (vše se děje v souvislostech) na základě aplikace několika kritérií, pomocí nichž se stanovuje optimální řešení z pohledu dosažení cíle. Používané metody rozhodování dle [8] jsou:
- empiricko-intuitivní,
- situační,
- rozhodovací analýza,
- rozhodovací tabulky,
- větvené rozhodování,
- rozhodování za neurčitosti,
- operační výzkum,
- simulace a modelování
- heuristické metody.

Racionální jádro jejich aplikace spočívá v efektivním využití omezených zdrojů za účelem maximálního dosažení cílů, resp. žádoucích užitků. Přitom se používají ekonomické analýzy, jejichž smyslem a posláním je zvýšit míru informovanosti o daném problému rozhodnutí, o možných variantách jeho řešení a o jejich společenských nákladech a užitcích.

4.3.3.1. Obecné zásady postupů práce s riziky složitých technických děl

U složitých systémů, do kterých patří technická díla, je skutečností, že cíle jednotlivých systémů jsou stejné jen v určitém intervalu podmínek. Proto pro práci s riziky použití jednoduchých metod, které byly sledovány v předchozím odstavci, má řadu nedostatků. Proto se používají metody založené na heuristickém přístupu a přitom se postupuje takto:

1. Rizika jsou pravděpodobné ztráty, škody a újmy na chráněných aktivech v konkrétním místě, které jsou závislé na velikosti pohromy a místní zranitelnosti.
2. Pro speciální cíle se definují dílčí procesní modely tak, aby byly transparentní a aby bylo možno jejich použitím získat výsledky s vysokou nebo alespoň dostatečnou vypovídací hodnotou.
3. Požaduje se, aby kritéria pro vyhledávání vazeb byla jasně formulovaná, jednoznačná a směřovala k vytyčenému cíli. Vhodné je použití kontrolních seznamů.
4. Při analýzách se používají zranitelnosti položek technického díla (prvky, vazby, toky), které se skórují s hodnotami důležitosti položek z pohledu funkčnosti technického díla.
5. Pro vyhledávání kritických míst napříč technickým dílem se nejčastěji používají rozhodovací matice. Protože praxe čas od času vyžaduje také řešení specifických úkolů, pro které aplikace matice kritičnosti (tj. rozhodovací matice) je příliš hrubým nástrojem, jsou používány metody preciznější založené na teorii grafů, a to např. metoda kritické cesty (tzv. CPM), metoda optimalizace řešení problému v čase a prostoru (tzv. PERT) a metoda modelování procesů v síti (tzv. Petriho sítě).
6. Vyhodnocení kritických míst se provádí na počátku hodnocení a pak při každé změně nebo po uplynutí určitého stanoveného časového intervalu (např. 3 roky) a mezi tím se ve zvlášť důležitých případech kritických infrastruktur používá inspekce založená na specifickém kontrolním seznamu.

Z důvodu složitosti je třeba používat multikriteriální rozhodovací metody. Z důvodu objektivnosti se předmětné metody opírají o příčinné (kauzální) vazby, tj. jejich závěry odrážejí vztah mezi příčinou a následkem (vše se děje v souvislostech) na základě aplikace několika kritérií, pomocí nichž se stanovuje optimální řešení z pohledu dosažení cíle. Používané metody rozhodování dle [8] jsou: empiricko-intuitivní; situační; rozhodovací analýza; rozhodovací tabulky; větvené rozhodování; rozhodování za neurčitosti; operační výzkum; simulace, modelování; a heuristické metody. Racionální jádro jejich aplikace spočívá v efektivním využití omezených zdrojů za účelem maximálního dosažení cílů, resp. žádoucích užitků. Přitom se používají ekonomické analýzy, jejichž smyslem a posláním je zvýšit míru informovanosti o daném problému rozhodnutí, o možných variantách jeho řešení a o jejich společenských nákladech a užitcích.

4.3.3.2. Základní postupy používané v praxi

Základní používané postupy v inženýrských disciplínách pracujících s riziky jsou: APPEL, ARAMIS, ARIS, cyklus PDCA, PRISM, postup pro bezpečnou přepravu založený na modelu QRAM a postup REHRA. V odborné literatuře lze najít postupy další.

APPEL je postup, který se především věnuje nebezpečným činnostem uvnitř jednotlivých zařízení a dopravě nebezpečných látek v rámci regionu. Při realizaci programu APELL mohou být zainteresováni jednotlivci i společnosti překračující rámec místa, regionu či státu. Hranice teritorií a pole působnosti zákonů by neměly omezovat účast všech zainteresovaných stran na programu APELL, ale měly by naopak vést k potřebě koordinace tohoto programu. Základní informace jsou na internetových stránkách OSN, *Program APPEL* (Awareness and Preparedness for Emergencies at the Local Level) [2,72].

APELL (Awareness and Preparedness for Emergencies at Local Level) je iniciativa sponzorovaná IEO (Industry and Enviroment Office) v rámci programu UNEP (United Nations Environment Programme) ve spolupráci se CMA (United States Chemical Manufactures Association) a CEFIC (Fédérations de l'Industrie Chimique). Ochranný program CAER (Community Awareness and Emergency Response) je rozvíjen CMA a zkušenosti při jeho uplatňování jsou zdrojem APELLu. APELL také uznává specifika odpovědnosti a roli, kterou hrají národní vlády a mezinárodní plánovací společenství. APELL zahrnuje dvě základní hlediska:

1. Vytvořit nebo zlepšit uvědomění regionální populace o možných rizicích při výrobě, manipulaci a použití nebezpečných látek a o postupech úřadů a průmyslu při zajištění ochrany populace před těmito látkami.
2. Na základě vědomostí regionální populace a ve spolupráci s místní komunitou vytvořit nouzový plán pro případ ohrožení, který by zahrnoval do odezvy celou místní společnost.

Proto se APELL skládá ze dvou částí:

1. Příprava informací pro veřejnost, která se nazývá „uvědomění veřejnosti".
2. Vytvoření plánu k ochraně veřejnosti, který se nazývá „nouzový plán“.

ARAMIS (Accident Risk Assessment Methodologies for Industries) je postup, kterým se charakterizuje úroveň rizika podniku či provozu pomocí integrálního indexu rizika (číslo 0 – 100), jehož určení vychází z hodnocení scénářů možných havárií s přítomností nebezpečných látek, zranitelností, účinnosti preventivních opatření a z pravděpodobností výskytu kritických jevů. Postup je výsledkem projektu EU na tvorbu řízení bezpečnosti v mezích určených směrnicí Seveso. Obsahuje principy detekce a diagnostikování nehod a principy převodu technologického zařízení z kritického do bezpečného stavu. V jeho rámci se provádí popis a klasifikace bariér, definice SMS (Safety Management Systém) a měření indikátorů bezpečnosti. K posouzení bezpečnosti se používají dotazníky typu kontrolních seznamů (check list) různé úrovně a hloubky [2].

ARIS - Architektura Integrovaných Informačních Systémů je metodika a softwarový nástroj firmy IDS Scheer pro modelování, analýzu, optimalizaci a dokumentaci procesů. ARIS vychází ze skutečnosti, že modelovaná realita obsahuje mnoho vazeb a vztahů, které lze obtížně zachytit v jednom srozumitelném modelu. Metodika ARIS tento problém řeší vytvářením tzv. pohledů, při kterých se strukturovaně zachycuje

realita organizace z hlediska různých aspektů [2].

CYKLUS PDCA (Plan – Do – Check - Act) – plánuj, dělej, kontroluj, pracuj - je v tomto případě chápán jako nedílná součást každého procesu, který se plánuje, realizuje, kontroluje a návazně se do dalšího plánování zapracovávají připomínky či nápravná opatření, která při předchozím cyklu vznikla. V některých případech je vhodné použít cyklus SDCA (Standardize-Do-Check-Act), ve kterém se nejprve vytvoří standard a poté se realizují všechny činnosti obdobné jako u cyklu PDCA [2].

PRISM (Process Industries Safety Management) je postup řízení, jehož cílem je vylepšit chování lidí ve vypjatých (zátěžových) situacích během pracovního procesu. Pracovní zátěž obsluhy je definovaná jako psychosomatická odezva člověka na práci v určitých podmínkách. K hodnocení pracovní zátěže personálu se nejčastěji používá multikriteriální metoda SWAT (Subjective Workload Assessment Technique). V jejím rámci se hodnotí mentální a časové nároky a psychická zátěž obsluhy. Často se také používá další subjektivní metoda NASA TLX, která používá při hodnocení šest aspektů, a to: mentální, fyzické a časové nároky, úsilí, výkon a flustrace.

Postup pro bezpečnou přepravu založený na modelu QRAM (Quantitative Risk Assessment Model) připravený pod hlavičkou EU obsahuje pro hodnocení rizik kvantitativní model, který umožňuje ve sledovaném případě sestavit konečný soubor možných scénářů, spočíst pravděpodobnost jejich výskytu a vyhodnotit jednotlivé dopady a z nich plynoucí rizika pro chráněné zájmy lidského systému.

REHRA (Rapid Environment and Health Risk Assessment) [9] je postup pro rychlé ohodnocení rizika, který používá světová zdravotnická organizace (WHO). Jedná se o indexovou metodu, která pro účely analýzy rizika odděleně hodnotí nebezpečnost lokality, zranitelnost a dosahy působení dopadů pohrom. Postup je schematicky znázorněn na obrázku 9.

Obr. 9. Postup REHRA.

4.3.4. Multikriteriální metody a jejich zázemí

Klíčovým prvkem vícekriteriálního rozhodování je, jak název napovídá, práce s kritérii a alternativami (variantami), a proto je důležité předmětné prvky charakterizovat. ***Kritéria*** představují hodnotitelné (kvantifikovatelné) faktory jako jsou názory a postoje kompetentních osob, anebo profesních zájmových skupin. K formulaci kritérií se obvykle přistupuje dvěma způsoby:

1. Přístup shora - dolů odpovídá kategoriím tzv. ***hodnotového myšlení***, které vytváří strom kategorií hodnot a kritéria jsou tak hierarchicky uspořádána.
2. Přístup zdola - nahoru je příkladem tzv. ***alternativního myšlení***, v němž se kritéria formulují systematickým procesem odvozování a vyvozování a mohou se následně seskupovat do širších kategorií.

Kritéria vytvořená jak přístupem shora - dolů, tak přístupem zdola - nahoru musí splňovat následující požadavky:

1. *Hodnotová významnost kritérií* označuje spjatost s cíli a preferencemi zájmových skupin.
2. *Měřitelnost kritérií* znamená ustavení kvantitativní nebo kvalitativní škály měření výkonnosti alternativ.
3. *Úplnost kritérií* vyjadřuje jejich schopnost pokrýt všechna podstatná hlediska zvažovaného problému, přičemž jsou výstižná a akceschopná.
4. *Srozumitelnost kritérií* zabraňuje nejednoznačnému použití a výkladu.

Metody zpracování podkladů pro rozhodování rozdělujeme takto:
- metody koncipované jako systém, tj. stromy významnosti, morfologická analýza, analýza křížových interakcí, apod.,
- metody převzaté z jiných oblastí pro určení pořadí, např. prahy citlivosti, Kennedyho medián, apod.

Metoda stromu významnosti pomáhá klasifikovat a ohodnotit i velké množství rozhodovacích faktorů, které v různém stupni významnosti souvisí s obecným cílem studovaného objektu. Morfologická analýza je nástrojem na strukturování problému. Spočívá v systematickém zkoumání všech myslitelných řešení, jejichž parametry jsme schopni identifikovat. Jednotlivé parametry a hodnoty, kterých parametry mohou nabývat, se uspořádají do morfologické matice. Analýza křížových interakcí je používána v případě, že se zabýváme systémem, ve kterém probíhají vzájemně se ovlivňující jevy. Tímto způsobem vybraná nejpravděpodobnější řešení se dále rozpracovávají do podoby scénářů.

Z možných metod uvedených v [9] se zmíníme se o dvou efektivních nástrojích. ***Situační analýza pro podporu rozhodování*** používá jednoduché metody jako: metoda pro uspořádání informací / názorů; metoda kauzální analýzy; metodu 4 W a 1 H; metodu 5PROČ; metoda PROČ-PROČ DIAGRAM; metoda JAK-JAK DIAGRAM; metoda JAK-JAK DIAGRAM; a Dunckerův diagram. ***Metoda kauzální analýzy*** používá diagram příčina – následek / účinek. Její varianty jsou Rybí kost - Ishikawův diagram. Analýza příčin a následků napomáhá důkladnému pochopení podstaty problému, protože nutí, abychom se zabývali všemi možnými příčinami. Postup při její aplikaci je:

- identifikace problému (to znamená odpovědi na otázky: kde se problém vyskytuje?; Jaká je jeho podstata?; Kdy se vyskytl?; Jak často se vyskytl?; Koho se problém týká?; apod.),
- výčet podstatných faktorů problému (faktory jsou jako kosti rybí páteře),
- identifikace možných příčin (malé čárky na „rybích“ kostech“),
- analýza diagramu.

Rozhodnutí, který přístup je pro dané technické dílo vhodný, závisí zejména na následujícím:
- jakých cílů má být použitím stanovení (identifikace, analýzy a hodnocení) rizik dosaženo,
- k jakým účelům aktiva technického díla slouží,
- jaká je hodnota aktiv technického díla,
- zda jsou funkce, které technické dílo poskytuje, kritické a pro koho,
- jaká je úroveň investic do technického díla,
- jaká je výše nákladů na obnovení funkčnosti technického díla.

Na základě [4,43,44,47,52] v případě, že technické dílo má vysoké výrobní cíle, náklady na hrazení případných ztrát a škod a dopadů jsou vysoké, obnovení opětovného chodu technického díla po odstranění dopadů realizovaného rizika je taktéž střední až vysoké, aktiva technického díla jsou cenná, pak je podrobná analýza rizik nutná.

Každé technické dílo neustále čelí rizikům, a proto je nutné, aby správa technického díla rizika řídit. K tomu je třeba rizika pojmenovat, popsat a pochopit je pohledem přes priority pro dané technické dílo a jeho okolí (veřejný zájem). K tomu, aby rizika technického díla byla dobře řízena, je nutné použit takovou metodu analýzy rizik, která je vhodná pro danou organizaci. Pochopitelně nejprve je třeba odpovědět na otázku „která metoda je ta nejvhodnější?“. Na tuto jednoduchou otázku není tak jednoduchá odpověď. Je nutné se na tento problém podívat komplexně, systematicky, ale i lidsky z pohledu dané ho technického díla. Znamená to odpovědět na základní otázky, co chceme eliminovat a co chceme řídit. Správné pochopení vztahů v organizaci je pro úspěšné provedení analýzy rizik klíčové.

V praxi jsou stále více používány metody založené na metodách operační analýzy, tj. síťové modely – PERT, GERT, Petriho sítě, a to v provedení deterministickém, stochastickém a dokonce barevném [9]. Stále více se uplatňují aplikace bayesovských sítí, např. [73-76], protože se pomocí nich lze postihnout neurčitosti procesů probíhajících v technických dílech.

Z práce [77] vyplývá, že pro studium SoS, jejich chování a selhání se nejčastěji používají specifické metody pro sestavení modelů, a to: Bayesian Method; Bayesian Network; Mixed Bayesian Network; Fuzzy Bayesian Network Model; Bayesian Reliability Model; Fuzzy Rule-based Bayesian Reasoning (FuRBaR); Petri Nets (PN); Coloured Petri Nets (CPN); Stochastic Petri Nets (SPN); Coloured Stochastic Petri Nets (CSPN); Case Study (CS); Multi-Attribute Utility Theory (MAUT); Multi-Criteria Analysis (MCA); Weighted Sum Approach (WSA); Concordance, Discordance Analysis (CDA); Technique for Order Preference by Similarity to Ideal Solution (TOPSIS); Ideal Point Analysis (IPA); Aggregation Preferences (AGREPREF); Preference Ranking Organisation Method for Enrichment Evaluations (PROMETHEE); Markov Chain (MC); Multi-Objective Genetic Algorithm (MOGA); a Multiplicative Intuitionist Linear Logic (MILL).

Cílem je zajistit rozhodování ve prospěch věci. Proto musí být používaný otestovaný soubor kritérií, který zaručuje objektivitu, nezávislost a nezaujatost hodnocení. Kritéria dělíme podle těchto hledisek:

- objektivní a subjektivní, přičemž objektivní kritéria jsou taková, kde limita (srovnávací hodnota) je tvořena běžně měřitelnou jednotkou, která je zjistitelná laboratorně, výpočtem nebo ekonomickou rozvahou,
- kritéria výhod a užitečnosti (čím vyšší, tím lepší) či kritéria nákladů, ztrát a obsahu kontaminantů (čím nižší, tím lepší),
- kritéria kumulativní, která jsou charakterizovaná vztahem vzájemné komplementarity, tj. vzájemně se doplňující a podporující. Vyšší plnění jednoho je splněno s vyšším plněním druhého a naopak. Extrémně kumulativní jsou taková kritéria, kdy plnění jednoho je podmíněno plněním druhého; kritéria tohoto druhu je třeba ze souboru kritérií vyřadit,
- kritéria alternativní jsou dána vztahem vzájemné konkurence, popř. jsou protichůdná. Zvýšené plnění jednoho ukazatele je spojeno se sníženým plněním druhého a naopak. Extrémně alternativní kritéria se absolutně vylučují a ze souboru kritérií musí být vyřazeny,
- kritéria nezávislá jsou daná indiferentními nebo variabilními vztahy.

Opět si je třeba uvědomit, že u složitých technických děl je pro správné rozhodování důležité systémové hodnocení. Systémovým hodnocením se rozumí aplikace určité, vhodně zvolené soustavy kritérií, resp. hodnotících funkcí na sledované objekty definované systémově. To znamená, že předpokládáme a specifikujeme určité charakteristické chování objektu v čase a prostoru, určité odezvy na možné reakce atd. Kritéria dělíme na:

- *vnitřní*, tj. taková, která zajišťují hodnocení předmětného objektu (zohledňují pouze objekt jako takový), tj. jeho kvalitu, realizovatelnost, splňování určitých cílů, potřeb, požadavků apod.,
- *vnější*, tj. taková, která zajišťují hodnocení objektu jako součásti širšího systému (zohledňují objekt a okolí), tj. realizovatelnost, materiálové a energetické nároky, zdroje, lidské aspekty, ekologické dopady, sociální dopady apod.,
- *spjatá se směrem času*, tj. s možnými změnami posuzování v čase či se změnami funkce objektu v čase (tj. bere se v úvahu očekávané dynamické chování objektu v čase).

Hodnocení technického díla, procesu jeho užívání se děje na základě zjištěných dat. Má několik kvalitativních úrovní. Nejjednodušší je porovnání konkrétní hodnoty kvalitativních nebo kvantitativních dat (např. údaj o třídě jakosti) s určitým pevně stanoveným limitem nebo modelem (nastal či nenastal sledovaný jev). Srovnání s limitem se používá, když sledování je zaměřeno na kontrolu kvality jisté položky či na určení, zda je či není třeba nastartovat specifikovaná regulační nebo varovná opatření. Srovnání s parametry určitého modelu je více typické pro pozorovací sítě, které mají jeden z cílů identifikovat jevy v oblasti, kterou pokrývají.

Vícekriteriální (multikriteriální) metody převážně řeší konfliktní rozhodovací situace, ve kterých výhody jednoho kritéria vedou k nevýhodám druhého kritéria a opačně. Zároveň tam, kde působí náhodné jevy a vlivy je složité určit jednoznačně důsledky rozhodnutí. O řešeních za podmínek nejistoty a neurčitostí není možné rozhodovat okamžitě, ale rozhodnutí se stávají výsledkem procesu, určitých obecných zásad podrobných analýz. Přestože jejich obsah bývá formulován různě, lze rozlišit jednotlivé pracovní etapy:

- identifikace a formulace problému (tj. soustředění, utřídění a zpracování informací),
- volba strategií,
- matematická analýza, popř. konstrukce modelu (tj. simulace a numerická analýza, popis neuvažovaných vztahů, posouzení jednotlivých variant, výběr preferované (optimální - superiorní) varianty),
- výsledné rozhodnutí včetně realizace,
- kontrola, ověření a verifikace provedeného rozhodnutí, tj. provedení potřebných úprav, posouzení zpětné vazby a regulace ve smyslu rozhodnutí a stanovených cílů.

Podstatou rozhodovacího procesu je možnost výběru řešení. Jednotlivá rozhodnutí se označují jako možné strategie a rozhodovací proces jako výběr strategie. Podle povahy rozhodnutí z hlediska jeho následků lze rozeznat strategie maximální, minimální a smíšené.

Maximální strategie se soustřeďuje na jediný prostředek k dosažení úspěchu, většinou maximální zisk. Jde-li o zisk bez ohledu na možnou ztrátu, nazývá se strategií optimistickou.

Minimální strategie jde cestou nejmenšího rizika, zpravidla nejmenší ztráty, popř. minimalizace nákladů. Jestliže minimalizuje ztrátu a nezajímá se o dosažení zisku, jde o tzv. strategii pesimistickou.

Smíšená strategie přizpůsobuje postup konkrétním podmínkám, předpokládá přesná pravidla a dokonalý informační systém. Za objektivní, exaktní nebo matematické metody lze považovat metody s přesně kvantitativně vyjádřenými úlohami, používající jako nástroj matematický aparát a při větším rozsahu i strojovou výpočetní techniku.

Protože technickoekonomické metody optimalizace vedou k násilnému ohodnocení (číselnému naplnění) obtížně kvantifikovatelných kritérií, které hrají velkou roli, je vhodné používat pro rozhodovací proces *systémový přístup. V případech, kdy je obtížné nebo nemožné odvodit optimální řešení analyticky, používá se metoda simulace*. V podstatě jde o experimentování na modelu, na kterém lze měřit jednotlivé parametry zkoumaného systému a sledovat vliv těchto změn až do okamžiku nalezení přijatelného optima. Uvedený postup se týká především aplikace metod vektorové optimalizace matematického programování, která umožní nalézt kompromisní řešení z nekonečné množiny přípustných řešení. Teoretické optimum může být z různých důvodů (např. politických) nepřijatelné.

Teoretický rozbor metod a práce s kritérii lze nalézt v [9] v souvislosti s používáním třídících kritérií pro tzv. screening (tj. prosvícení problému ze všech stran). Pro systémový přístup je třeba zvažovat tři soustavy kritérií, tj. soustavu interních kritérií, soustavu externích kritérií a soustavu kritérií spojených s chováním zkoumaného systému v čase, viz výše. Podobný postup je používán i při hodnocení techniky [64], které je běžné ve vyspělých zemích světa.

V praxi je třeba srovnávat nesouměřitelné jevy a veličiny s cílem určit priority a zásady v rozhodování pro dosažení žádoucího cíle. O řízení bezpečnosti to platí také, protože se jedná o mnohaoborovou a mezioborovou disciplínu, ve které jsou předmětem např. živelné a jiné pohromy a jejich charakteristiky, které jsou produktem různých planetárních, regionálních nebo lokálních procesů a dějů či činností provozovaných člověkem. S ohledem na tuto skutečnost, tj. na zcela rozdílnou podstatu těchto položek, nelze jednoduše použít explicitní nebo implicitní závislosti, protože by chy-

běla rozumová podstata. Je třeba nejprve vytvořit srovnávací platformu a na jejím základě určit srovnávací matici, ze které lze odvodit existující platné zákonitosti. Jinými slovy to znamená, že souměřitelnosti se dosahuje zvolením určité vybrané verbální stupnice a klasifikací hodnot veličin, které potřebujeme vzájemně posoudit. Klasifikaci musí provést experti vhodnou metodou, např. vícestupňovou delfskou metodou. To znamená, že nejprve se specifickým způsobem vytvoří data, která se vynesou do specifických matic či grafů [2-4,78-81].

Hlavním problémem ovšem je nejistota a neurčitost vstupních dat (tj. hodnot ohrožení), protože na výstupu jsou nejistoty a neurčitosti výsledků vždy větší [3, 82-84]. Návrhů, jak postupovat je celá řada. Např. práce [85] navrhuje používat Markovovy procesy.

4.4. Metodiky používané v praxi při práci s riziky zacílené na zvládnutí rizik

Nejprve vyjmenujeme metody používané v základním logickém postupu, který vede ke zvládnutí rizik u technických děl a pak se budeme věnovat vybraným postupům a metodám.

4.4.1. Metodika pro zvládnutí rizik technických děl

Vzhledem ke složitosti technických děl i území je nutno na základě výsledků shrnutých v pracích [9,58] při práci s riziky použít celou řadu provázaných postupů, aby se zajistilo jejich zvládnutí. Je nutno začít u začátku logického řetězce, a to u výběru jevů, tj. pohrom, které mají potenciál poškodit sledovaná chráněná aktiva technického díla a jeho okolí. Jde o metody pro:

1. Stanovení relevantních pohrom v území, ve kterém se nachází technické dílo a v samotném technickém díle.
2. Stanovení největší očekávané velikosti relevantních pohrom:
   a) když zdrojem ohrožení je jeden zdroj pohromy,
   b) když zdrojem ohrožení je více zdrojů pohromy.
3. Stanovení poklesu velikosti dopadů pohromy se vzdáleností od místa vzniku pohromy ke sledovaným aktivům.
4. Stanovení anomálií v rozložení dopadů pohromy v území a v technickém díle.
5. Výběr nepřijatelných dopadů pohromy v území a v technickém díle.
6. Ocenění potenciálních škod na sledovaných aktivech způsobených nepřijatelnými dopady pohrom.
7. Zajištění zdrojů, sil a prostředků a provedení kvalitní odezvy na havárii technického díla a popř. jeho okolí
8. Určení vhodných nápravných opatření pro očekávané pohromy v území a v technickém díle.
9. Výběr optimálních nápravných opatření pro obnovu technického díla a jeho okolí.

10. Implementaci nápravných opatření pro zajištění obnovy technického díla a jeho okolí.
11. Vytvoření databáze nápravných opatření a jejich technické a finanční zajištění.
12. Stanovení parametrické závislosti nákladů na obnovu vs. velikost pohromy a vytvoření finanční rezervy na obnovu.

Dalšími nástroji, které jsou používané v praxi pro zvládnutí rizik, jsou: bezpečnostní plánování; postupy civilní ochrany; postupy provedení evakuace; postupy pro stanovení kategorií nouzových situací; postupy pro stanovení kategorií zvládání rizika (přijatelné, tolerovatelné, podmíněně přijatelné, nepřijatelné); nouzové (havarijní, povodňové, protipožární aj.) plánování; krizové plánování; aplikace principů kultury bezpečnosti; metoda pro normativní klasifikaci pohrom – výpočet ohrožení; nouzové hospodářství; nouzové plánování; postupy obnovy; postupy odezvy; postupy pro ochranu důležitých (kritických, prioritních) komponent technického díla; postupy pro ochranu zaměstnanců technického díla a obyvatelstva; postupy pro ochranu technologií a infrastruktur; vypracování poučení z pohrom a z jejich zvládání; pracovní inženýrské metody – výpočet ohrožení od možných pohrom, výpočet velikosti rizika, postupy pro vyjednávání s riziky (v technických normách se doporučuje použít postup TQM [56]). Dále následují průkazy odolnosti, soubory limit a podmínek, určení nebezpečnosti látek nacházejících se v technickém díle, stanovení projektové (návrhové) pohromy, stanovení velikosti největší očekávané pohromy, stanovení zdrojových oblastí pohrom a hlavně havárií uvnitř technického díla, způsoby řízení bezpečnosti, způsoby řízení nouzových situací, způsoby řízení kontinuity technického díla, způsoby krizového řízení technického díla, způsoby řízení havárií v technickém díle, způsoby řízení rizik (plány řízení prioritních rizik); zpracování scénářů pro specifické a kritické pohromy; postupy pro ukrytí zaměstnanců a popř. obyvatel v okolí; postupy varování; postupy vyrozumění.

4.4.2. Způsoby stanovení rizik používané v praxi

Pro řešení otázek bezpečnosti [17,20] je důležité v území či technickém díle kvalifikovaně zvažovat všechny důležité aspekty [2]. Správnost řešení založených na metodologií konstrukce případových studií lze přezkoumat vytvářením vývojových diagramů, křížové matice, matice kritičnosti nebo zvláštními kontrolní seznamy [9,66]. Když zjištění konvergují, zvyšuje se důvěryhodnost výsledků. Když se objeví nějaké disparitní (konfliktní) zjištění, tak problém musí být zkoumán hlouběji, musí se najít příčiny konfliktů [46]. Testy aplikované na skutečných případech potvrdily užitečnost a účinnost nástroje [63].

Současné poznání ukazuje, že pohromy vzhledem ke své povaze nemají rovnoměrný vliv na veřejná i privátní aktiva, protože jejich konkrétní individuální zranitelnosti vůči potenciálním pohromám jsou odlišné [18,58]. Stanovení rizik musí respektovat ztráty, škody a újmy na veřejných i privátních aktivech, které jsou způsobené jak přímými dopady pohrom, tak těmi, které jsou spojené s vnitřními závislostmi mezi aktivy, které se projeví v čase. Pro řízení a vypořádání rizik v čase je třeba použít u technických děl specifický postup [58].

Z pochopitelných důvodů pro potřeby strategického rozhodování nelze používat metody, které slouží jen pro identifikaci rizika nebo kontrolu rizika [2]. Určení ohrožení od pohromy $\boldsymbol{H}$ a periody návratu τ (v rocích) provádíme metodami založenými na teorii velkých čísel, teorii extrémů, teorii mlhavých množin, teorii chaosu, teorii fraktá-

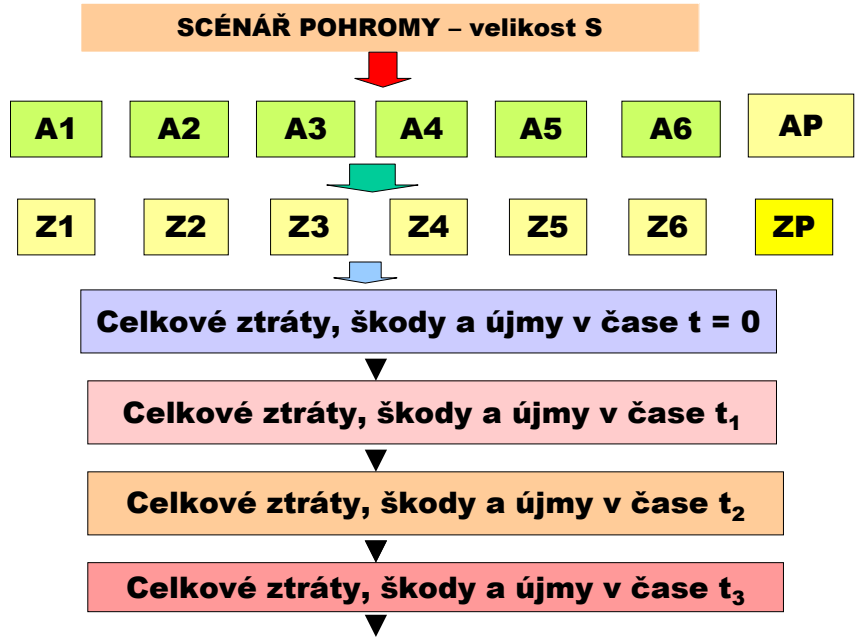
lů apod. Podle místní zranitelnosti chráněných aktiv v definovaném území (např. čtverec 10 x 10 km; kružnice o poloměru 5 km), stanovíme celkovou škodu pro ohrožení ***H*** (v penězích) označenou ***C***. Na základě velikosti celkové ztráty, škody a újmy na chráněných aktivech ***C*** při dané velikosti projektové pohromy a periody jejího návratu τ (v rocích) se stanovuje riziko ***R*** podle vztahu

$$R = C \cdot \tau^{1}.$$

V případech pohrom, u kterých nelze určit periodu návratu, protože neexistují kvalitní datové soubory (např. technologické havárie), se vychází z velikosti celkové ztráty, škody a újmy na chráněných aktivech ***C***, která je reálně možná (je určená např. množstvím nebezpečné látky, maximální koncentrací škodliviny apod.), a podle expertních odhadů se určí četnost jejího výskytu normovaná na 1 rok ***f*** a riziko se stanovuje ***R*** podle vztahu

$$R = C \cdot f.$$

Určení celkových ztrát a škod na chráněných aktivech se počítá dle postupu, který je zobrazen na obrázku 10; celkové ztráty, škody a újmy při velikosti projektové pohromy $C = Z1+Z2+\ldots+Z6+ZP$ a položky označené písmenem ***Z*** jsou ztráty, škody a újmy na chráněných aktivech A_i.



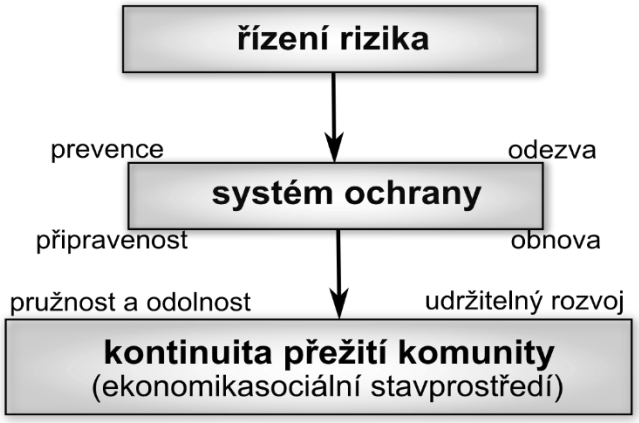
Obr. 10. Vývojový diagram pro stanovení rizik pro potřeby strategického řízení bezpečnosti; A – aktiva a Z ztráty, škody a újmy na aktivech; označení: 1- životy a zdraví lidí, 2- bezpečí lidí, 3 – majetek, 4 – veřejné blaho, 5 – životní prostředí, 6 – infrastruktury a technologie, P – privátní.

Obrázek 10 je v souladu s postupy, které kodifikuje česká legislativa při oceňování škod a s postupy, které používá územní plánování při výstavbě kritických objektů [11,47]. Respektuje lidské hodnoty znázorněné Maslowovou pyramidou, kterými jsou potřeby lidí: fyziologické; bezpečí a jistota; sociální; společenské uznání; a seberea-

lizace. Vychází z poznání, že míru kritičnosti pro lidi totiž zvyšují s časem narůstající ztráty, škody a újmy, které způsobují:

- snížení kvality života (ztráta jistot lidí, která se může promítnout až do násilných akcí; ztráty společenských kontaktů a ztráty možností uplatnění, které vedou k sociální deprivaci a následně i k neschopnosti společnosti realizovat odezvu na pohromy další),
- ztráta obslužnosti území,
- ztráta konkurenceschopnosti privátních subjektů a z toho plynoucí nezaměstnanost,
- ztráta schopnosti rozvoje kvůli rostoucím výdajům na sociální dávky, zdravotnictví apod.).

Důležité je při strategickém rozhodování zvažovat i sekundární dopady a mít připraveny akceschopné kvalifikované plány odezvy a plány obnovy [1,9,10], a to jak pro území, tak pro složité technologické objekty a infrastruktury, u kterých je potřebné mít i plány kontinuity [1,17]. Vysoce nebezpečným sekundárním jevům je třeba buď zabránit, anebo mít připravena opatření na jejich rychlé zvládnutí. Pro lidskou komunitu je vyjádřen vztah mezi řízením rizika a přežitím na obrázku 11. Řízení rizika zajišťuje podmínky pro přežití komunity.



Obr. 11. Logický postup pro zajištění přežití komunity či technického díla.

4.4.3. Výpočet ohrožení

Jak již bylo uvedeno výše, riziko je místně specifické a závisí na dvou faktorech, a to velikosti pohromy, havárie či selhání objektu, která je jeho zdrojem, a na množství a zranitelnosti sledovaných aktiv. Postupy pro stanovení ohrožení, která představují jednotlivé pohromy pro člověka, území či objekty se vyvíjely v čase. Od odhadů založených na výběru maximálně pozorované velikosti pohromy v daném místě od dob historických až po dnešek, přes aplikaci: metod matematické statistiky; algoritmů teorie mezních hodnot; teorie velkých čísel; matematického modelování; analýzy založené na pravděpodobnosti hraničních hodnot; analýzy založené na horních a dolních odhadech hodnot pravděpodobnosti výskytu; teorii fuzzy množin; teorii možností až po teorii Dempster-Shaferovu [61,62], která kombinuje přesné výpočty a heuristiky, a tímto způsobem zvažuje náhodné nejistoty a neurčitosti v režimu výskytu pohrom.

Mírou velikosti očekávané pohromy je veličina ***ohrožení***, tj. normativně stanovená velikost pohromy - nehody, havárie či selhání u technických děl. Podle zavedených normativů určujeme hodnoty ohrožení v daném místě. Dle práce [58] se používají

- velikost stoleté povodně, stoletého zemětřesení atd.,
- maximální pozorovaná pohroma v historické době či maximální možná havárie technického díla,
- maximální očekávaná pohroma či maximální očekávaná havárie technického díla.

Dle naposledy citované práce se hodnota ohrožení zjišťuje:

- odhadem na základě minulých zkušeností,
- odečtem z map maximálních dopadů pohromy, např. mapa seismických zón, mapa dopadů vichřic, mapa dopadů srážek apod.,
- provedením mezních odhadů hodnot ohrožení na základě scénářů minulých pohrom (obalová křivka všech scénářů, mediánový scénář všech možných scénářů, nejméně příznivý scénář),
- provedením mezního odhadu pro nejméně příznivý scénář pro největší očekávanou pohromu,
- výpočtem dle postupů stanovených v normách (např. maximální zemětřesení, očekávané maximální zemětřesení, maximální síla vichřice, očekávaná síla vichřice, velikost koncentrace nebezpečných látek, velikost tlakové vlny, …),
- u objektů zásadní důležitosti se použijí specifické postupy jako: aplikace teorie extrémních hodnot; aplikace fuzzy množin; recentně teorie možností.

Při výpočtu ohrožení se předpokládají modely rozložení pravděpodobnosti výskytu pohrom [3,82-86] jako jsou rozložení log-normální, Gamma, Pearsonovo, Frechet-Weilbullovo (dvouparametrické či tříparametrické), Frechetovo, Fiskovo a další.

Některé práce, např. [82] ukazují, že výsledky pravděpodobnostních výpočtů jsou citlivé na výběr rozložení, jiné opak. Např. v práci [83] bylo provedeno porovnání parametrů vypočtených na základě rozdělení trojúhelníkového, normálního, Weilbullova, Gumbelova a Gamma. Vypočtené střední hodnoty ležely v intervalu daném standardními odchylkami a rozdíly v koeficientech korelace byly až na třetím desetinném místě. V práci [84] na několika desítkách příkladů pro zemětřesení bylo ukázáno, že oba zmíněné případy jsou možné a že konkrétní výsledek závisí na charakteru vstupních dat.

Je si třeba uvědomit, že když při určení ohrožení jsou použita nesprávná data (neúplné nebo krátké časové řady), nebo nesprávný výpočetní postup, tak je ohrožena bezpečnost sledovaného objektu, jak bude dále ukázáno; konkrétní příklady rozdílů mezi výsledky různých metod pro zemětřesení jsou uvedené v [84].

Algoritmus výpočtu ohrožení založený na teorii extrémních hodnot vychází z Gumbelova rozdělení pravděpodobnosti nepřekročení $R_t(M_o \geq M_{oi})$, která je dle [3] dána vztahem

$$R_t(M_0 \geq M_{0i}) = 1 - \left[\frac{T}{T + t \cdot P(M_0 \geq M_{0i})}\right]^{n+1}$$

ve kterém M_o a M_{oi} pro i =1,2,…,n označují velikosti sledované pohromy (ve stupních či fyzikálních jednotkách jako je posunutí, rychlost, zrychlení, anebo jiných mírách) a $P(M_o \geq M_{oi})$ je dáno vztahem

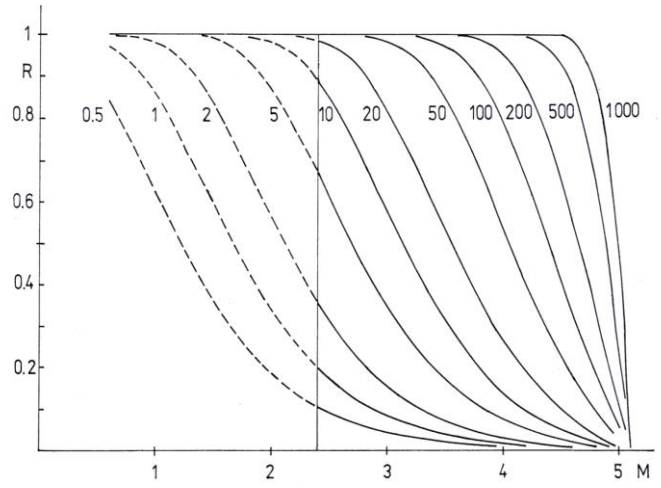
$$P(M_0 \geq M_{0i}) = \frac{e^{-\beta M_{0i}} - e^{-\beta M_{0max}}}{e^{-\beta M_{0min}} - e^{-\beta M_{0max}}}$$

přičemž M_{omax} je maximální velikost pohromy zastoupená v daném souboru, M_{omin} je hranice homogenity dat, T je doba pozorování, ze které jsou data, t je časový interval, pro který je ohrožení stanoveno, n je počet jevů a $\beta = \ln b$, kde b je sklon grafu ze vztahu

$$\log N_{ci} = a - b\, M_{oi}$$

ve kterém ***pro i = 1,2,..., n*** označuje N_{ci} kumulativní četnost, M_{oi} velikost pohromy, a, b numerické parametry.

Ilustrační příklad průběhu pravděpodobností nepřekročení ***R*** ukazuje obrázek 12 pro velikost pohromy ***M*** a časové intervaly ***t = 0.5 roku, 1 rok až 1000let***.



Obr. 12. Průběh funkcí vyjadřujících pravděpodobnost nepřekročení pro časové intervaly t = 0.5, 1,2,…, 1000 let.

Velikost největší očekávané pohromy (tj. velikost ohrožení ***H***) pro jisté ***t*** se určí jako průsečík příslušné křivky na obrázku 12 se zvolenou hladinou významnosti. Hladina významnosti vyjadřuje, s jakou nepřesností vyslovujeme závěr – nejčastěji se volí ***v = 0.05*** nebo ***0.01.*** Hodnotu 0.05 interpretujeme jako míru nepřesnosti nebo obecně jako možnost omylu 5%; parametr

p = 1 - v

pak udává pravděpodobnost, s jakou je výsledek správný. Střední perioda opakování / návratu (return period) τ pro pohromu s velikostí M_o je rovna ***času t,*** pro který platí rovnost

$$R_t = 0.633.$$

Předmětným výpočtem se určí velikost pohromy v místě vzniku. Dále je třeba provést korekci na vzdálenost sledovaného místa od místa vzniku, což je samostatný problém, protože kromě útlumu se vzdáleností se uplatňují i nehomogenity a anizotropie prostředí mezi místem vzniku a místem sledování, jak ukazují příklady v práci [3]. V citované práci je pak ukázán výpočet velikosti projektové pohromy pro zadávací podmínky technického díla.

Z fyzikálních a praktických důvodů je důležité srovnávat jen výsledky získané stejným způsobem [8]. Důvod ukazuje příklad výpočtu seismického ohrožení v jedné lokalitě ve středních Čechách, které na základě jednoho datového souboru [87] je spočteno více postupy používanými v praxi [88]. Vidíme zřejmé rozdíly:

- odečet z mapy seismických zón v novelizované ČSN 73 0036 [89] stanovuje hodnotu 5.5 °MSK-64,
- deterministicky určené hodnoty pro vybraná údobí jsou v tabulce 8,
- stochasticky určené hodnoty pro vybraná údobí jsou v tabulce 9.

Tabulka 8. Velikost seismického ohrožení H spočtená deterministicky na základě teorie extrémních hodnot a dat z různých časových období.

Časový interval	**Velikost seismického ohrožení H [° MSK-64]**
50 let	5.5
100 let	5.7
10 000 let	6.1

Tabulka 9. Velikost seismického ohrožení ***H*** spočtená pomocí pravděpodobnostního přístupu na základě teorie extrémních hodnot pro různá časová období a pomocí metody PSA.

Časový interval	**Pravděpodobnostní přístup**			***H* [° MSK-64] metoda PSA**
	Standardní odchylka [° MSK-64]	***H* [° MSK-64] medián**	***H* [° MSK-64] medián + standardní odchylka**	
50 let	0.10011	5.0	5.1	5.3
100 let	0.08286	5.2	5.3	5.5
10 000 let	0.00148	5.5	5.6	5.9

Tabulky 8 i 9 ukazují, že velikost seismického ohrožení (tj. maximálního očekávaného zemětřesení) v jedné lokalitě roste se zvětšující délkou doby, ze které jsou použita data. Předmětný fakt je vysoce důležitý pro stanovení rizika a jeho zvládnutí, a to nejen u zemětřesení.

Práce [3,43-45,50,53,58] ukazují, že když u libovolné pohromy použijeme pro výpočet ohrožení, tj. očekávané maximální velikosti pohromy, datový soubor z krátkého

časového údobí, tak dostaneme hodnotu ohrožení, která neodpovídá realitě dané periodou opakování silných pohrom.

Jelikož hodnota ohrožení (dle stavebních norem a standardů velikost projektové pohromy) tvoří základ zadávacích podmínek pro technická díla, na jejich základě se určuje velikost rizika pro technické dílo, tak výsledkem je podcenění velikosti rizika. V praxi to znamená, že preventivní opatření vložená do projektu s cílem zabránit realizaci souvisejícího rizika, anebo alespoň zmírnit jeho dopady na chráněná aktiva veřejná i technického díla, jsou podceněná. V důsledku podcenění dochází dříve či později k haváriím či selháním technických děl, jejichž příčinu označujeme jako chybu projektu díla; řada příkladů v archivu [63].

Příkladem je havárie jaderné elektrárny Fukushima v r. 2011 [90], která byla odstartována extrémním tsunami, jehož velikost nebyla zvážena v projektu. Citovaná práce ukazuje, že jaderná elektrárna Onagawa, jen 30 km vzdálená od jaderné elektrárny Fukushima, byla postavena na základě zadávacích podmínek pro datový soubor o tsunami od r. 860 a tsunami v r. 2011 vydržela (normálně odstavila a po prohlídce byla schopna provozu), a jaderná elektrárna Fukushima postavena na základě zadávacích podmínek pro datový soubor o tsunami jen od r. 1890, tsunami nevydržela a vznikla velká jaderná havárie.

Srovnání tabulek 8 a 9 také ukazuje, že hodnoty určené deterministicky jsou vyšší než ty určené pravděpodobnostním přístupem. Proto se při projektování technických děl používají hodnoty určené deterministicky a při inspekcích během provozu hodnoty určené pravděpodobnostně [3,43,44,87].

4.5. Vybrané heuristické nástroje používané při práci s riziky technických děl

Práce [9] ukazuje, že nástrojů předmětného typu je mnoho. Podrobněji se zmíníme o třech metodách, a to DELPHI, rybí kost a kontrolní seznam používaný jako DSS (systém pro podporu rozhodování).

4.5.1. Metoda DELPHI

Jak již bylo výše uvedeno, bezpečnost složitých technických děl závisí na mnoha oblastech (obrázek 3), které nejsou vzájemně souměřitelné, a proto se u nich používají metody, které dovolují zohlednit názory expertů z více oborů.

Metoda DELPHI je v současné době velmi upřednostňovaná, protože je vhodná pro expertní týmové hodnocení. V USA jsou některé předpisy pro rozhodování založeny právě na ní [9]. V metodě je bezprostřední styk expertů nahrazen propracovaným programem postupného individuálního dotazování, zpravidla formou anket. Dotazování je provázeno pravidelným informováním expertů o výsledcích zpracování dříve získaných odpovědí. Postup je následující:

- písemně každý expert odpoví na otázky v dotazníku,
- odpovědi expertů se zpracují a experti dostanou veličiny mediánu a intervalu mezi krajními kvartily, pak jsou experti požádáni o přezkoumání odpovědí a případné korekce.

Experti, jejichž ocenění leží mimo interval, vymezený krajními kvartily, jsou požádáni o zdůvodnění oprávněnosti svých stanovisek. Odpovědi expertů jsou opět zpracovány a získané výsledky jsou opět předány účastníkům expertízy. Vedle toho experti dostávají stručný souhrn zdůvodnění, která byla uvedena na podporu stanovisek, jež se značně odlišovala od mínění většiny expertů. Metoda se obvykle realizuje ve 4 - 5 ti etapách. Za směrodatný názor expertní skupiny se považuje medián konečných hodnot odpovědí.

Byly rozpracovány i složitější postupy, např. v případě posuzování procesů v čase se celý výše uvedený postup opakuje pro každý časový úsek v časové chronologii. Velmi často se používá vícestupňová metoda DELPHI (tj. rozdělení problému do dílčích částí dle stromů událostí a aplikace delfské metody na posouzení jednotlivých uzlů tohoto stromu).

Vícestupňová delfská metoda ***DELPHI*** patří do skupiny intuitivních prognostických metod, založených na tvůrčím myšlení [9]. Její podstata spočívá v postupném zjišťování a porovnávání názorů expertů o budoucím vývoji zvolené oblasti, přičemž je zaručena jejich vzájemná anonymita, řízená zpětná vazba informací a statistické identifikace shody názorů zkoumané skupiny expertů. Hlavní cíl je určení, *kdy se jistá událost stane, nebo kdy může nastat a za jakých podmínek.*

Metoda se uskutečňuje prostřednictvím promyšleně voleného systému otázek, které se kladou zvolené skupině expertů, a to formou dotazníku, nebo osobním rozhovorem organizátora ankety („systémového inženýra“) s jednotlivými respondenty, aby se zjistil jejich individuální názor, přičemž respondent nikdy nepřichází do kontaktu s ostatními respondenty. Pro zajímavost je třeba poznamenat, že metoda je široce používaná a např. legislativa USA obsahuje specifický právní předpis, který kodifikuje pravidla pro její užívání. Další podrobnosti jsou dostupné v [9].

Vzhledem k tomu, že mnoha čtenářům je známa metoda panelové diskuse, tak rozdíl mezi ní a delfskou metodou je následující: cílem panelové diskuse je dosáhnout souhlasného názoru účastníků diskuse; cílem delfské metody není souhlasný názor (konsensus) expertů, ale shrnutí názorů expertů a výsledkem je medián názorů expertů. Počítá se totiž s tím, že vzhledem k existenci neurčitostí v datech, různí odborníci mohou dle svých znalostí a zkušeností vidět problém v různých úrovních.

4.5.2. Metoda stromu významnosti

Metoda pomáhá vhodně klasifikovat a ohodnotit velké množství problémů, které v různém stupni významnosti souvisí s obecným cílem daného technického díla [9]. Nejčastěji jsou používány následující přístupy:

1. PATTERN (Planning Assistance Through Technical Evaluation of Relevance Numbers) je finančně a časově náročný a skládá se z následujících kroků:
   - sestavení verbálního scénáře (chronologický popis očekávaných změn, rozhodnutí a mezioborových souvislostí),
   - vytvoření stromu významnosti,
   - ocenění současného stavu uvažovaných technických řešení,
   - převedení kvantitativních vazeb mezi cíli a prostředky do algoritmizované podoby,
   - sestavení konečného modelu řešení,

2. QUEST (Quantitative Utility Estimates for Science and Technology) se používá pro zvýšení efektivnosti a spočívá v:
   - kvantitativním ocenění významnosti různých úkolů,
   - kvantitativním ocenění přínosů různých směrů řešení,
   - určení celkové významnosti každého směru řešení pro jednotlivé úkoly,
   - vymezení prostředků.
3. SEER (System for Event Evaluation and Review), který v sobě spojuje metodu DELPHI s extrapolačními a normativními postupy.

4.5.3. Morfologická analýza

Metoda se používá při aplikaci morfologického přístupu, který je charakterizován v odstavci 4.1. Je nástrojem na strukturování problému [9]. Spočívá v systematickém zkoumání všech myslitelných řešení, jejichž parametry jsme schopni identifikovat. Jednotlivé parametry a hodnoty, kterých parametry mohou nabývat, se uspořádají do morfologické matice. Metodika se skládá z:
- přesného vymezení (identifikace) problému, který má být řešen,
- určení parametrů, na kterých bude záviset řešení problému,
- pro každý parametr řešeného problému se stanoví určitý počet různých, nezávislých a dále neredukovatelných hodnot, kterých může nabývat morfologická matice.

4.5.4. Analýza metodou matice křížových interakcí

Metoda je používána v případě, že se zabýváme systémem, ve kterém probíhají vzájemně se ovlivňující jevy [9]. Vybraná pravděpodobná řešení se rozpracovávají do podoby scénářů. Důležité poznatky z oblasti tvorby scénářů:
- scénář je historicko – systémový model,
- úkolem scénáře je popsat budoucí vývoj v jeho různých podobách závislých na učiněných rozhodnutích,
- scénář je orientován na proces, imituje probíhající mechanismy v systému,
- cílem scénáře je především určit kritické události, kritické body vývoje, ve kterých je nutné učinit zásadní rozhodnutí, ovlivňující další rozvoj.

Důsledky možných rozhodnutí jsou ve scénáři uvedeny jako alternativní volby mezi konečnými stavy v budoucnosti.

Sestavení scénáře sestává z:
- shromáždění prognostických informací o daném systému a jeho okolí,
- identifikace cílů studovaného systému,
- identifikace vnitřních faktorů, popř. bariér rozvoje systému,
- identifikace vnějších faktorů, popř. bariér rozvoje systému,
- identifikace variantních strategií řízení systému (je nutné vzít v úvahu stávající mechanismus řízení a jeho různé varianty, které se mohou realizovat v budoucím období; současně je nutné formulovat strategii rozvoje systému – jakým směrem je žádoucí, aby se systém rozvíjel),
- vlastního sestavení scénáře,
- interpretace scénáře.

Při výše uvedených krocích je třeba zvažovat:

- posouzení současného stavu a současných rozhodnutí z hlediska budoucího vývoje,
- kvalitativní faktory a strategie různých účastníků,
- mnoha rozměrnost a neurčitost budoucnosti,
- pohled globální i systémový,
- možnou tendenčnost informací a strategií,
- více přístupů, které se doplňují,
- fakt, že existují předpojatosti strategií i lidí a zamezit jim.

Vlastní metoda křížové matice interakcí se používá např. v procesu posuzování vlivů na životní prostředí EIA (Cross-Impact Matrix) a při přímém posouzení rizika (Risk Matrix). V obou případech přísluší do skupiny metod pro předběžné posuzování sledovaného jevu; v prvním případě jde o screening a proces PES (Preliminary Environmental Study), ve druhém případě o proces PHA (Preliminary Hazard Analysis). Z toho vyplývá, že se aplikuje podrobná formalizovaná metoda. Nevýhody jednostupňové matice se snaží někteří autoři vylepšit konceptem vícestupňovitosti [9].

4.5.5. Citlivostní analýza a testy citlivosti

Metody sledující citlivost výsledku na vybrané parametry se používají v případech, ve kterých je třeba posoudit vliv nejistot, nepřesností a různých změn v základních parametrech, které provázejí hodnocení od okamžiku stanovení (kvantifikace) ukazatelů kritérií až po určení jejich relativní důležitosti, na výsledek hodnocení [9]. Zpravidla jde o zjištění:
- vlivu různých kritérií na výsledek,
- stability výsledku řešeného úkolu (v závislosti na změnách určitých parametrů),
- odhad možných vlivů nejistot a neúplných informací.

V detailu je citlivostní analýza řešena pomocí testů citlivosti, které lze rozlišit na dále uvedené druhy testů:
- zaměřené na zjištění, jaká změna určitého vstupního parametru (parametrů) je nutná, aby se změnil výsledek hodnocení (pořadí variant). Jestliže tato změna výsledku vyžaduje nepřiměřeně velkou nebo nepřijatelnou změnu vstupního parametru, svědčí to o stabilitě původního hodnocení,
- založené na změně hodnot ukazatelů,
- založené na změně tvaru nebo minima či maxima dílčích funkcí užitku,
- založené na změnách použitých hodnot relativní důležitosti při zachování podmínky, že po úpravě jsou znovu normalizovány,
- zaměřené pouze na podrobné zkoumání ukazatelů kritérií s nejvyšším vlivem na výsledek hodnocení.

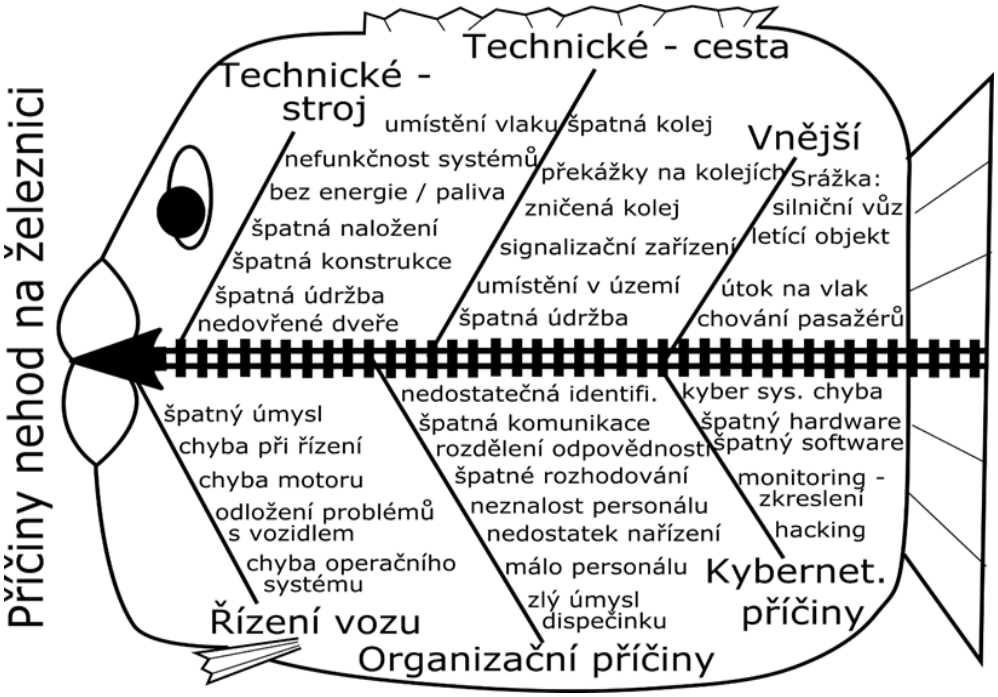
Pro všechny testy obecně platí, že jsou-li výsledky původního hodnocení (pořadí variant) a testů citlivosti stejné, lze posuzovaný systém pokládat za stabilní.

4.5.6. Diagram rybí kosti

Diagram rybí kosti představuje grafické znázornění příčin jistého děje, procesu či jevu. Kauzální diagram (Ishikawa Diagram = graf rybí kosti, graf rybí páteře) je nástroj, který podporuje v dané problematice analýzy příčin a důsledků určitého procesu, jevu či stavu a usnadňuje hledání východisek řešení vyvolaných problémů. Cílem metody je identifikovat možné příčiny či zdroje problému (případně oblastí, které mají na pro-

blém vliv) a graficky je strukturovat.

Organizátor řešení problémů nakreslí "rybí kostru". Ve skupinové diskusi jsou definované důsledky situované na příslušná místa "kostry" podle příbuznosti a poté jsou na základě diskuse (brainstormingu) hledány kauzální řetězce příčin a důsledků. Metodu lze použít např. při tvorbě rezortních koncepcí při identifikaci výchozího stavu a při definování východisek. Metodou lze získat rychle i údaje, které běžným sběrem nebo měřením dat jsou zjistitelné se značným úsilím. Úskalím metody jsou však znalosti a zkušenosti (tj. kvalifikace) diskutujících. Podrobnosti jsou dostupné v práci [9]; příklady jsou uvedeny v práci [4]. Jako příklad roztřídění zdrojů (příčin) dopravních nehod na železnici pomocí diagramu rybí kosti, obrázek 13.



Obr. 13. Zdroje dopravních nehod na železnici [4].

4.5.7. Vybrané kontrolní seznamy pro řízení technických děl

Praxe ukazuje, že kontrolní seznamy jsou vhodné pro oblast řízení, kde se kontrolní seznam používá k systematické kontrole plnění předem stanovených podmínek a opatření pro technické dílo. Seznamy kontrolních otázek (checklists) jsou zpravidla generovány na základě seznamu charakteristik sledovaného technického díla nebo činností, které souvisejí s technickým dílem a potenciálními dopady, selháním prvků technického díla a vznikem škod. Jejich struktura se může měnit od jednoduchého seznamu až po složitý formulář, který umožňuje zahrnout různou relativní důležitost parametru (váhu) v rámci daného souboru. Uvedeme příklady, které byly otestovány v praxi; další jsou v práci [66].

Příklad jednoduchého kontrolního seznamu pro zpracovatelský závod je v tabulce 10. Kontrolní seznamy mohou používat váhu, mohou dle potřeby používat klasifikační stupnice různého druhu; příklady jsou v pracích [2,4,9,17].

Tabulka 10. Příklad jednoduchého kontrolního seznamu pro řídícího pracovníka technického díla.

OTÁZKA	VÁHA	ANO	NE
Obsahuje dokumentace technického díla schémata, návody?			
Obsahuje dokumentace technického díla protokoly o zkouškách?			
Jsou součástí dokumentace technického díla informace o výcviku obsluhy?			
Jsou v dokumentaci technického díla uvedeny podmínky, za nichž zařízení nesmí být používáno?			
Jsou v dokumentaci technického díla upozornění na možná nebezpečí?			
Analyzovala se rizika zařízení technického díla pro všechny etapy jeho technického života a pro všechny podmínky užívání (instalace, údržba, obsluha)?			
Identifikovala se všechna možná významná ohrožení technického díla a byla oceněna jejich závažnost včetně odhadu četnosti výskytu?			
Specifikovala se v technickém díle opatření pro snížení / odstranění rizik?			
Zahrnuje analýza rizik technického díla také stavy způsobené nesprávnou obsluhou?			
Počítalo se při analýze rizik technického díla i s případy, které se mohou důvodně předpokládat?			
Vzalo se při analýze rizik technického díla v úvahu i možné nepohodlí vyplývající z užívání ochranných pomůcek a prostředků?			
Jsou výsledky analýzy rizik technického díla součástí dokumentace?			

Často se kontrolní seznamy používají při projektování. Jsou generovány po linii převládajícího typu rozvojového projektu (např. viz typologie staveb: dálnice, přehrady, zneškodňování odpadů, atd.) nebo výrobní technologie (chemický průmysl, potravinářských průmysl aj.), který je simulován jako procesní model [9]. Kontrolní seznamy nejsou efektivní při odhalování dopadů vyšších řádů, tj. sekundárních a dalších, anebo vztahů mezi dopady.

Tradiční kontrolní seznamy se značně liší, co se týče úrovně detailů, a jsou široce využívány k označení splnění standardů a zvyklostí. Analýza kontrolním seznamem se používá jednoduše a může být aplikována v kterémkoli stadiu života technického díla nebo sledovaného procesu. Kontrolní seznamy mohou být použity k detailnímu seznámení nezkušeného personálu s procesem pomocí srovnávání procesních vlastností s různými požadavky kontrolního seznamu. Kontrolní seznamy rovněž zajišťují společný základ pro hodnocení procesu nebo provozu managementem.

Podrobný kontrolní seznam poskytuje základ pro standardní hodnocení procesních zdrojů rizika. Může být rozsáhlý do té míry, aby odpovídal specifické situaci, ale měl by být aplikován svědomitě, aby byly odhaleny problémy vyžadující pozdější podrobnou analýzu. Obecné kontrolní seznamy jsou často kombinovány s jinou technikou identifikace zdrojů rizika. Jsou limitovány zkušenostmi jejich autora, a proto by měly být tvořeny autory s rozličným technickým vzděláním, kteří mají rozsáhlé zkušenosti

s podobnými systémy, jako je ten analyzovaný. Často mají kontrolní seznamy strukturu informací podle příslušných běžných kódů, standardů a předpisů či pravidel. Kontrolní seznamy by měly být živé dokumenty a měly by být pravidelně kontrolovány a aktualizovány.

Ve světě jsou používány standardní kontrolní seznamy pro řízení provozu technického díla – od jeho zahájení až po ukončení jeho provozu. Vyplněný kontrolní seznam musí být často schválen různými členy vrcholového managementu technického díla před tím, než se provoz může přesunout z jedné etapy do další. Tímto způsobem působí jako komunikační prostředek i jako forma řízení.

Tradiční kontrolní seznamy slouží především jako pojistka toho, že se provoz technického díla shoduje se standardní praxí. V některých případech analytikové používají obecnější kontrolní seznam v kombinaci s jinou metodou odhalování zdrojů rizika, aby nedošlo k opomenutí některého z nich. Analytik pro vytvoření tradičního kontrolního seznamu definuje standardní projektové nebo provozní postupy, pak je používá k vytvoření seznamu otázek založených na nedostatcích nebo rozdílech. Vyplněný kontrolní seznam obsahuje na dané otázky odpovědi typu „ano“, „ne“, „neaplikovatelný“ nebo „potřeba více informací“. Kvalitativní výsledky se liší podle jednotlivé situace, ale obecně vedou k rozhodnutí typu „ano“ nebo „ne“ podle shody se standardními postupy. Abychom správně provedli tuto techniku, potřebujeme patřičný kontrolní seznam, inženýrské projektové postupy a provozní manuál a pro vyplnění seznamu někoho, kdo má základní znalosti o revidovaném provozu. Pokud je patřičný kontrolní seznam dostupný z předchozí činnosti, analytik by měl být schopen jej použít. Pokud patřičný kontrolní seznam dostupný není, pak jedna osoba (někdy i více lidí) musí připravit kontrolní seznam a provést vyhodnocení. Zkušený manažer nebo vedoucí inženýr by měl zkontrolovat výsledky analýzy kontrolním seznamem a nasměrovat další postup.

Propojení procesního modelu pro zajištění bezpečnosti technického dílka a kontrolního seznamu ukazuje tabulka 11.

Tabulka 11. Kontrolní seznam pro posouzení kritičnosti technického díla pomocí identifikace rizik v procesu řízení bezpečnosti.

Procesní model pro řízení bezpečnosti	**Kontrolní seznam**

	Otázka	**ANO**	**NE**
1. Identifikovat kritický majetek a dopady jeho ztrát – tj. kritičnost	1. Jsou určeny kritické činnosti v daném technickém díle? 2. Jaká kritická nebo hodnotná zařízení jsou v daném technickém díle nebo jeho v jeho okolí? 3. Je známo, kde je kritický majetek technického díla umístěn? 4. Byli při hodnocení kritického majetku zváženi lidé, podniky a provozy? 5. Jsou plně dokumentovány kybernetické sítě (např. SCA-		

	DA systémy, internetové sítě aj.)?		
Dopady ztrát	1. Jsou určeny ztráty při selhání či havárii daném technického díla? 2. Bude možno technické dílo po selhání nebo havárii provozovat v původním rozsahu? 3. Je připraveno, jak zajistit kontinuitu provozu kritických zařízení během havárie nebo selhání technického díla? 4. Je známo, jaký potenciál pohromy (tj. velikost ohrožení od pohromy) způsobuje bezprostřední a významné místní dopady, které způsobí ztrátu technickému dílu? 5. Je známo, jaký potenciál pohromy (tj. velikost ohrožení od pohromy) způsobí nepřijatelné dopady na lidi a životní prostředí v okolí technického díla? 6. Je známo, jak ztráty technického díla ovlivní podnik, personál, vlastníka a popř. nezúčastněné? 7. Je známo, jak se odrazí ztráty technického díla na lidských životech, národním a místním bezpečí (pocitu jistoty)? 8. Je známo, jak se odrazí ztráta technického díla na finančních rozpočtech místního společenství?		
Hodnota majetku	1. Existují malé nebo neexistují žádné zálohované kapacity, které by mohly zmírnit ztráty technického díla? 2. Je známo, jaký je potenciál pohromy a s ním spojená ztráta technického díla vyvolá vznik kaskády jevů (např. dopady na další vzájemně závislé infrastruktury nebo průmyslová odvětví)? 3. Je známo, jak ovlivní ztráty technického díla situace spojené např. s nemocnicemi, obslužnými systémy, nouzovými službami, které jsou s tímto majetkem spojeny? 1. Je znám potenciál katastrofických dopadů, tj. úplného zničení nebo destrukce technického díla? 2. Je známo, kolik bude stát obnova technického díla? 3. Je známo, jak dlouho bude trvat oprava technického díla a hlavně jak dlouho budou přerušené služby s ním spojené a co to bude znamenat pro život v okolí? 4. Je známo, jak je třeba chránit kritický majetek technického díla?		
2. Identifikovat, co chrání a podporuje kritický majetek	Je zváženo, že každá infrastruktura závisí na mnoha dalších infrastrukturách, a že právě tyto vnitřní závislosti jsou její největší zranitelnosti?		
Rozpoznat závislosti napříč infrastrukturou	1. Je určeno, kdo odpovídá za zajištění bezpečnosti kritické infrastruktury technického díla? 2. Je určeno, jak je zabezpečení kritické infrastruktury prováděno? 3. Je zajištěna fyzická ochrana kritické infrastruktury? 4. Je známo, jaké jednotlivé prvky ochrany - např. zdi, střecha/přístup, okna, dveře, brány, jsou použity a jaký stupeň bezpečí poskytují?		

	5. Je v provozu systém detekce narušení technického díla či jeho kritické infrastruktury? 6. Jsou použity při ochraně technického díla a jeho kritické infrastruktury – bezpečnostní systémy, systémy související s bezpečností? 7. Je známo, proti jakým pohromám a nežádoucím jevům jsou technické dílo a jeho kritická infrastruktura chráněny? 8. Je známo, za jakých podmínek pracují zabezpečovací systémy technického díla a jeho kritické infrastruktury a pracují nepřetržitě nebo v jiném režimu? 9. Je známo, co chrání zabezpečovací systémy technického díla a jak? 10. Existuje přehled o možných projektových selháních (a to jednoduchých i vícestupňových) zabezpečovacího systému technického díla a jsou tato pravidelně vyhodnocována? 11. Je známo, jaká je korelace mezi účinností zabezpečovacího systému a hodnoceními v bezpečnostní dokumentaci technického díla, kde jsou hodnocení možných scénářů selhání zabezpečovacího systému technického díla? 12. Jsou uzavřeny spolupráce technického díla se samosprávou, policií, hasiči, lékařskou záchrannou službou, armádou a veřejnými službami?		
Majetek a infrastruktura	1. Jaké infrastruktury (interní a externí) jsou základní pro kritický majetek technického díla? 2. Je známo, která služba je běžným poskytovatelem každé infrastruktury pro každý kritický majetek technického díla a jak je každá infrastruktura spojena s každým majetkem technického díla (např. typy a trasy vedení, potrubí, a kabely)?		
Alternativy	1. Je známo, jaké alternativy zálohování služeb spojených s infrastrukturou technického díla jsou dostupné, když normální provoz obslužných systémů je narušen a jak dlouho tyto mohou podpořit kritické funkce technického díla? 2. Je známo, jaký je potenciál dopadů vnitřních závislostí (např. na dodávky elektřiny, vody a potravin, dopravu, finance, nouzové služby atd.) na technické dílo?		
Ochrana a citlivé informace	1. Je známo, jaké typy informací o technickém díle a jeho infrastruktuře, jejím majetku a provozu jsou kritické nebo citlivé? 2. Je známo, pomocí jakých metod a prostředků mohou být citlivé informace technického díla zneužity (rozladění zaměstnanci, přístup veřejnosti, tisk, Internet aj.)? 3. Jsou k dispozici koncepce a postupy na ochranu citlivých informací technického díla?		
3. Identifikovat a charakterizovat dopady útoků	1. Je známo, jaké typy nepřijatelné dopadů lze očekávat při útoku na technické dílo? 2. Je známo, jaké specifické nepřijatelné dopady lze očekávat při útoku na technické dílo?		

	3. Je známo, co nastane, když dojde k velkému útoku na technické dílo? 4. Je známo, jaký kritický majetek technického díla bude napaden při útoku? 5. Je známo, že v případě útoku na technické dílo si může být protivník vědom, jak nejlépe zničit kritický majetek technického díla? 6. Je znám pravděpodobný režim útoku na technické dílo (např. výbušnina nebo zápalná bomba dovezené autem, nákladním autem, letadlem, sabotáž, chemikálie, bojové biologické prostředky, radioaktivní materiál, kybernetický útok)? 7. Je známo, že útočník na technické dílo může mít další cíle? 8. Jsou známy pravděpodobnosti, že útočník si vybere určité metody útoku na technické dílo? 4. Jsou známy zvláštní události, které mohou protivníka donutit k útoku na technické dílo?		
4. Identifikovat a analyzovat zranitelnosti	1. Je známo, jak citlivý je každý kritický majetek technického díla na pohromy dle typu? 2. Je známo, jak citlivý je každý kritický majetek technického díla na fyzický útok? 3. Je známo, jak citlivý je každý kritický majetek technického díla na útok insiderů? 4. Je známo, že nějaký kritický majetek technického díla je nechráněný? 5. Je známo, že nějaký kritický majetek technického díla je málo chráněný? 6. Je známo, jak je kritický majetek technického díla citlivý na kybernetický útok?		
5. Hodnocení rizik a určení priorit pro ochranu	Je provedeno skórování rizik za použití rozhodovací matice?		
6. Identifikovat možnosti na zmírnění, náklady a dohody o pomoci	1. Jsou přijata opatření na zmírnění dopadů havárie či selhání technického díla na technické dílo? 2. Jsou místní veřejnou správou přijata opatření na zmírnění dopadů havárie či selhání technického díla na okolí technického díla? 3. Zná místní veřejná správa zranitelnosti kritických infrastruktur a má schopnost pomoci zvládnout technickému dílu dopady havárie či selhání technického díla na technické dílo? 4. Má místní veřejná správa schopnost zajistit přežití obyvatel při selhání či havárii technického díla?		

V případě systémového pojetí technického díla (SoS); existence nelinearit v chování technického díla; potřeby zajistit koexistenci technického díla s okolím; potřeby aplikovat přístup All-Hazard-Approach; potřeby aplikovat přístup Defence-In-Depth

(ochrana do hloubky); a potřeby řešit při řízení bezpečnosti technického díla možné konflikty, je třeba dle [3] při řízení:

1. Posoudit, zda při umístění, výstavbě a provozu jsou adekvátně zvažovány všechny možné pohromy v daném místě a jaký typ opatření z oblasti řízení pohrom jsou na ně zacílené.
2. Posoudit pro každou možnou specifickou pohromu nedostatky z pohledu aplikace přístupu Defence-In-Depth.
3. Posoudit pro každou kritickou pohromu vliv možných spřažení.

V praxi byly odzkoušeny tři typy kontrolních seznamů pro identifikaci kritických míst v řízení bezpečnosti technického díla

Tabulka 12 obsahuje kontrolní seznam pro stanovení kritičnosti technického díla na základě identifikace nedostatků z pohledu aplikace přístupu All-Hazard-Approach. Při vyplňování tabulky se zvažují všechny pohromy obsažené v seznamu All-Hazard-Approach upraveného pro Evropu [16,18], tj. i= 1,2,....,n.

Tabulka 13 obsahuje kontrolní seznam pro stanovení kritičnosti technického díla na základě identifikace nedostatků z pohledu aplikace přístupu Defence-In-Depth. Zvažují se pouze specifické pohromy v daném území (i= 1,2,....,N), které mají dopady na technické dílo, které vyžadují opatření a činnosti odezvy.

Tabulka 14 obsahuje kontrolní seznam pro stanovení kritičnosti technického díla na základě identifikace nedostatků v řízení technického díla při výskytu kritické pohromy (i = 1,2,...,K).

Z logického důvodu platí ***n > N > K.***

Tabulka 12. Kontrolní seznam pro identifikaci nedostatků z pohledu aplikace přístupu All-Hazard-Approach. Berou se v úvahu všechny pohromy obsažené v seznamu All-Hazard-Approach upraveného pro Evropu [16,18], tj. i= 1,2,....,n; u pohrom, které v daném místě nejsou možné, tj. nejsou relevantní, se řádky začerní nebo nevyplňují.

Pohroma – název i= 1,2,....,n.	Je pohroma relevantní?		Patří-li pohroma do kategorie specifických pohrom, je to zohledněno v umístění, projektování, výstavbě objektu účinnými preventivními technickými opatřeními?		Patří-li pohroma do kategorie specifických pohrom, je to zohledněno v provozu objektu účinnými preventivními organizačními opatřeními?		Patří-li pohroma do kategorie kritických pohrom, je to zohledněno v provozu objektu reaktivními opatřeními na ochranu zaměstnanců, technologie a životního prostředí uvnitř objektu?		Patří-li pohroma do kategorie kritických pohrom, je to zohledněno v provozu objektu reaktivními opatřeními zaměřenými na ochranu zaměstnanců, technologie, lidí a životního prostředí uvnitř i vně objektu?	
	NE	ANO	NE	ANO	NE	ANO	NE	ANO	NE	ANO

.....										
n										
CELKEM										

Tabulka 13. Kontrolní seznam pro identifikaci nedostatků z pohledu aplikace přístupu Defence-In-Depth; i= 1,2,....,N; N je počet specifických pohrom.

Pohroma i=1,2,....,N	**Otázka**	**Odpověď**		**Pozn.**
		ANO	**NE**	
1	1. Má technologický systém zapracované principy inherentní bezpečnosti, tj. bezpečného designu?			
	2. Má řídicí systém technologického systému (SMS) nastaveny základní řídící funkce, alarmy a reakce operátora nastaveny tak, aby se technologický systém udržel v normálním (stabilním) stavu?			
	3. Má řídicí systém (SMS) instrumentace (zabudované bezpečnostní instrukce) a příslušné fyzické bariéry, které při odchylce od normálního stavu udrží technologický systém v dobrém stavu, tj. zabrání výskytu nežádoucího jevu? Provoz je úspěšný, když se po výskytu abnormálního stavu technologický systém vrátí do normálního stavu v důsledku resilience nebo po aplikaci nápravných opatření (vyčištění, oprava, výměna části).			
	4. Má řídicí systém (SMS) pro případ ztráty kontroly, tj. kritické podmínky opatření pro nouzovou odezvu, kterými se zmírní dopady na technologický systém a zajistí se schopnost návratu do normálního stavu? Provoz technologického objektu je úspěšný, když je dobrý plán kontinuity, který zajistí, že technologický systém zajistí nezbytné úkoly.			
	5. Má řídicí systém (SMS) pro případ ztráty kontroly, tj. nadkritické (nadprojektové, extrémní) podmínky opatření pro: - udržení provozuschopnosti technologického systému po jeho opravě a údržbě, - a opatření pro zajištění ochrany veřejných aktiv (lidí, životního prostředí a dalších aktiv) v okolí technologického systému?			
2	1. Má technologický systém zapracované principy inherentní bezpečnosti, tj. bezpečného designu?			

	2. Má řídicí systém technologického systému (SMS) nastaveny základní řídící funkce, alarmy a reakce operátora nastaveny tak, aby se technologický systém udržel v normálním (stabilním) stavu?			
	3. Má řídicí systém (SMS) instrumentace (zabudované bezpečnostní instrukce) a příslušné fyzické bariéry, které při odchylce od normálního stavu udrží technologický systém v dobrém stavu, tj. zabrání výskytu nežádoucího jevu? Provoz je úspěšný, když se po výskytu abnormálního stavu technologický systém vrátí do normálního stavu v důsledku resilience nebo po aplikaci nápravných opatření (vyčištění, oprava, výměna části).			
	4. Má řídicí systém (SMS) pro případ ztráty kontroly, tj. kritické podmínky opatření pro nouzovou odezvu, kterými se zmírní dopady na technologický systém a zajistí se schopnost návratu do normálního stavu? Provoz technologického objektu je úspěšný, když je dobrý plán kontinuity, který zajistí, že technologický systém zajistí nezbytné úkoly.			
	5. Má řídicí systém (SMS) pro případ ztráty kontroly, tj. nadkritické (nadprojektové, extrémní) podmínky opatření pro: - udržení provozuschopnosti technologického systému po jeho opravě a údržbě, - a opatření pro zajištění ochrany veřejných aktiv (lidí, životního prostředí a dalších aktiv) v okolí technologického systému?			
	.....			
N	1. Má technologický systém zapracované principy inherentní bezpečnosti, tj. bezpečného designu?			
	2. Má řídicí systém technologického systému (SMS) nastaveny základní řídící funkce, alarmy a reakce operátora nastaveny tak, aby se technologický systém udržel v normálním (stabilním) stavu?			
	3. Má řídicí systém (SMS) instrumentace (zabudované bezpečnostní instrukce) a příslušné fyzické bariéry, které při odchylce od normálního stavu udrží technologický systém v dobrém stavu, tj. zabrání výskytu nežádoucího jevu? Provoz je úspěšný, když se po výskytu abnormálního stavu technologický systém vrátí do normálního stavu v důsledku resilience nebo po aplikaci nápravných opatření (vyčištění, oprava, výměna části).			
	4. Má řídicí systém (SMS) pro případ ztráty kontroly, tj. kritické podmínky opatření pro nouzovou odezvu, kterými se zmírní dopady na technologický systém a zajistí se schopnost návratu do normálního stavu? Provoz technologického objektu je úspěšný, když je dobrý plán kontinuity, který zajistí, že technologický systém zajistí nezbytné úkoly.			

	5. Má řídicí systém (SMS) pro případ ztráty kontroly, tj. nadkritické (nadprojektové, extrémní) podmínky opatření pro: - udržení provozuschopnosti technologického systému po jeho opravě a údržbě, - a opatření pro zajištění ochrany veřejných aktiv (lidí, životního prostředí a dalších aktiv) v okolí technologického systému?			
CELKEM				

Tabulka 14. Kontrolní seznam pro identifikaci kritických míst technického díla při výskytu kritické pohromy (i= 1,2,....,K); výsledky expertního šetření jsou: 3, je-li odpověď ANO; 2, je-li odpověď spíše ANO; 1, je-li odpověď spíše NE; 0, je-li odpověď NE; K je počet kritických pohrom.

Kritická pohroma i= 1,2,....,K.	**Jsou zajištěna ochranná opatření a činnosti pro**					**Jsou zajištěny ochranné postupy pro špatnou odezvu?**	**Jsou zajištěny ochranné postupy pro špatné řízení provozu?**	**Jsou zajištěny ochranné postupy pro aplikaci špatných předpisů?**
	zaměstnance a lidi v okolí přítomné v objektu	**provoz technologie**	**životní prostředí v okolí**	**lidi v okolí objektu**	**obnovu provozu do 14 dní**			
1								
2								
.....								
K								
CELKEM								

Předmětné tabulky jsou používány v praxi [63] s tím, že hodnotové stupnice jsou v první fázi nastaveny shodně, jako byly původně nastaveny pro ČSN [3], tabulka 15, což je blízké stupnici, kterou používá FEMA; viz údaje v práci [16].

Tabulka 15. Hodnotová stupnice.

Míra kritičnosti	**Hodnoty 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 %

Další kontrolní seznamy připravené pro technická díla jsou v pracích [2-4,17,66]. Pomocí kontrolních seznamů se odhalí kritická místa, kterým je třeba věnovat specifickou pozornost z hlediska bezpečnosti technického díla. V případě použití kontrolního seznamu jak DSS se určí položky, které zvyšují kritičnost technického díla, kterým je třeba věnovat pozornost.

Řada údajů o stupnicích je v práci [17]. Tabulka 16 ukazuje stupnici pro stanovení kritičnosti technického díla, která se podle prací [91-93] používá v oblasti BOZP.

Tabulka 16. Stupnice pro míru kritičnosti technického díla používaná v BOZP.

Hodnota kritičnosti	**Verbální popis**	**Dopady**
1	Zanedbatelná	Žádná ztráta pracovních hodin; není nutná první pomoc
2	Malá	Žádná ztráta pracovního dne; není trvalý dopad a ambulantní vyšetření; požadovaná první pomoc
3	Střední	Malé zranění; potřeba ambulantní ošetření
4	Vážná	Vážné zranění; dlouhodobá pracovní neschopnost; nemoc z povolání
5	Katastrofická	Smrt; trvalá neschopnost

Tabulka 17 je propojená s tabulkou 16 a ukazuje stupnici pro stanovení kritičnosti technického díla sestavené na základě matice rizika podle práce [92], která se rovněž používá v BOZP.

Tabulka 18 je propojená s tabulkou 17 a obsahuje stupnici pro určení přijatelnosti rizika a souvisejících reakcí podle prací [3,92], která se používá v BOZP.

Tabulka 17. Stupnice pro míru kritičnosti ve formě matice používaná v BOZP.

Hodnota kritičnosti	**Míra rizika**				
	Pravděpodobnost výskytu				
	nezvyklá	nepravděpodobná	Možná	pravděpodobná	téměř jistá

Zanedbatelná (1)	1	2	3	4	5
Malá (2)	2	4	6	8	10
Střední (3)	3	6	9	12	15
Vážná (4)	4	8	12	16	20
Katastrofická (5)	5	10	16	20	25

Tabulka 18. Určení přijatelnosti rizika a reakcí BOZP.

Úroveň rizika	**Přijatelnost rizika**	**Doporučená akce**
Malé (1-3)	Přijatelné	Žádná protiopatření nejsou potřeba. Je třeba monitorovat ohrožení od prioritních / kritických pohrom a zranitelnost aktiv, aby se riziko nezvýšilo během času
Střední (4-12)	Tolerovatelné	Po pečlivém vyhodnocení ohrožení od kritických pohrom je třeba zajistit, aby úroveň rizika byla snížena dle principu ALARA během stanovené rozumné doby Opatření dočasného řízení rizika administrativního charakteru nebo osobních ochranných pomůcek musí být aplikovány po dobu, dokud dlouhodobá opatření nebudou zavedena do praxe. Správa /management technického díla musí situaci sledovat.
Velké (15-25)	nepřijatelné	Úroveň rizika musí být redukována alespoň na úroveň střední před zahájením provozu. Opatření na snížení úrovně rizika nemohou spočívat pouze v použití osobních ochranných pomůcek a prostředků. Když je to možné, tak by měla být velikost ohrožení snížena před zahájením provozu. Před zahájením provozu musí být proveden audit.

Zdroje rizik dle práce [14] pro oblast BOZP (bezpečné pracoviště, bezpečná osoba, bezpečné technické dílo) se rozdělují do tří dále uvedených kategorií:

1. Pro bezpečné místo je třeba sledovat:
   - nouzovou připravenost přítomných,
   - kvalitu přítomných zařízení,
   - přítomnost nebezpečných látek,
   - úroveň hluku,
   - kvalitu elektrických zařízení,
   - skutečnost, zda je provedeno základní hodnocení rizika,
   - skutečnost, zda se provádí inspekce a monitoring místa s ohledem na rizika,
   - skutečnost, zda se sleduje bezpečí lidí,
   - kvalitu nakládání s odpadem,
   - kvalitu strojů,
   - kvalitu úklidu,
   - kvalitu systému řízení změn,

- kvalitu preventivní údržby a oprav,
- kvalitu a rozmístění vchodů a východů,
- kvalitu ergonomických hodnocení,
- úroveň radiace,
- přítomnost a úroveň biologických ohrožení,
- kvalitu přejímání a odebírání materiál, zboží atd.
- kvalitu věcí pro životní pohodlí a pro životní prostředí.

2. Pro bezpečnou osobu je třeba sledovat:
   - úroveň výcviku,
   - kvalitu popisu práce a struktury úkolů,
   - schopnost poskytnutí první pomoci,
   - existence a kvalitu osobních ochranných zařízení,
   - způsoby řešení konfliktů a způsoby rozhodování,
   - kvalitu a úroveň odhadu výkonu osoby,
   - existence a kvalitu možnosti zotavení pracovníka při a po namáhavé práci,
   - kvalitu asistenčních programů pro zaměstnance (nebo v území pro občany ze strany veřejné správy),
   - kvalitu organizace práce a způsoby vypořádání s únavou fyzickou i psychickou,
   - kvalitu a úroveň rovných příležitostí, tj. existují či neexistují opatření s ohledem na diskriminaci,
   - úroveň a kvalitu ubytování,
   - úroveň a kvalitu zdravotního dohledu,
   - úroveň a kvalitu zdravotních postupů,
   - úroveň a kvalitu dohledu nad návštěvníky a kontraktory (v území pak nad nežádoucími elementy),
   - úroveň a kvalitu kritérií výběru osob pro řízení a konkrétní úkony,
   - úroveň a kvalitu sledování vnímavosti ke stresu,
   - úroveň a kvalitu revize fluktuace osob,
   - úroveň a kvalitu programů odezvy a jejich zpětné vazby,
   - úroveň a kvalitu budování sociální sítě,
   - úroveň a kvalitu modifikace chování.

3. Pro bezpečné technické dílo je třeba sledovat:
   - úroveň a kvalitu řízení nehod (obecně nouzových situací všeho druhu) ze strany řídících pracovníků,
   - úroveň a kvalitu spolupráce řídících pracovníků s orgány pro bezpečnost práce při zvažování zdravotních aspektů,
   - úroveň a kvalitu politiky a postupů orgánů pro bezpečnost práce.
   - úroveň možnosti konzultací a postupů pro bezpečnou práci,
   - úroveň a kvalitu kompetentnosti řízení,
   - úroveň a kvalitu vytyčování úkolů,
   - úroveň a kvalitu služeb zákazníkům,
   - úroveň a kvalitu řízení kontraktorů,
   - úroveň a kvalitu alokace zdrojů,
   - úroveň a kvalitu odpovědnosti,
   - úroveň a kvalitu péče o záznamy a archivace,
   - úroveň a kvalitu modernizace legislativy,
   - úroveň a kvalitu komunikace,
   - úroveň a kvalitu souladu s kritérii orgánů pro bezpečnost práce,

- úroveň a kvalitu revize pracovních postupů, včetně analýzy mezer, nedostatků a revize systému,
- úroveň a kvalitu auditů,
- úroveň a kvalitu sebehodnocení,
- úroveň a kvalitu modernizace postupů.

Kritické vyhodnocení poznatků získaných studiem havárií [3,4,64] umožnilo určit položky spojené s vysokým rizikem takto:

1. Vysoké riziko pro bezpečné místo představují:
   - přítomnost nebezpečných látek,
   - neexistující nebo nekvalitní nouzová připravenost,
   - přítomnost elektrických zařízení,
   - přítomnost výrobních prostředků,
   - přítomnost přebírání či odebírání materiál, zboží apod.,
   - přítomnost vchodů a východů,
   - neprovádění nebo špatné provádění ergonomických hodnocení,
   - neprovádění nebo špatné provádění základního hodnocení rizika (často se porušuje).
2. Vysoké riziko pro bezpečnou osobu představují:
   - neexistující nebo špatný zdravotní dohled,
   - nesledování vnímavosti ke stresu,
   - neexistující nebo špatný dohled na návštěvníky a kontraktory,
   - nepoužívaná nebo špatně používaná osobní ochranná zařízení,
   - nekvalitní organizace práce a nerespektování únavy (často se porušuje).
3. Vysoké riziko pro bezpečný systém představují:
   - nekvalitní řízení nehod,
   - nemožnost konzultací,
   - špatné řízení kontraktorů,
   - špatná alokace zdrojů,
   - neprovádění nebo špatné provádění revize pracovních postupů, analýzy mezer a nedostatků,
   - nekvalitní zajištění odpovědnosti.

Vyhodnocení dopadů výše uvedených rizik a velikostí rizik spojených s člověkem (bezpečné místo, bezpečná osoba) z pohledu BOZP v návaznosti na stupnice použité v tabulkách 17 a 18 je uvedeno v tabulce 19.

Tabulka 19. Vyhodnocení rizika (L – pravděpodobnost; S – velikost; R – celkové skóre rizika).

Zdroj rizika	**Dopady realizace rizika**	**L**	**S**	**R**
Elektrická zařízení (zkrat / výboj)	Vážná zranění / úmrtí v důsledku zkratu nebo výboje	3	5	15
Požár	Dopady požáru – úmrtí způsobená ohněm nebo kouřem	5	5	25
Uklouznutí / zakopnutí	Zranění	4	3	12
Manuální na-	Zranění jako namožení svalu nebo pohmoždění svalu	2	3	6

kládání s těžkými předměty				
Nakládaní s potravou	Vysušení kůže v důsledku častého mytí. Některé druhy stravy nebo krmiva působí alergie	3	3	9
Strojírenství	Vážné úrazy při kontaktu s nebezpečnými nebo pohybujícími se částmi strojů	4	4	16
Tlakové systémy (parní kotle, potrubí, nádoby atd.)	Vážná zranění / úmrtí při explozi	3	5	15
Přeprava na pracovišti	Vážná zranění	3	3	9
Hluk	Diskomfort (nepříjemný pocit) až ohluchnutí v důsledku hluku na pracovišti nebo při používání hlučného zařízení	3	4	12
Teplota na pracovišti	Poškození zdraví v důsledku přehřátí nebo promrznutí organismu	3	3	9
Špatné ovzduší a špatná ventilace	Poškození zdraví v důsledku špatného ovzduší, nepříjemný pocit, pocení	1	3	3
Prach	Nemoci očí a nemoci plící v důsledku inhalace prachu, astma	4	3	12
Nedostatečné sanitární prostory	Zranění / nemoci	2	1	2
Nedostatečná hygiena	Nemoci	3	4	12
Problematické WC	Mikroorganizmy působí nemoci	3	3	9
Stress	Špatné řízení práce a šikana personálu	1	2	2
Nedostatek varovacích tabulek a bezpečnostní prevence	Zranění	4	2	8

4.5.8. Safety Audit (bezpečnostní kontrola)

Bezpečnostní kontrola je postup, při kterém se hledají nebezpečné položky, které mohou způsobit nebezpečné situace a navrhují se opatření na zvýšení bezpečnosti. Metoda představuje postup hledání potenciálně možné události nebo provozního problému, který se může vždy nebo jen za jistých podmínek objevit v posuzovaném systému. Formálně je používán připravený seznam otázek (kontrolní seznam) a matice pro skórování rizik [9]. Metoda v podstatě přísluší do skupiny metod pro předběžné posouzení ohrožení PHA (Preliminary Hazard Analysis), v rámci kterých je v praxi komerčně deklarována. Používá se pro různé průmyslové problémy a technologie, včetně peněžního sektoru (financial cash flows).

Bezpečnostní kontrola je postup založený na systematickém hledání nebezpečné situace a navržení opatření na zvýšení bezpečnosti. Např. ekologický audit (Eco-Audit) se zabývá aktuální prověrkou stávajícího stavu kvality životního prostředí. Jde o systematické, dokumentované a pravidelné prověřování vlivů stávajících výrobních procesů a technologií na životní prostředí a pravidelné vyhodnocování toho, jak pracuje nejen výrobní zařízení, ale také vedení společnosti v oblasti managementu ochrany životního prostředí. Formálně jde o postupy, které uplatňují zásady pro multivariantní řešení, alternativní posuzování výrobních technologií a práce s katalogy kritérií.

Bezpečnostní kontrola byla nepochybně první technika, která byla použitá pro identifikaci zdrojů rizika. Může být aplikována v jakékoli fázi průběhu, realizace procesu. Pro existující zařízení se obvykle skládá z inspekčních pochůzek, které mohou být informační, vizuálně rutinní, příp. až po přesné metodické týmové vyšetřování trvající několik týdnů. Bezpečnostní prohlídky jsou určeny pro identifikaci podmínek nebo provozních činností v podniku, které by mohly vést k nehodě, následně ke zranění, významné ztrátě na majetku nebo újmě na životním prostředí. Typická bezpečnostní prohlídka zahrnuje rozhovory s pracovníky, zaměstnanci podniku: operátory, údržbáři, inženýry, manažery, bezpečnostními pracovníky a jinými, v závislosti na organizační struktuře.

Na bezpečnostní prohlídky by mělo být nahlíženo jako na společné úsilí ke zlepšení všeobecné bezpečnosti podniku, nikoliv jako na narušování normálních činností nebo na trest za nalezené nedostatky. Spolupráce je základem pro identifikaci a snížení rizik. Bezpečnostní prohlídka se v prvé řadě soustřeďuje na závažné nouzové situace a doplňuje ostatní bezpečnostně procesní činnosti (jako je rutinní vizuální kontrola) a ostatní techniky identifikace zdrojů rizika (jako jsou analýza kontrolním seznamem a analýza „Co se stane, když …“). Na konci bezpečnostní prohlídky analytik navrhuje a doporučuje potřebná opatření a jejich opodstatnění, doporučuje odpovědnosti a termíny splnění. Může být naplánováno vyhodnocení nebo opakovaná inspekce k ověření, že nápravná opatření byla správně splněna.

Bezpečnostní prohlídky se používají pro ověření, že podnik a jeho provozní a údržbářské postupy odpovídají záměrům a normám. Výsledkem bezpečnostní prohlídky jsou kvalitativní popisy možných bezpečnostních problémů včetně podnětů k jejich nápravě. Zpráva inspekčního týmu zahrnuje seznam odchylek od projektových záměrů a od schválených postupů i seznam nově objevených bezpečnostních problémů. Odpovědnost za uplatnění nápravných opatření zůstává na podnikovém managementu. Pro vytvoření obsažné studie potřebují mít členové týmu přístup k:

- použitelným kódům a standardům,
- předešlým bezpečnostním studiím,

- podrobnému popisů procesu (P&ID, procesní toky),
- procedurám pro najíždění, normální provoz, odstávku a nouzové situace,
- zprávám o zraněních,
- zprávám o nehodách,
- zprávám o údržbě (revize přístrojů, testy pojistných ventilů, inspekce tlakových nádob),
- charakteristikám procesních materiálů (toxicita, informace o reaktivitě apod.).

Personál vykonávající bezpečnostní prohlídku musí být velmi dobře obeznámen s bezpečnostními standardy a postupy. Speciální technické dovednosti a zkušenosti jsou vítány pro vyhodnocování přístrojů, elektrických systémů, tlakových nádob, procesních materiálů a chemismu, atd.

4.6. Nástroje pro řízení rizik technických děl

Podle současného poznání základem kvalitního řízení bezpečnosti technického díla je cílené řízení rizik procesů v rámci řízení bezpečnosti technického díla [1,3,4,45,47,50]. Vzhledem k neznalostem a změnám v dynamickém vývoji světa, které nejsou lineární, je nutné zpracovávat u složitých technologických objektů komplexní nástroje, kterými jsou plány kontinuity a plány řízení rizik, ve kterých jsou připravena opatření pro řešení případných konfliktů [3,4].

Pro řízení bezpečnosti složitých technologických objektů je nezbytné používat nástroj, který vychází z integrální bezpečnosti, tj. respektuje systémové pojetí. Jelikož cíle různých systémů nejsou za všech podmínek konzistentní, ale nastávají konflikty, je třeba pro potřeby řízení a rozhodování používat multikriteriální přístup, tj. vytvářet vhodné a efektivní systémy pro podporu rozhodování (DSS) [2,9]. Všechny procesy v objektu musí být v každém okamžiku zacíleny na bezpečnost, viz schéma na obrázku 14, které navazuje na obrázek 3.

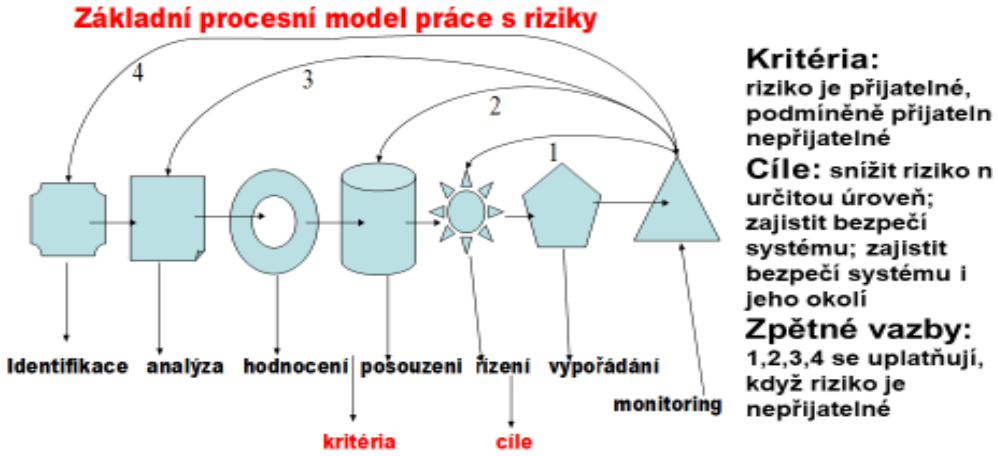
4.6.1. Základní modely používané při řízení rizik a řízení bezpečnosti technických děl

Podle [3] jsou nástroje pro ovládání složitých technologických objektů zacílené na bezpečnost, konkurenceschopnost a rozvoj. Jinými slovy jde o:
- zachování existence,
- ochranu a rozvoj chráněných aktiv,
- promyšlený řídicí systém zahrnující řízení strategické, taktické a operativní, který je založen na kvalifikovaných datech, odborných znalostech, expertních hodnoceních a dobrých metodách rozhodování,
- vzdělávání a výcvik zaměstnanců,
- podporu TSO, tj. profesních organizací, které provádí výzkum a zajišťují profesionální podporu provozovatele na úseku vývoje,
- specifické vzdělávání technických a řídících pracovníků,
- znalost a aplikace technických, zdravotních, ekologických, sociálních, kybernetických a dalších standardů, norem a předpisů, aby se zajistila obrana proti pohromám a zachoval soulad se státem,
- inspekce,

- systém spolupráce s veřejnou správou, s organizacemi na území a s organizacemi, které používají podobné technologie,
- personál pro zvládání nouzových situací,
- komponenty a systémy pro zvládání kritických situací (tj. všemi způsoby zajistit řízení kontinuity a krizové řízení); a bezpečnostní, nouzové a krizové plánování.

Obr. 14. Schéma řízení každého procesu ve složitém technologickém objektu.

Procesní model práce s riziky je uveden na obrázku 15; začíná se identifikací rizik a končí se sledováním rizik, která nebylo možno odstranit provedenými opatřeními, anebo jsou v čase proměnná.

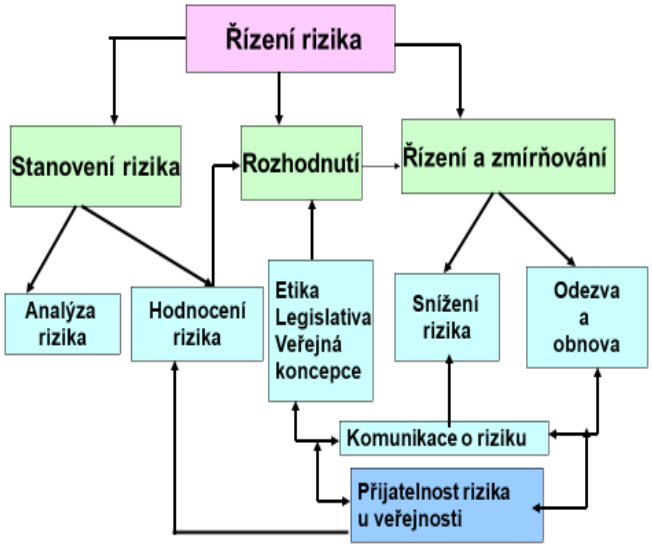


Obr. 15. Procesní model práce s riziky. Kritéria = podmínky, které stanovují, kdy je riziko přijatelné, podmíněně přijatelné nebo nepřijatelné. Cíle označují žádoucí stavy. Čísla 1,2,3,4 označují zpětné vazby, které se používají, když monitoring ukáže, že nejsou splněny stanovené požadavky na bezpečnost.

Na základě monitoringu se v případě, že velikost rizik překročí hranici přijatelnosti, provádí protiopatření; tj. aplikuje se dle závažnosti výše rizika některá ze zpětných vazeb vyznačených na obrázku 15 (z ekonomických důvodů se nejprve aplikuje zpětná vazba 1 atd.). Z obrázku 15 je zřejmé, že důležitý je výběr kritérií pro posu-

zování rizik (např.: která aktiva jsou sledována; zda vazba a toky mezi aktivy jsou sledovány jako aktiva apod.).

Model řízení rizik je na obrázcích 16 a 17, které jsou provázané; podrobnosti k modelům jsou v práci [2].



Obr. 16. Model řízení rizik entity.

Pro model řízení rizik je důležité, že bere v úvahu pohromu po pohromě a že jde o snížení rizika. Ukazuje jasné rozdělení prací s riziky:
- stanovení rizika provádí odborníci, protože mají data a znají příslušné metody,
- o rizicích rozhodují osoby, které mají příslušné kompetence, tj. v území veřejná správa a v technickém díle vlastník či provozovatel,
- řízení a zmírňování rizik provádí odborníci, tj. inženýři, technici a záchranáři, protože mají příslušné znalosti a dovednosti.

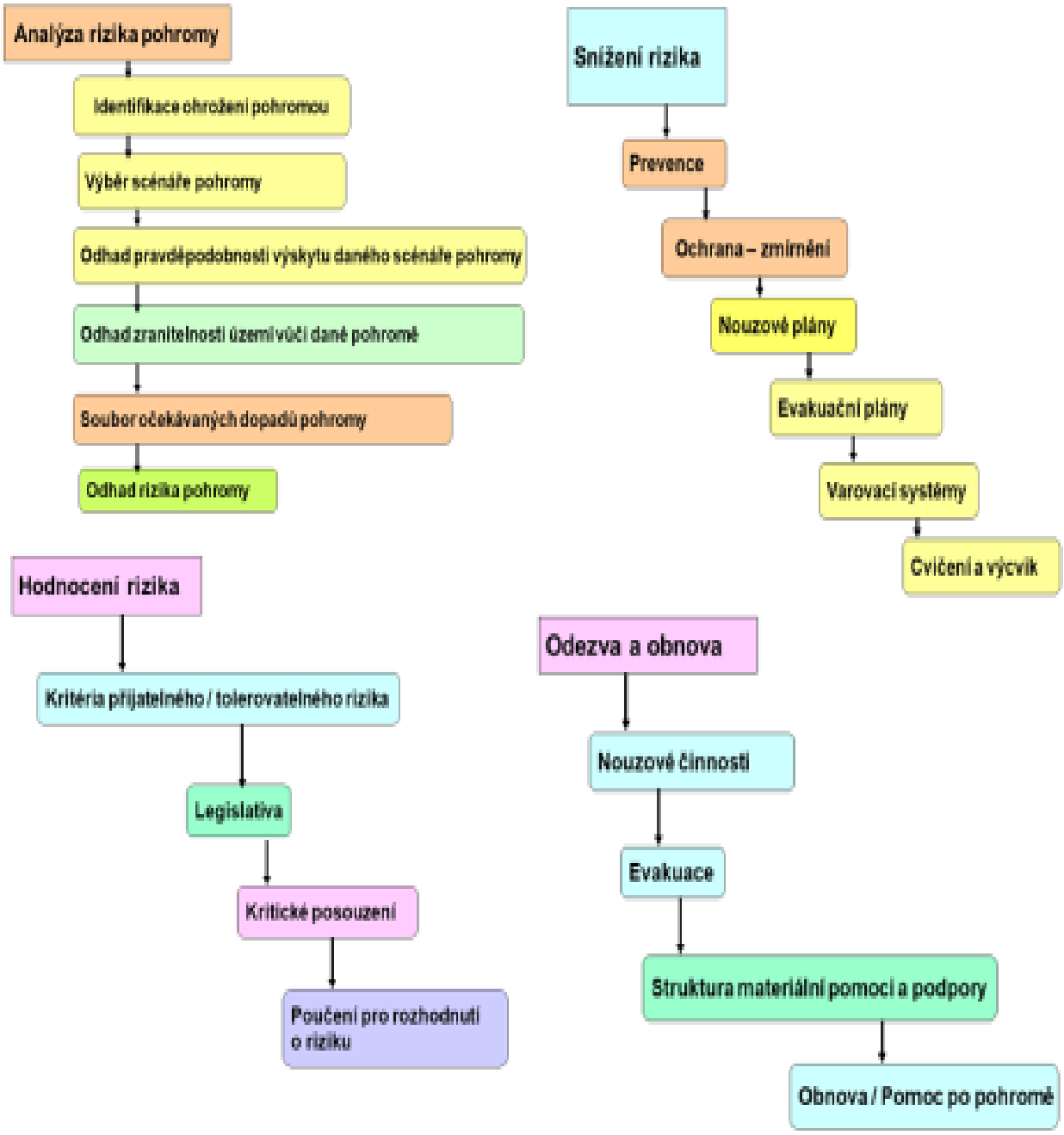
Pro stanovení rizik technického díla je důležité:
- jaká chráněná aktiva jsou sledována,
- jaké pohromy mohou vzniknout v daném místě / území / objektu a způsobit dopady na chráněná aktiva,
- jak je chápán proces, jehož výsledkem je realizace rizika (výskyt nepřijatelných dopadů jisté pohromy, výskyt kombinace malé pohromy a selhání bezpečnostních systémů nebo náhodná kombinace malých jevů,
- od jaké úrovně škod jsou dopady nepřijatelné.

V praxi používáme několik úrovní analýzy rizik:
A – předběžná analýza rizika,
B – standardní (rychlá a méně přesná) analýza rizika,
C – detailní analýza rizika v souhrnném kontextu,
D – individuální a specifická analýza rizika.

Jednotlivé úrovně se liší požadavky na kvalifikovaná data, jejich kvalifikované zpracování a vyhodnocení; největší nároky jsou vyžadovány při strategickém plánování zacíleném na bezpečný systém v dlouhodobém časovém měřítku.

Hodnocení dopadů pohrom v konkrétním místě je základní součástí jakéhokoliv pokusu o kvantifikaci a hodnocení rizika. Hodnocení rizika je strukturovaná procedura,

která se pokouší odpovědět na dále uvedené otázky:



Obr. 17. Rozpracování základních položek z obrázku 16.

- jaké ztráty, škody a újmy budou na chráněných aktivech při výskytu pohromy o určité velikosti?
- jak často se pohroma o určité velikosti vyskytne?
- jak zareagují bezpečnostní systémy ve sledovaném objektu, tj. v technickém díle či území?
- jaké ztráty, škody a újmy budou na chráněných aktivech, když selžou bezpečnostní systémy v technickém díle či území?

Podle cíle vyjednávání s riziky je nutno odlišovat metody, které jsou vhodné pro:

- identifikaci rizika,

- stanovení hodnoty rizika, ve kterém jde o přesný údaj pro potřeby strategického rozhodování,
- stanovení hodnoty rizika pro potřeby kontroly rizika konkrétního procesu v čase a prostoru, při kterém lze použít míru (a to i verbální) a o taktické a operativní rozhodování.

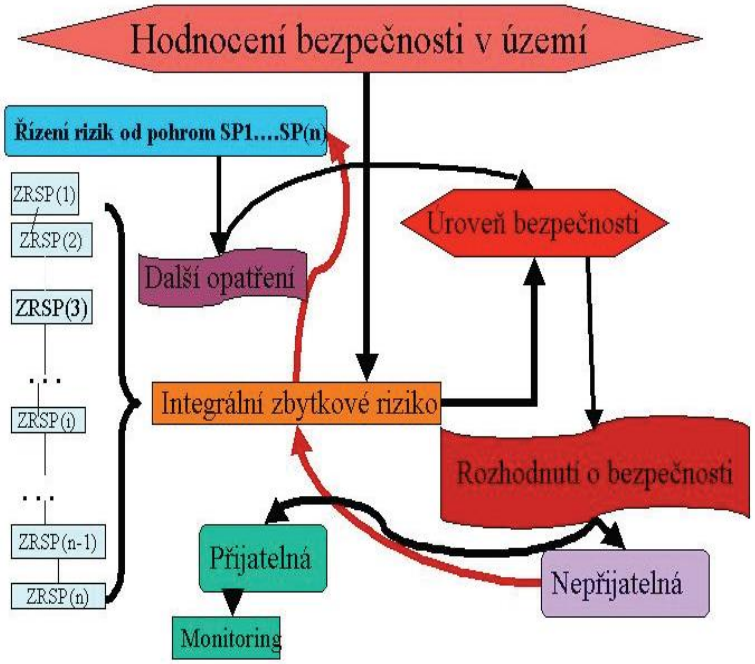
Aby hodnoty rizika měly jasnou vypovídací hodnotu, tak je důležité mít nejenom nástroj, ale jasně definovanou hodnotovou stupnici jak pro klasifikaci dílčích položek, dle kterých stanovujeme úroveň rizika, tak pro souhrn těchto položek.

Na základě [1-4,17] a zkušeností získaných přímo z šetření v praxi [62] v technické praxi platí:

1. Hodnocení rizik, která jsou spojená se strategickými cíli a operacemi musí zahrnovat faktory: externí a interní; sociálně – politické; technické a ekonomické. Musí brát v úvahu, že z hlediska zajištění rozvoje je třeba: prosazovat prevenci, tj. snížení zranitelnosti objektu, a tím i snížení rizik; pravidelné hodnocení rizik a sledování jejich aktuálnosti; prosadit změny specifických úprav určité činnosti; a revidovat adekvátnost hodnocení rizik.
2. Sociálně – politická rizika jsou obtížně kvantifikovatelná, např. politická stabilita, dopad teroristického útoku apod. Často se interní sociálně – politické faktory odlišují od externích (viz názor české a rakouské veřejnosti na jadernou elektrárnu Temelín). V dosavadní praxi se při jejich sledování používá:
   - sociologický přístup, který spočívá v tom, že se vytváří popis povahy rizika z pohledu sociálních skupin a vztahů se zaměřením na ekologická a sociální rizika a na aktivizaci veřejného mínění,
   - politická analýza, která tato rizika hodnotí pragmaticky a hledá jejich ekonomické dopady,
   - analýza rozložení rizik ve společnosti, která spočívá v identifikaci původce (zdroje) rizika, způsobu „šíření“ (realizace) rizika a „spotřebitele“ (skupiny lidí, která je postižena dopady realizace) rizika.
3. Technická rizika lze kvantitativně vyjádřit např. odchýlením od standardů určitého technického parametru, předpisů, norem apod. Není přesné, protože normy odpovídají mediánu ± σ, 68.5% případů. Tam, kde jde o vysokou bezpečnost, tam se nemohou použít běžné metody, pro které jsou software [3,17].
4. Ekonomická rizika lze rovněž kvantitativně postihnout, je však zapotřebí zvažovat nejen vzniklé situace, ale i předpokládaný hospodářský vývoj a politiku vlády. V makroekonomice se jedná o ekonomickou stabilitu země, směnné kurzy, dovozní a vývozní politiku, daňovou politiku apod. V mikroekonomice se může při jejich zanedbání zhoršovat ekonomická situace a platební schopnost podniků, a tím schopnost plnit závazky vůči zahraničním a domácím partnerům. Např. dochází k různému plnění vládních trendů v různých zemích a k různým změnám portfolia produktů v závislosti na uplatněných tendencích.
5. Kategorii zvládání rizika lze definovat jako výběr a implementaci nejpřijatelnějších regulačních činností, na podkladě předcházejících výsledků a různých vstupů [8] v podobě:
   - analýzy rizik,
   - dostupné řídící (kontrolní) technologie,
   - analýzy metodou nákladů a užitků CBA (Cost-Benefit Analysis),
   - rizika, přijatelnosti počtu případů; politické analýzy,

- sociálních a politických faktorů.

Řízení rizik ve prospěch bezpečnosti neboli zkráceně řízení bezpečnosti technického díla [2,3], obrázek 18, se provádí tak, že se zvažují všechna rizika od všech možných pohrom v daném technickém díle ***dohromady*** a dle stanovené úrovně bezpečnosti se vybírá soubor optimálních opatření pro vyjednávání se všemi specifickými a kritickými pohromami (relevantní pohroma je taková pohroma, která působí na organizaci, ale její dopady jsou přijatelné; specifická pohroma je pohroma, která má na organizaci nepřijatelné dopady; kritická pohroma je taková pohroma, která má kritické dopady, které mohou vést k rozložení až zániku organizace). Pozornost se věnuje i rizikům, která jsou málo pravděpodobná, ale dopady s nimi spojené vyvolají nebo mohou vyvolat velké ztráty, škody a újmy na chráněných zájmech, tj. uplatňuje se ***princip předběžné opatrnosti***.



Obr. 18. Model řízení bezpečnosti entity.

Přechod od klasického řízení rizik (obrázek 16) na řízení rizik zacílené na bezpečnost (anglicky Risk Governance) [1-3], obrázek 18 v praxi znamená:
- stanovit synergické vztahy mezi riziky, zranitelností a bezpečím,
- modelovat proces rozhodování správy organizace s ohledem na rizika, nejistoty a neurčitosti (viz podpůrné systémy rozhodování),
- specifikovat rámcové právní podmínky a ochranná opatření,
- zlepšovat činnosti institucí (institucionální změny).

Základním rozdílem mezi řízením rizik (obrázek 16) a řízením bezpečnosti (obrázek 18) je v tom, že v druhém případě se rozhodování provádí na základě míry bezpečnosti, která se stanovuje podle integrovaného rizika, které zvažuje všechny specifické pohromy (tj. pohromy, které mohou způsobit ztráty, škody a újmy na sledovaných aktivech).

Při práci s riziky je důležité aplikovat výsledky poznání, tj. aby řízení dosáhlo cílů, je nutné:
- používat jen podklady získané na základě kvalifikovaných dat, která splňují poža-

davky na reprezentativní datové soubory (úplnost, ocenění nejistot, vypořádání s neurčitostmi v datech pomocí specifických matematických přístupů),
- aplikovat správné metody rozhodování, které jsou adekvátní problému.

Dle zásad uvedených v pracích [1-4,17] platí, že pro:
- strategické řízení entity, které z pohledu zajištění existence je zacílené na bezpečnost, je třeba používat integrální riziko, a pro jeho zjištění ověřené reprezentativní datové soubory, ověřené metody pro zpracování dat a ověřené metody pro rozhodování, protože na tomto úseku je důležitá dlouhodobá udržitelnost,
- střednědobé (taktické) řízení možno používat integrované riziko, a pro jeho zjištění méně přesná data, metody zpracování dat i metody rozhodování (je možné použít software) s tím, že při rozhodování se budou respektovat záměry dané strategickým řízením,
- operativní řízení je možno používat dílčí rizika a na základě cíleně získaných znalostí a zkušeností použít naučené a procvičené postupy a nouzové situace zvládnout s tím, že se především soustředíme na životy a zdraví lidí a na další chráněná aktiva v technické entitě a jejím okolí.

Pro klasické řízení rizik i pro řízení rizik ve prospěch bezpečnosti [1-4,17], je nutné:

1. Rozumět procesu vzniku pohrom a podmínkám, ve kterých proces probíhá.
2. Znát, ve kterých místech pohroma může vzniknout a jaké může mít fyzikální a jiné charakteristiky.
3. Identifikovat ohrožení, které představuje v daném místě pohroma dle stanovených standardů.
4. Stanovit dopady pohrom o velikosti ohrožení na chráněné zájmy.
5. Eliminovat nepřijatelné dopady pohrom v případech, ve kterých to jde za přijatelných nákladů.
6. U zbylých dopadů vypočítat pomocí prognostických modelů pravděpodobnost jejich realizace s tím, že se vezmou v úvahu i možná selhání preventivních opatření.
7. Vypočítat možné škody na chráněné zájmy v konkrétním území podle chráněných zájmů, které jsou skutečně v území a na základě pravděpodobností určit výši rizika.
8. Identifikovat a realizovat zmírňující opatření s ohledem na lidi, majetek a životní prostředí tak, aby byla ALARP (tak malá, jak je rozumně možné dosáhnout).
9. Prokázat, že byla provedena všechna opatření k zabránění a zmírnění dopadů pohrom.

Přijatelné riziko pro technické dílo i jeho okolí lze dosáhnout snížením ohrožení od konkrétních pohrom, což však jde jen u pohrom, které souvisí s činností člověka, a především snížením zranitelnosti technického díla, která je předmětem hodnocení rizika.

Aby management technického díla mohl pracovat účinně s riziky, je třeba stanovit postup pro stanovení rizik právním předpisem a zároveň je třeba stanovit hodnotové stupnice, dle kterých se interpretují výstupy z nástrojů na stanovení rizik v organizaci, tj. je třeba určit, co je přijatelné, co je podmíněně přijatelné a co je nepřijatelné. Mezi nástroji pro stanovení rizik je třeba odlišit sofistikované nástroje pro odbornou sféru a nástroje pro řízení / správu organizace, pro kterou jsou nejvhodnější kontrolní se-

znamy. Mechanismus zvládání rizik v technickém díle pomocí legislativních pravidel je diskutován v pracích [1,3,4,10,17].

4.6.2. Obecné principy řízení bezpečnosti entit na základě řízení pohrom

Řada přístupů uvedených v odborné literatuře vychází při zajišťování bezpečnosti entit od škodlivých jevů, tj. pohrom. Proto pro vrcholové řízení bezpečnosti byl odsouhlasen v rámci programů OSN, a to IDNDR i ISDR postup řízení pohrom, který po přizpůsobení na technické dílo má dále uvedené postupné základní úkoly [1] rozpracované pro potřeby technického díla:

1. Určit seznam relevantních pohrom v území i v technickém díle.
2. Provést analýzu poznatků a zkušeností, spojených s každou relevantní pohromou s cílem:
   - v daném konkrétním místě a pro určité časové intervaly určit ohrožení od dané pohromy, tj. možnou velikost pohromy a jejich dopadů v místě technického díla, četnost výskytu této velikosti v určených časových intervalech,
   - pochopit rizika od dané pohromy v širokých souvislostech a určit cíle práce s riziky technického díla z pohledu zajištění jeho bezpečnosti,
   - projednat všechny aspekty rizik a aspekty řízení bezpečnosti technického díla z pohledu požadavků integrovaného systému,
   - identifikovat zdroje všech rizik, zranitelnosti, utrpení a možné ztráty spojené s danou pohromou v daném technickém díle,
   - vyjasnit možné problémy, spouštěcí mechanismy a podmínky při výskytu pohromy v technickém díle,
   - vytvořit možné scénáře pohromy s ohledem na místní podmínky v technickém díle,
   - zhodnotit dopady všech možných scénářů pohromy v technickém díle, zvláště z bezpečnostních aspektů,
   - odděleně zvážit újmy a škody na životech, majetku a životním prostředí v technickém díle a jeho okolí,
   - zvážit záznamy, empirické důkazy, zkušenosti a expertní posudky.
3. Provést hodnocení dopadů sledované pohromy v technickém díle takto:
   - objektivní kvantifikace všech parametrů a jejich neurčitosti,
   - výsledky citlivostní analýzy pro dynamickou situaci,
   - existující fyzikální omezení a špatně určitelné hranice některých charakteristických parametrů,
   - definovaný charakter dopadu pohromy i velikost možných dopadů,
   - četnost výskytu pohromy,
   - výsledky aplikace pravděpodobnostního přístupu.
4. Provést ocenění sledované pohromy ohledem na:
   - věrohodnost odhadnutého ohrožení (v absolutní i relativní míře),
   - přijatelnost ohrožení (z hlediska jednotlivce i společnosti),
   - ekonomický dopad na společnost a existující fondy pro obnovu technického díla a popř. jeho okolí,
   - náklady a zdroje při regulaci nejzávažnějších dopadů pohromy,
   - analýzu nákladů a užitků s ohledem na velikost rizik od dané pohromy,
   - přijatelnost, snížení nebo přenos rizik od dané pohromy.
5. Regulovat činnosti v dané oblasti s cílem:

- minimalizovat, zmírňovat a zvládat dopady pohromy, tj. aplikovat opatření, aby se: změnila pravděpodobnost výskytu pohromy a/nebo jejich velkých dopadů; snížila velikost dopadů; opatřily zdroje na zásah proti dopadům pohromy a na následnou obnovu,
- zvážit všechny možnosti na snížení velikosti dopadů pohromy, tj.: zavedení bezpečnostních opatření v projektu z pohledu prevence, ochrany a omezení škod; snížení neurčitosti v informacích o dopadech pohromy, soustavný monitoring klíčových částí technologie z hlediska velkých dopadů v případě pohrom, oprava a vylepšování systému řízení; zavedení norem a aplikování QC (kontroly kvality) na všech stupních; vytvoření obrany do hloubky (Defence-In-Depth) na paralyzování malých selhání; redukce pravděpodobnosti výskytu lidských chyb nebo zvrhlostí (výcvik a kultura bezpečnosti).

6. Soustavně ověřovat přijatou metodiku vrcholového řízení bezpečnosti technického díla s cílem:
   - testovat účinnost strategií na snížení dopadů pohrom v technickém díle,
   - provádět nezávislý bezpečnostní audit a inspekci dopadů pohrom v technickém díle,
   - ustanovit metodu na hlášení událostí (skoro nehod, havárií), která zahrnuje odezvy na dopady pohrom v technickém díle,
   - sledovat mechanismy zpětné vazby s cílem poučit se ze zkušeností a případně změnit priority ve vrcholovém řízení technického díla,
   - vytvořit programy, které zahrnují způsoby řízení, výcvik a postupy v případě výskytu dopadů pohromy v technickém díle,
   - zhodnotit celkové narušení technického díla ve všech fázích odezvy na pohromu (včetně všech narušení vyvolaných zásahem proti dopadům pohromy),
   - zavést mechanismus QA (kontroly jakosti) tak, aby všechny části řízení bezpečnosti v technickém díle společnosti byly optimálně vyváženy,
   - spojitě monitorovat, posuzovat a vylepšovat systém vrcholového řízení technického díla.

V řízení bezpečnosti se vyděluji čtyři základní fáze:
- prevence,
- připravenost,
- odezva,
- obnova.

Každá z těchto fází má svá specifika a jejich opatření musí být založena na kvalifikovaných datech a na kvalifikovaných hodnoceních. K nim pochopitelně patří i poučení ze zkušenosti z každé nepřijatelné situace.

4.6.3. Nástroje používané v jednotlivých fázích řízení bezpečnosti

Pro-aktivní řízení rizik je základem řízení bezpečnosti. Antropogenní opatření a činnosti se řídí tím, že na základě dostupných znalostí, sil a prostředků lidé provádí cíleně opatření s cílem pohromě a jejím dopadům zabránit, anebo alespoň dopady zmírnit se dostávají ve formě numerických i grafických výstupů, tj. používají se různé tabulky, mapy či zobrazení na GIS, které jsou instruktivní a pomohou zvláště těm, kteří nejsou hlubokými specialisty v příslušném oboru [2,3,4,9].

Rozhodovací proces je logicky návazná, účelná posloupnost kroků subjektu rozhodování od zjištění problému rozhodování až po formulaci rozhodnutí. Skládá se z následujících kroků:

- shromáždění a zpracování informací, přičemž zpracování musí být adekvátní problému, který sledujeme (např. to znamená, že metody zpracování dat pro potřeby řízení bezpečnosti musí respektovat, že velké pohromy s ničivou silou se vyskytují zřídka, a proto se musí používat postupy respektující zákon velkých čísel, tj. algoritmy založené na extrémních nebo mezních odhadech, viz práce [3,4,8,14] a odkazy v nich uvedené),
- rozpoznání variant řešení,
- hledání optimálního řešení problému,
- vlastního rozhodnutí.

Aby rozhodování bylo objektivní a kvalifikované, tak je třeba:
- mít dostatek spolehlivých informací, jejich objektivní zpracování a poznání vhodných reakcí,
- neustálá reakce na příliv nových poznatků,
- chápat řešené problémy v souvislosti k jejich okolí a v jejich vnitřní struktuře,
- vhodně kombinovat poznatky, zkušenosti a nové informace, aby byl získán účelný způsob řešení problému, základem je hodnocení věrohodnosti dat.

Při rozhodování je třeba zvažovat:
- posouzení současného stavu a současných rozhodnutí z hlediska budoucího vývoje,
- kvalitativní faktory a strategie různých účastníků,
- fakt, že budoucnost je mnohorozměrná a neurčitá,
- fakt, že každý systém je třeba zkoumat globálně i systémově,
- fakt, že informace i strategie nejsou neutrální, ale tendenční,
- více přístupů, které se doplňují,
- fakt, že existují předpojatosti strategií i lidí a zamezit jim.

Další údaje jsou např. v pracích [2-4,9,11].

Z poznatků shromážděných v pracích [1-4,11,13,17,20,25-34,43,44,47,48] vyplývá, že při řízení bezpečnosti je nutné respektovat:

1. Technické dílo má více chráněných aktiv a je otevřený systém systémů, mezi nimi existují různé vnitřní vazby a toky.
2. Odolnosti, zranitelnosti a adaptabilitu jednotlivých systémů i systému systémů. Kdy (při jaké kombinaci vlastností) je systém udržitelný?
3. Zásady pro řízení bezpečnosti systému systémů.
4. Legislativu pro podporu řízení bezpečnosti systému systémů.
5. Kontrolní mechanismy pro monitorování (úrovně) bezpečnosti systému systémů.

S ohledem na současné poznání je třeba sledovat v technickém díle vnitřní závislosti, které zprostředkovávají sekundární a další dopady pohrom na chráněná aktiva technického díla i aktiva veřejná. K tomuto cíli je třeba:
- zavést do praxe monitoring bezpečnosti,
- dopracovat a kodifikovat metodiky pro sběr dat, odborné zpracování veličin nutných pro analýzu rizik,
- vypracovat metodiky pro rozhodování o rizicích a systémy kontrolních seznamů na podporu rozhodování,
- pro zaměstnance vypracovat soubory opatření o tom, co mají dělat před, při a po pohromě, která v organizaci patří mezi specifické či dokonce kritické pohromy,

- pro potřeby strategického řízení technického díla zpracovat plány pro zajišťování bezpečí a rozvoje technického díla, nouzové plány, plány kontinuity a krizové plány organizace, které budou navzájem provázané a ve kterých budou podchyceny úkoly řízení bezpečnosti a rozvoje za všech okolností,
- zajistit podpůrné systémy pro podporu řízení bezpečnosti, protože kvalifikovaná řešení vždy ušetří peníze, síly i prostředky. Dosavadní poznání totiž ukazuje, že zjednodušená řešení jsou možná jen někdy, ale i v případech, ve kterých jsou možná, je třeba znát, jaká zjednodušení situace byla provedena a proč je bylo možno použít.

Nástroje bezpečnostní politiky, kterou se řízení bezpečnosti uvádí do praxe, jsou:
- koncepce, které vytyčují cíle bezpečnostní politiky,
- strategie, které určují základní způsoby, kterými bude cílů dosaženo,
- plány, které podrobně popisují a zahrnují činnosti v určitém časovém harmonogramu,
- nástroje a instituce, tj. zdroje, síly a prostředky, kterými se dosahuje splnění cílů bezpečnostní politiky.

Plánování tvoří základní součást každého řízení. Musí specifikovat nejen cíle, ale i rozpracovat možné varianty dosažení žádoucích cílů řízení, provést jejich vyhodnocení a výběr optimální varianty s ohledem na disponibilní síly, prostředky a zdroje. Poté je třeba provádět monitorování úspěšnosti vybrané varianty s ohledem na žádoucí cíl a systematicky odstraňovat nesoulady a překážky na cestě k realizaci vybraného cíle a přitom zabránit deformacím a ztrátě iniciativy účastníků procesu. K dosažení dlouhodobých cílů se používá strategické plánování a pro dosažení krátkodobých cílů plánování operativní; obě mají svá specifika, která předurčují výběr metod a způsobů.

Pro podporu správného řízení technického díla je také nutné analyzovat každou nouzovou situaci a přijmout poučení, tj. podklady pro zlepšení prevence, zajištění zmírnění dopadů příští situace na chráněná aktiva, pro zlepšení odezvy atd. Dle [1-4,11,13,17,20,25-34,43,44,47,50,54] je třeba:

1. Při každé větší nouzové situaci je třeba v rámci poučení:
   - určovat slabé a silné stránky technického díla a jejího systému řízení,
   - získat poznatky pro zvýšení odolnosti technického díla s tím, že bude zvyšována adaptabilita,
   - získat poznatky pro to, abychom robustní systémy odezvy zaměřovali správně.
2. Pro podporu řízení nouzových situací nestačí jen jednooboroví specialisté, ale je třeba mít specialisty, kteří znají více oborové a mnoha oborové disciplíny a systém řízení technického díla v daném případě. Každé technické dílo si musí tento odborný potenciál vybudovat k tomu, aby bylo schopné zvládat rozsáhlé nouzové a kritické situace.
3. Tým pro řízení nouzových situací se musí skládat z vysoce zkušených lidí, musí mít určitou nezávislost při rozhodování a musí mít vlastní zdroje pro činnosti odezvy. Jeho úkolem je zajistit urgentní a bezprostřední odezvu, řešit neočekávané problémy, orientovat se na důsledky, zajistit kvalifikovanou odezvu za přijatelných zdrojů, sil a prostředků.
4. Je nutné zvyšovat neustále bezpečnost technického díla i procesů, jichž se účastní zaměstnanci.

5. Odezva na hurikán Katrina v USA ukázala jeden důležitý fakt - za hranicemi kompetencí se v kritické situaci nedá téměř nic pořádného udělat [62]. Proto je důležité pro zvládnutí všech situací mít předem připravené rozdělení kompetencí pro všechny možné situace, tj. i pro ty téměř nemožné.
6. Zkušenosti získané studiem odezev na nouzové situace velkého rozsahu ukázaly, že práce, které se dělají v rámci odezvy na kritickou situaci, musí být:
   - jasné,
   - snadno proveditelné,
   - rychlé, aby podpořily účinnost akcí,
   - vést k výsledku.

Základní druhy plánování, které podporují základní úrovně řízení, jsou bezpečnostní plánování, nouzové plánování a krizové plánování.

Provedené teoretické analýzy i rozbory praktických postupů [1] ukázaly na nutnost při plánování obecně dodržovat zásady jako:

1. Plánovat s nadhledem, tj. neplánovat pro případy konkrétních pohrom, protože při výskytu konkrétních jevů jsou různé podmínky a dochází ke kumulaci různých faktorů, které zesilují nebo zeslabují působení pohromy a mění situaci v organizaci.
2. Nouzové situace vyvolané pohromami jsou jen v prvním okamžiku determinovány příčinou, tj. dopady konkrétní pohromy, která je vyvolala. Poté jsou determinovány dobou, po kterou trvají a rozsahem zasažené organizace.
3. V případě, že dojde k významnému zdržení v nastartování vhodné odezvy na pohromu, dochází ke kritické situaci, která může mít až katastrofické dopady, protože v důsledku domino efektů vznikají další a další řetězce nežádoucích jevů.
4. Plány rychle zastarávají, a proto jsou nezbytné pravidelné aktualizace a testování.
5. Bezpečnost, odolnost či zranitelnost každého systému je vždy daná nejslabším prvkem organizace.

Plánování bezpečného technického díla proto vyžaduje bezpodmínečně interdisciplinární přístup vycházející a navazující na koncept lidské bezpečnosti (společnost je posedlá strachem z narušení bezpečnosti, protože současná společnost je složitá a velmi zranitelná) a udržitelného rozvoje (ekologická odpovědnost má vztah k environmentální bezpečnosti, ekonomická účinnost souvisí s ekonomickou a technologickou bezpečností, sociální solidarita je odrazem sociální a zdravotní bezpečnosti atd.).

V případě, ve kterém neexistuje účinná obrana technického díla před pohromou, je nutností být připraven. To znamená, že správce technického díla musí mít připraveny postupy, jimiž se musí zajistit odezva na situaci zaměřená na stabilizaci zasažené části organizace a obnova kritických procesů a zdrojů pro jejich realizaci. Nouzové plánování neomezuje rizika a musí být na míru toho, kdo provádí odezvu i navazující obnovu. V žádném případě nejde o levnou záležitost. Jde o zajištění uspořádání souboru znalostí a o prosazení, že každá odpovědně řízená instituce bude mít bezpečnostní koncepci. Ta musí vycházet z klasifikace nouzových situací a z analýzy rizik zaměřené na zjištění očekávání, jaké dopady a jak jsou pravděpodobné při vzniku pohromy o očekávané (právně definované) velikosti.

Plánování je spolehlivé, když postupy:

- vedou k cíli pomocí optimálního způsobu, který lze zajistit disponibilními zdroji, silami a prostředky,
- jsou formalizované,
- obsahují opatření k omezení (zmírnění) dopadů,
- zajišťují kontinuální proces,
- umožní zvládnout možné situace,
- jsou multidisciplinární (tj. nejsou naivní a levné),
- respektují problémy v zajištění potřebných zdrojů, a proto s nimi neplýtvají,
- racionálně využívají bezpečnostní infrastrukturu.

Plány musí mít hierarchickou strukturu, protože hierarchické jsou jak procesy, tak zdroje. Nejčastěji se používají tři úrovně:

1. Analýza rizik, která stanovuje strategická pravidla:
   - základní klasifikace klíčových procesů a zdrojů a jejich zabezpečení,
   - plán zachování funkčnosti.
2. Zajištění dat a informací; jde o sestavení souboru znalostí a návrh cílů.
3. Seznam konkrétních realizačních opatření a návrh postupů na jejich realizaci (lze využít nástroje multikriteriálního rozhodování, např. metodu kritické cesty, Petriho sítě, optimalizační metody síťové analýzy apod. [9].

Musíme si uvědomit, že např. proces zvládnutí nouzové situace probíhá v opakujícím se životním cyklu:

1. Normální podmínky provozu.
2. Reakce na vznik nouzové situace vyvolané výskytem pohromy.
3. Obnova základních funkcí organizace.
4. Prozatímní provoz organizace.
5. Obnova plného provozu organizace.
6. Normální provoz organizace po obnovení plné funkce.

Obnova plného provozu znamená přechod z nouzového provozu organizace na plný provoz. Obvykle je nejvíce opomíjená.

Dalším příkladem je formální postup pro proces zvládání konkrétní nouzové situace, který je vždy v hlavních rysech tento:
- analýza rizik,
- zjištění dopadů, zranitelností a jejich ocenění,
- stanovení kritických procesů a zdrojů potřebných pro jejich realizaci,
- stanovení doby, za kterou musí být kritické procesy obnoveny, aby nedošlo k další eskalaci nouzové situace vyvolané pohromou. Jde totiž o to, aby příliš dlouho nepůsobila spřažení vzniklá v organizaci v důsledku vnitřních vazeb.

Pro každý kritický proces se nejprve pro potřeby řízení musí určit možné scénáře. Za vše odpovídá vrcholový management. Plán je ***komplexní obrázek o procesech a jejich závislostech.*** Plán má proto ***řešit problémy, porozumět budoucím situacím, formulovat priority a stanovit odpovědnosti***. Nástroje řízení, které stanovuje plán, jsou:
- soustava indikátorů,
- monitoring,
- cíle.

Podle těchto nástrojů jsou nastaveny všechny další části řízení. Když je plán formální, tak řízení je bezbřehé a není zajištěno dosažení cílů. Proto při každém plánování si je třeba uvědomit, že prostorové uspořádání, funkční využívání organizace i předurčení chování lidí je komplexní proces pro zajištění vzájemného souladu požadavků hospodářských a jiných činností.

Plánování v organizaci založené na stanovení cílů, odstranění možných problémů a na ceně, kterou organizace zaplatí za selhání, je zvláště nutné zaměřit se na ten majetek, který nejvíce vyžaduje investice a sledovat dopady na vazby mezi prvky a vazby napříč celého systému infrastruktury. Poslední výzkumy ukazují, že zvláště důležité je sledovat spletitost vnitřních závislostí napříč kritickou infrastrukturou. Při znázornění organizace jako systému se zjistí, že některé prvky, vazby či toky jsou vysoce zásadní pro stabilitu, kontinuitu a rozvoj organizace. V těchto případech je nutno v zájmu bezpečnosti provést specifická opatření a tyto prvky, vazby či toky speciálně zodolnit a případně zálohovat, a to i několikrát (např. u jaderných elektráren, jež jsou v provozu v České republice, je zálohování 300 %). To také platí pro dodávky kritického materiálu nebo pro zajištění kritických služeb (např. záložní zdroje elektrické energie).

Základním nástrojem pro plánování i řízení jsou procesní modely. Ty umožňují sestavit postupy a scénáře pro určité situace, které mají určité podobné rysy. Jsou vhodné pro plánování i pro odezvu a obnovu. Modely se sestrojují na základě konkrétních potřeb. *Základem jejich každé aplikace je požadavek, že k tomu, aby daly správný výsledek, musí být splněny předpoklady, na jejichž základě byly vytvořeny.* Výsledkem aplikace procesních modelů jsou normy, standardy, havarijní, nouzové, krizové a jiné plány, scénáře pohrom, scénáře odezvy, scénáře obnovy apod.

4.6.4. Logické postupy pro zajištění bezpečnosti

Protože zdrojů, sil a prostředků má vždy každá organizace nedostatek, tak pro řízení bezpečnosti je nutno se soustředit na priority. V první řadě to znamená na základě velikosti ohrožení od konkrétní pohromy a zranitelnosti organizace vůči konkrétní pohromě rozdělit existující pohromy do následujících skupin:

- pohromy, které nemohou mít dopady na organizaci,
- pohromy, které mají jen přijatelné dopady na organizaci, pro které používáme označení pohromy relevantní,
- pohromy, které mají v organizaci takové dopady, které jsou zvládnutelné při provedení připravených preventivních a zmírňujících opatření, pro které používáme označení pohromy specifické,
- pohromy, které mají v organizaci nepřijatelné dopady, a tudíž je nutné provést zásadní preventivní opatření v oblasti technické, organizační, právní i vzdělávací a je nutné mít možnost aktivovat všechna zdroje a prostředky na zvládnutí jejich dopadů a nastartování dalšího rozvoje, pro které používáme označení pohromy kritické. Tyto vyvolají nebo mohou vyvolat krizové situace.

Problémové oblasti při řízení bezpečnosti technického díla dle výzkumu provedeného v [58] jsou:

1. Ve kterém místě se v území, ve kterém je technické dílo může vyskytnout pohromy a jak jsou při výskytu pohromy v technickém díle rozloženy jejich dopady?
2. Jaké pohromy se v technickém díle mohou vyskytnout a jaké mají dopady?

3. Za jakých podmínek se jednotlivé pohromy v technickém díle mohou vyskytnout a jaké podmínky mohou způsobit eskalaci jejich dopadů?
4. Jak často se jednotlivé pohromy v technickém díle mohou vyskytnout?
5. Od jaké velikosti mají pohromy na technické dílo nežádoucí, tj. nepřijatelné dopady, které působí škody na chráněných aktivech, tj. i na prioritním majetku technického díla?
6. Jaká je maximální možná (očekávaná) velikost pohromy v daném technickém díle?
7. Jaké škody na majetku může vyvolat maximální možná pohroma určená na specifikované hladině věrohodnosti v organizaci a jaké jsou její dopady na majetek a ostatní chráněná aktiva technického díla?
8. Co se proti nežádoucím dopadům pohrom dá dělat v technickém díle na úseku bezpečnostního plánování, projektování, výstavby a provozu občanských i technologických objektů a infrastruktury a popř. v dalších oblastech jako jsou monitoring, inspekce, vzdělání aj., aby se zabránilo výskytu pohrom, kterým lze zabránit nebo aby se zabránilo jejich vysoce nepřijatelným dopadům, anebo aby se nepřijatelné dopady zmírnily preventivními opatřeními, připraveností, vhodnou odezvou na pohromu a obnovou, při níž bude respektována prevence ztrát a cíle udržitelného rozvoje?
9. Jaká opatření vůči konkrétním pohromám v technickém díle jsou žádoucí v oblasti technické, organizační, finanční, sociální, právní, vzdělání a výchovy?
10. Jaká nepřijatelná a zbytková rizika (tj. nežádoucí dopady s pravděpodobností výskytu vyšší než stanovená mez) s ohledem na možné pohromy v technickém díle zůstanou, když se provedou racionální opatření, která může správa technického díla zajistit v oblasti technické, organizační, finanční, sociální, právní, vzdělání a výchovy?
11. Jak provádět odezvu na pohromu, jaké jsou její priority, kritická místa apod.?
12. Jak provádět obnovu majetku po pohromě v technickém díle, aby se racionálně využily zdroje, síly a prostředky, aby se zamezilo dalším ztrátám, aby se zvýšila odolnost proti pohromám a aby se nastartoval další rozvoj technického díla se všemi položkami (majetkem, životním prostředím, infrastrukturou, službami apod.), na nichž je technické dílo závislé?
13. Jaká forma řízení a provádění obnovy majetku po pohromě v technickém díle je vhodná a jak ji lze realizovat?
14. Jak vytvořit finanční rezervu správy technického díla na racionální obnovu majetku po pohromě v technickém díle?

Strategie pro zajištění bezpečného technického díla [1-4,11,13,17,20] spočívá v:

- aplikaci systémového a proaktivního řízení, které se opírá o znalosti a zkušenosti získané pro technické dílo z kvalifikovaných dat,
- kvalifikované vyjednávání s riziky ve prospěch bezpečí a udržitelného rozvoje technického díla,
- vypořádání rizik pomocí prevence, zmírnění, pojištění, rezervy, připravenosti na odezvu a obnovu a sestavení plánu na zvládnutí nepředvídaných situací (contingency plan),

- aplikace správného řízení, ve kterém jsou provázané řízení bezpečnosti za normálních podmínek, nouzové řízení a krizové řízení,
- sestavení programu na zvyšování bezpečnosti technického díla,
- stanovení měr na posuzování úrovně bezpečnosti ve smyslu účinnosti bezpečnostního systému (indikátory),
- naplnění programu provázanými projekty + naplnění projektů provázanými procesy,
- adresné přidělení úkolů a odpovědností všem zúčastněným,
- realizace spojená s kvalifikovaným a důsledným monitoringem,

Základním principem je kvalifikované propojení řízení oblastí technické, organizační, finanční, personální, sociální, znalostní; jasné role a odpovědnosti všech zúčastněných. Systém řízení bezpečnosti (SMS) technického díla proto postihuje řadu oblastí, tj. technickou, vojenskou, legislativní, finanční, ekonomickou, sociální, ekologickou, vzdělávací, výzkumnou apod. Na úseku bezpečnosti a udržitelného rozvoje mají z hlediska současného poznání a současných koncepcí sofistikovaných bezpečnostních systémů úkoly všichni zúčastnění. Úkoly jednotlivých zúčastněných a jejich propojení v různých situacích stanoví právní předpisy, morální a jiné standardy a normy.

V rámci strategie pro zajištění bezpečí a udržitelného rozvoje technického díla [1] musí být:
- sestaven program na zvyšování bezpečnosti technického díla,
- míry pro posuzování úrovně bezpečnosti ve smyslu účinnosti bezpečnostního systému (indikátory),
- program na zajištění bezpečnosti naplněný provázanými projekty,
- projekty naplněné provázanými procesy.

Nástroje správy technického díla, které zajišťují bezpečí a rozvoj systému, tj. jinými slovy zachování či ochranu a rozvoj chráněných zájmů [1,3], jsou:
- provázaný systém řízení (strategické, taktické i operativní) založené na kvalifikovaných datech, odborných hodnoceních a správných metodách rozhodování,
- výchova a vzdělání zaměstnanců,
- věda, výzkum a TSO / odborné organizace zajišťující odbornou podporu organizaci,
- specifická výchova technických a řídících pracovníků,
- technické, zdravotnické, ekologické, společenské, kybernetické a jiné standardy, normy a předpisy, tj. nástroje pro regulaci procesů, které mohou nebo by mohly vést k výskytu (vzniku) pohromy nebo k zesílení jejich dopadů,
- inspekce,
- výkonné složky ke zvládnutí nouzových situací,
- systémy ke zvládnutí kritických situací (řízení kontinuity, krizové řízení),
- bezpečnostní, nouzové a krizové plánování.

Aby řízení bylo správné, je nutné nástroje kvalifikovaně používat. To znamená:
- používat podklady získané na základě kvalifikovaných dat, která splňují požadavky na reprezentativní datové soubory (úplnost, ocenění nejistot, vypořádání neurčitostí v datech pomocí specifických matematických přístupů),
- aplikovat správné metody rozhodování, které jsou adekvátní problému, o kterém se rozhoduje.

To znamená, že pro:

- strategické řízení technického díla, které je zaměřené na řízení bezpečnosti, je nutné ***používat ověřené datové soubory, ověřené metody pro zpracování dat a ověřené metody pro rozhodování***,
- střednědobé řízení technického díla, které je zaměřené na připravenost směrovanou na zvládnutí problémů spojených s nouzovými situacemi (povodně, havárie apod.) v technickém díle, je možno používat ***méně přesná data, metody zpracování dat i metody rozhodování*** (méně přesné procesní modely, software, odhady apod.), protože každá nouzová situace je jedinečná kvůli proměnným podmínkám při jejím vzniku a změnám v disponibilitě zdrojů, sil a prostředků správy technického díla na reakci,
- operativní řízení, kdy se rozhoduje v časové tísni a při nedostatku dat (odezva), je nutno ***na základě cíleně získaných znalostí a zkušeností použít naučené a procvičené postupy*** (zpracované např. formou případových studií), protože rychlá reakce je žádoucí.

Systém řízení bezpečnosti (tzv. SMS – Safety Management System) technického díla zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v území. Zpravidla se týká řady otázek, kromě jiného i organizace, pracovníků, identifikace a hodnocení ohrožení a z nich plynoucích rizik, řízení chodu organizace, řízení změn v organizaci, nouzového a krizového plánování, monitorování bezpečnosti, auditů a přezkoumávání [3]. Na základě citované práce SMS organizace se skládá z oblastí:

1. Oblast koncepce a řízení, která se dále dělí na podoblasti:
   - podoblast celkové koncepce,
   - podoblast dílčích cílů bezpečnosti,
   - podoblast vedení / spravování bezpečnosti,
   - podoblast systému řízení bezpečnosti,
   - podoblast personálu, která se dále dělí na úseky:
     * úsek řízení lidských zdrojů,
     * úsek výcviku a vzdělání,
     * úsek vnitřní komunikace / informovanosti,
     * úsek pracovního prostředí,
   - podoblast revize a hodnocení plnění cílů v bezpečnosti.
2. Oblast administrativních postupů, která se dále dělí na podoblasti:
   - podoblast identifikace ohrožení od možných pohrom a hodnocení rizika,
   - podoblast dokumentace,
   - podoblast postupů (včetně systémů pracovních povolení),
   - podoblast řízení změny,
   - podoblast bezpečnosti ve spojení s kontraktory,
   - podoblast dozoru nad bezpečností výrobků.
3. Oblast technických záležitostí, která se dále dělí na podoblasti:
   - podoblast výzkumu a vývoje,
   - podoblast projektování a montáže,
   - podoblast inherentně bezpečnějších procesů,
   - podoblast průmyslových standardů,
   - podoblast skladování nebezpečných látek,
   - podoblast údržby integrity a údržby zařízení a objektů.
4. Oblast vnější spolupráce, která se dále dělí na podoblasti:

- podoblast spolupráce se správními úřady,
- podoblast spolupráce s veřejností a dalšími zúčastněnými (včetně akademických pracovišť),
- podoblast spolupráce s dalšími podniky.

5. Oblast nouzové připravenosti a odezvy, která se dále dělí na podoblasti:
   - podoblast plánování vnitřní (on-site) připravenosti,
   - podoblast usnadnění plánování vnější (off-site) připravenosti (za kterou odpovídá veřejná správa),
   - podoblast koordinace činností resortních organizací při zajišťování nouzové připravenosti a při odezvě.
6. Oblast zpráv a šetření havárií / skoro nehod, která se dále dělí na podoblasti:
   - podoblast zprávy o haváriích, skoro nehodách a dalších poučných zkušenostech,
   - podoblast vyšetřování
   - podoblast odezvy a následné činnosti po nehodách (včetně aplikace poučení a sdílení informací).

Systém řízení bezpečnosti organizace se opírá o koncepce prevence pohrom či alespoň jejich závažných dopadů, která zahrnuje povinnost zavést a udržovat systém řízení, ve kterém jsou zohledněny dále uvedené problémy:

a) role a odpovědnosti osob podílejících se na řízení závažných ohrožení od pohrom na všech organizačních úrovních a opatření na zajištění výcviku, která jsou sladěna s identifikovanými potřebami výcviku,
b) plány pro systematické identifikování závažných ohrožení od pohrom a z nich plynoucích rizik, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti),
c) plány a postupy pro zajištění bezpečnosti všech komponent a funkcí v území, a to včetně údržby objektů, zařízení,
d) plány na implementaci změn v území, objektech i zařízeních,
e) plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na takové nouzové situace,
f) plány pro probíhající hodnocení souladu s cíli vyjasněnými v koncepci bezpečnosti a SMS a mechanismy pro vyšetřování a provádění korekčních činností v případě selhání s cílem dosáhnout stanovené cíle,
g) plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků.

Bezpečnost je záležitostí všech zúčastněných, tj. vedoucích pracovníků, zaměstnanců i náhodně přítomných. V těchto souvislostech se mluví o ***tzv. zlatých pravidlech všech zúčastněných*** [1,14], kterými jsou:

- dle svých možností preventivními opatřeními zabránit vzniku pohrom, anebo alespoň jejich nepřijatelným dopadům, zajistit připravenost na zvládnutí nepřijatelných dopadů na chráněná aktiva technického díla a účinnou odezvu technického díla,
- komunikovat a spolupracovat s ostatními zúčastněnými ve všech aspektech prevence, připravenosti a odezvy technického díla,
- znát ohrožení od pohrom a možná rizika v technickém díle a jeho okolí,

- implementovat a respektovat „kulturu bezpečnosti“, která je respektována a prosazována všemi zúčastněnými za všech okolností,
- zřizovat systémy řízení bezpečnosti, sledovat a popř. korigovat jejich činnost,
- používat principy inherentní bezpečnosti při navrhování, projektování a provozování objektů a jejich zařízení,
- pečlivě řídit změny v organizaci,
- být připraven na zvládnutí všech pohrom, které mohou nastat,
- pomáhat ostatním zúčastněným při vykonáváni jejich rolí a odpovědností,
- provádět neustálé vylepšování bezpečnosti,
- pracovat ve shodě s kulturou bezpečnosti, bezpečnými postupy a výcvikem,
- usilovat neustále o veškerou informovanost a poskytovat informace a pro řídící pracovníky zajišťovat zpětnou vazbu,
- usilovat o rozvoj, posilování a ustavičné zlepšování koncepce bezpečnosti, předpisů a směrnic,
- vést a motivovat všechny další zúčastněné k tomu, aby plnili své úlohy a odpovědnosti,
- znát rizika uvnitř sféry vlastní odpovědnosti, příslušně plánovat opatření pro jejich správné řízení,
- používat vhodnou a koherentní politiku plánování a následných činností,
- být si vědom rizik v organizaci a vědět co činit v případě jejich realizace,
- účastnit se nouzového plánování a odezvy.

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

Nástrojem pro zajištění bezpečného technického díla je účinná kultura bezpečnosti, je program na zvyšování bezpečnosti organizace [1,14]. Postup pro vytváření programu na zvyšování bezpečnosti organizace se skládá z dále uvedených kroků:

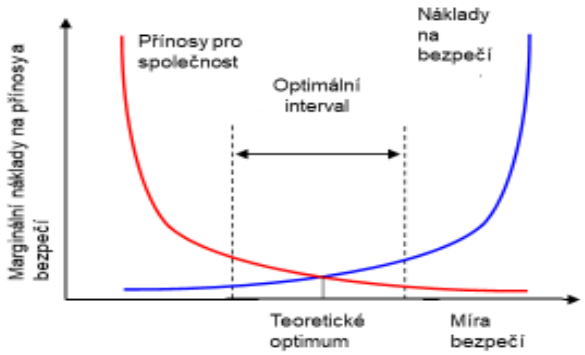
1. Definovat úkoly (dílčí cíle) a strategické cíle organizace s ohledem na bezpečnost.
2. Pro každý úsek organizace vybrat vhodné cílové a průběžné indikátory pro posuzování úrovně bezpečnosti.
3. Vytvořit slovník pro potřeby řízení integrální bezpečnosti.
4. Sladit standardy, metody dobré praxe a místní postupy.
5. Upravit seznam cílových indikátorů dle podmínek v předmětné organizaci.
6. Upravit seznam průběžných indikátorů dle podmínek v předmětné organizaci.
7. Stanovit způsob vyhodnocení cílových indikátorů (tj. hodnotový systém) dle podmínek v předmětné organizaci.
8. Stanovit způsob vyhodnocení průběžných indikátorů (tj. hodnotový systém) dle podmínek v předmětné organizaci.

9. Stanovit způsob / stupnici pro měření souboru indikátorů (tj. systém hodnot) a mezní limity dle podmínek v předmětné organizaci.

V praxi to znamená, že se pro každý úsek ve vybrané působnosti určí cílové a průběžné indikátory, které mají formu limitů a kontrolních seznamů [1,14]. K nim jsou v praxi přiřazená kritéria na vyhodnocení a stupnice, pomocí nichž se určuje, kdy je cíle dosaženo a kdy ne.

Na základě skutečností uvedených výše jsou náklady na zajištění bezpečí a udržitelného rozvoje organizace souhrnné náklady vynaložené na vyjednávání s riziky. Tj. jsou to náklady na opatření a činnosti prevence, připravenosti, odezvy a obnovy, náklady na pojištění a rezervní náklady na nepředvídané situace vyvolané např. málo pravděpodobnou kumulací nežádoucích jevů. Z hlediska účinnosti jsou nejefektivnější náklady na prevenci [58]. Jsou však nákladné na znalosti, zdroje, síly a prostředky, jejich výsledek není okamžitě viditelný a je zřejmý až v budoucnosti po pohromě, a proto jejich aplikaci je správa organizace obvykle nakloněna jen v období po velké pohromě. Z důvodů zajištění ochrany a udržitelného rozvoje je proto nutné právně prosadit vynutitelnost zásadních preventivních opatření právními předpisy.

Při zajištění přijatelné úrovně bezpečí v organizaci, které v sobě inherentně obsahuje dostatečnou úroveň udržitelného rozvoje nelze zanedbat skutečnost, že zdroje každé organizace jsou omezené a že každá činnost i opatření vyžaduje zdroje, síly a prostředky. Proto možná úroveň bezpečí odpovídá stavu organizace, ve kterém mezní náklady na prevenci se rovnají mezním nákladům na odstranění škod (tj. nákladům na odezvu a obnovu). Lze konstatovat, že takto definovaná úroveň bezpečí je ekonomickým optimem pro organizaci [95], obrázek 19.



Obr. 19. Bezpečí chápané jako ekonomické optimum pro technické dílo; zpracováno dle [95].

Ekonomické optimum znamená, že náklady na vypořádání rizik, tj. na bezpečí nejsou vyšší než přínosy pro společnost (organizaci). Teoretické optimum pochopitelně není obecně platné, platí pro konkrétní organizaci, protože podmínky i zdroje, síly a prostředky organizace jsou proměnné. Oblast přiměřenosti pak určuje správa organizace, která buď přímo v oblasti své působnosti, nebo prostřednictvím právních předpisů vyžaduje od ostatních zúčastněných realizaci určitých činností a opatření vedoucích k zajištění bezpečí zahrnujícího udržitelný rozvoj. Pochopitelně správné řízení může provádět jen kvalifikovaná správa a jen na základě disponibilních zdrojů.

Dnes jsou již kvalifikované postupy na identifikaci možných škod, možných ztrát i možné újmy v konkrétní organizaci při jednotlivých pohromách (metodiky používané Swiss Re, Munich Re a další popsané v práci [58]) v závislosti na tom, jaké chráněné zájmy v organizaci jsou a jaké jsou zranitelnosti dané organizace. Jsou i postupy na

vyčíslení nákladů na činnosti spojené s vyjednávání s riziky, a proto je možné podle zdrojů, sil a prostředků konkrétní organizace předurčit úroveň bezpečí zahrnující udržitelný rozvoj, které je v okolí teoretického optima. Z toho je rovněž zřejmé, že bohaté organizace mají predispozici zajistit vyšší úroveň bezpečí včetně udržitelného rozvoje než organizace chudé, mezi které patří i organizace ekonomicky bohaté, které se však soustřeďují jen na ekonomický růst a přehlížejí ostatní potřeby dnes i v budoucnu.

Výše uvedené údaje ukazují reálný pohled na svět, tj. i když organizace bude mít nejlepší snahu zajistit nejlepším způsobem bezpečí zahrnující udržitelný rozvoj, tak musí správně vynakládat zdroje, síly a prostředky, protože možnosti každé organizace jsou omezené. *Vyjednávání s jakýmkoliv rizikem* je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, kvalifikovaných lidí apod. Proto se v praxi hledá hranice, na kterou je únosné snížit riziko tak, aby vynaložené náklady byly ještě rozumné. Optimálně je třeba při vyjednávání s riziky také zvolit místně specifické přístupy, protože disponibilita zdrojů, sil a prostředků je rozdílná a mění se v čase. *Míra snížení rizika (určitá optimalizace) je většinou předmětem vrcholového řízení a politického rozhodování správy organizace*, při kterém se využívají současné vědecké a technické poznatky a zohledňují se ekonomické, sociální a další podmínky.

Zásadní obrat v řízení organizace s ohledem na žádoucí cíle nelze dosáhnout jednotlivými dílčími opatřeními, ale pouze komplexním přístupem s ohledem na místní podmínky. Složitá dělba kompetencí vede v praxi k vážným potížím a ve svém celku nepokrývá žádoucím způsobem celou problematiku. Pro zajištění bezpečí a udržitelného rozvoje organizace je třeba použít koordinovaný a cílevědomý přístup, který umožní postupně a v souladu s jejich důležitostí a naléhavostí řešit soubor úkolů ve všech sférách a součástech a docílit tak žádoucí stav organizace. Řešení problémů spočívá v oblasti investiční, technické, technickoorganizační, správní a řídící, vědeckovýzkumné, výchovy a dalších. Efektivní řešení problémů nelze zajistit bez strategického a koncepčního řízení, pro které musí připravit podrobné, objektivní a systematické údaje výzkum. Operativní přístup při řešení problémů bez navázání na strategické plány obvykle není správným řešením ve střednědobém a dlouhodobém výhledu.

4.6.5. Nástroj pro řízení bezpečnosti technického díla v čase

Každé technické dílo se mění v čase a jeho změny závisí na změnách okolí [1-4,17]. Proto na základě současného poznání, shrnutého v pracích [1-4,11,17,43,44,54], systém řízení bezpečnosti (tzv. SMS – Safety Management System) technického díla je postaven na zásadách procesního řízení a zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v území. Zpravidla se týká řady otázek, kromě jiného i organizace, pracovníků, identifikace a hodnocení ohrožení a z nich plynoucích rizik, řízení chodu organizace, řízení změn v organizaci, nouzového a krizového plánování, monitorování bezpečnosti, auditů a přezkoumávání.

Model SMS je zobrazen na obrázku 20. Je založen na řízení šesti hlavních procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií. Předmětné procesy byly

popsány v předchozím odstavci, ve kterém byly uvedeny a charakterizovány i jejich podprocesy.

Obr. 20. Model řízení bezpečnosti komplexního kritického objektu 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 poli označují zpětné vazby, které se používají při řízení.

Koordinace procesů je zacílena na zajištění bezpečného objektu za podmínek normálních, abnormálních a kritických. Koordinace je v daných souvislostech chápaná jako řízený proces, jehož cílem je vytvořit a provozovat technické dílo v potřebné kvalitě; sleduje procesy v prostoru, čase, personálu, materiálu, financích i dokumentech.

Z obrázku 20 je zřejmá zásadní role konceptu bezpečnosti objektu, průběžného hodnocení integrálního rizika a závažných dílčích rizik. V případě, že se při hodnocení zjistí, že riziko je nepřijatelné, je třeba provést změny, jak naznačují zpětné vazby na obrázku 20. Protože změny vyžadují zdroje, síly a prostředky, tak na základě zajištění hospodárnosti se nejprve realizuje zpětná vazba 1, a teprve, když nepřinese žádoucí stav, tak se realizuje zpětná vazba 2; poté zpětná vazba 3, a když ani po ní není žádoucí výsledek, tak zpětná vazba 4. V případě výskytu extrémních jevů s katastrofickými dopady se přikračuje okamžitě k realizaci zpětné vazby 4.

Zlatá pravidla se běžně používají v procesním řízení [14,47]. V řadě případů jsou role jednotlivých zúčastněných specifikovány takto:

1. Vrcholový management a řídící týmy provozující technologie a infrastruktury musí znát:
   - znát ohrožení od pohrom a možná rizika v území i objektu,
   - zavést a cíleně prosazovat „kulturu bezpečnosti“, která je respektována a prosazována všemi zúčastněnými za všech okolností,
   - ustanovit systémy řízení bezpečnosti, sledovat a popř. korigovat jejich činnost,
   - používat principy inherentní bezpečnosti při navrhování, projektování, výstavbě a provozování objektů a jejich zařízení,
   - pečlivě řídit změny,
   - být připraven na všechny pohromy, které mohou nastat,

- pomáhat ostatním zúčastněným při vykonávání jejich rolí a odpovědností,
- provádět neustálé vylepšování bezpečnosti.

2. Zaměstnanci v technologiích a infrastrukturách musí:
   - pracovat ve shodě s kulturou bezpečnosti, bezpečnými postupy a výcvikem,
   - usilovat neustále o veškerou informovanost a poskytovat informace a pro řídící pracovníky zajišťovat zpětnou vazbu,
3. Veřejná správa musí:
   - usilovat o rozvoj, posilování a ustavičné zlepšování koncepce bezpečnosti, předpisů a směrnic,
   - vést a motivovat všechny další zúčastněné k tomu, aby plnili své úlohy a odpovědnosti,
   - znát rizika uvnitř sféry vlastní odpovědnosti, příslušně plánovat opatření pro jejich správné řízení,
   - motivovat podniky k tomu, aby vyjednávaly s riziky odpovědně,
   - pomáhat efektivní komunikaci a spolupráci všech zúčastněných,
   - podporovat spolupráci mezi správními úřady,
   - používat vhodnou a koherentní politiku územního plánování a následných činností,
   - zmírňovat rizika vhodnými opatřeními odezvy, která spadá do její působnosti.
4. Veřejnost (ostatní zúčastnění) musí:
   - být si vědom rizik v obci a vědět co činit v případě jejich realizace,
   - spolupracovat při rozhodování o umístění, výstavbě a provozu technologií a infrastruktur,
   - účastnit se nouzového plánování a odezvy.

Kultura bezpečnosti znamená, že člověk ve všech svých rolích (řídící pracovník, zaměstnanec, občan či oběť pohromy) dodržuje zásady bezpečnosti, tj. chová se tak, aby sám nevyvolal realizaci možných rizik, a když se stane účastníkem realizace rizik, aby přispěl k účinné odezvě, stabilizaci chráněných aktiv a jejich obnově a k nastartování jejich dalšího rozvoje. Podle některých autorů jde o soubor postojů, domněnek, norem a hodnot, které existují v dané entitě, který je odrazem toho, jak je podnik řízený, tj. jsou to všeobecné principy rozdělení pravomoci a odpovědnosti, zásady řízení a jistý poměr mezi důrazem na pracovní výsledky, autoritou, péčí o lidi, dodržování zásad bezpečnosti a zajištění funkčnosti dané entity. Účinná kultura bezpečnosti je základním prvkem pro řízení bezpečnosti. Odráží koncepci bezpečnosti a vychází z hodnot, stanovisek a jednání vrcholových řídících pracovníků a z jejich komunikace se všemi zúčastněnými. Je zřetelným závazkem aktivně se podílet na řešení otázek bezpečnosti a prosazuje, aby všichni zúčastnění konali bezpečně a aby dodržovali příslušné právní předpisy, standardy a normy. Pravidla kultury bezpečnosti musí být zapracována do všech činností v území nebo jiné entitě. Jejich základem není koncentrace na potrestání viníků / původců chyb, ale poučení z chyb a zavedení takových nápravných opatření, aby se chyby nemohly opakovat nebo aby se alespoň výrazně snížila četnost jejich výskytu.

V souvislosti s kulturou bezpečnosti se často v současné odborné literatuře spojené s technologiemi používají pojmy prevence ztrát a procesní bezpečnost. Jejich definice uvedeme také proto, že jsou to nástroje, které slouží ve spojitostech s technologiemi k ochraně osob I majetku.

Prevence ztrát (Loss Prevention) je systematický přístup k prevenci (předcházení) havárií nebo k minimalizaci jejich dopadů. Zahrnuje prostředky pro eliminaci zdrojů

rizik nebo omezení pravděpodobnosti jejich realizace a pro zmírnění dopadů spojených s touto realizací (preventivní a následná opatření). Dále zahrnuje identifikaci vhodných kontrolních opatření, identifikaci a aplikaci vhodných nápravných opatření, kterými se zajišťuje bezpečná entita mající příslušnou úroveň bezpečí a udržitelného rozvoje a nepředstavující nepřijatelné nebezpečí pro své okolí [2,54].

Procesní bezpečnost nebo lépe bezpečnost procesů, což je v souladu s anglickým pojmem "Process Safety", je odvětví bezpečnosti zaměřené na bezpečnost v průmyslu, ve kterém je řada výrobních a přídavných procesů, které jsou nutné k vytvoření konečného produktu daného průmyslu. Jde přitom o zabránění vzniku havárií, které mají zvláštní a charakteristické rysy pro daný specifický průmysl. Zabývá se např. prevencí bezprostředních úniků chemických látek nebo energií ve škodlivém množství, a v případě, že se tyto úniky vyskytnou, tak omezením jejich velikosti, dopadů a následků. Nezahrnuje otázky klasické bezpečnosti a ochrany zdraví při práci, tj. zabývá se čistě technickými problémy, čímž se liší od systémové bezpečnosti definované dříve.

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie. Proto nyní připouštíme, že složité kritické objekty jsou z různých důvodů čas od času v nestabilním stavu a vznikají organizační havárie, kaskády selhání bez zjevné příčiny, tj. připouštíme nejistoty náhodné i epistemické (znalostní) v jejich chování. Z důvodu zajištění bezpečnosti kritických objektů a ochrany lidí hledáme řešení odezvy pro možné případy, které nelze odhalit pravděpodobnostními přístupy a budujeme pro ně náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik záchranářů.

Dosažení požadované úrovně bezpečnosti znamená dobře řídit a správně rozhodovat. Dobré / správné řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici. Data musí být správná, tj. zná se jejich velikost a přesnost; a musí mít vypovídací schopnost pro řešený problém, tj. musí být validovaná. Datové soubory musí být reprezentativní, tj.: úplné; obsahovat správná data; mít dostatečný počet dat; data musí být rozprostřena homogenně v celém sledovaném intervalu a musí být validovaná. Při aplikaci modelů musí být správně zváženy nejistoty a neurčitosti v datech. Je si nutno uvědomit, že v reálném světě při zajišťování bezpečnosti složitých technologických objektů a infrastruktur řešíme netriviální problémy, tj.: je více chráněných aktiv, jejichž cíle jsou konfliktní; aktiva se mění v čase a prostoru; a prostředí, ve kterém jsou aktiva, tj. lidský systém se dynamický vyvíjí.

Závěrem je tudíž možno konstatovat, že pro zajištění bezpečného technologického systému je nutné: uvědomit si aspekty technologického systému, které jsou důležité pro jeho bezpečnost; pochopit příčiny poruch bezpečnosti technologického systému a kontext jejich působení; soustředit pozornost na podobnosti i rozdíly pohrom (tj. jevů, které narušují bezpečnost technologického systému) samotných; pochopit roli území ve spojitosti s bezpečností technologických systémů, tj. především vlastnosti území, které eskalují nebo potlačují dopady pohrom vždy nebo jen za určitých okolností; používat uvědoměle metodiky hodnocení pohrom, jejich dopadů i identifikace nápravných opatření; stanovit cíle, harmonogramy, monitoringy, organizační struktury, normy, standardy a právní předpisy pro uvědomělé řízení bezpečnosti systému; odstranit multiplicity při přípravě opatření na zvládnutí dopadů pohrom; a při územním plánování, projektování, výstavbě, provozování, odezvě na pohromu v území a

při obnově území neaplikovat opatření, která zvyšují rizika spojená s dalšími možnými pohromami v daném území.

V zásadě lze odlišit dva režimy činnosti systémů souvisejících s bezpečností. Prvním je režim, kdy systém vyčkává a teprve v případě, že vznikne potřeba zásahu, realizuje bezpečnostní funkci. Druhým je režim, kdy systém trvale nebo často realizuje bezpečnostní funkci. Typickým reprezentantem systémů pracujících na vyžádání jsou ochranné a zabezpečovací systémy. Reprezentantem systémů pracujících v režimu s vysokým nebo nepřetržitým vyžádáním jsou například systémy regulace fyzikálního parametru technologického procesu, anebo obyčejné železniční závory.

Integrita bezpečnosti je definována jako „pravděpodobnost systému souvisejícího s bezpečností uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu“. Většinou se sleduje ve spojení s lidskými chybami v různých etapách životního cyklu systému. Patří sem např. chyby specifikace, chyby návrhu, chyby instalace, chyby údržby, chyby modifikace. Posouzení integrity bezpečnosti souvisí s posouzením, jak systém bezpečně selže. Tj. posuzuje pravděpodobnost výskytu bezpečného selhání a nebezpečného selhání. Spolehlivost ve smyslu reliability není samotná schopná zajistit SIL. Specifické nástroje řízení používající techniky zacílené na kontinuální hodnocení rizik zajišťují, že systém se vyhne chybám a omylům. Integrita (celistvost) bezpečnosti je tudíž základní mírou bezpečnosti technického díla.

Znalosti získané studiem havárií [3,4] ukazují, že velkou pozornost musíme věnovat chování lidí i lidským opatřením a činnostem a způsobu jejich řízení a provádění, abychom předcházeli organizačním haváriím. Bezpečnostní kultura tak souvisí s organizační kulturou, která je souborem dohodnutých pravidel uplatňovaných v řízení organizačních jednotek a podílí se na vytváření norem institucionálního chování. Znamená správné aplikování znalostí, přemýšlení a správné reakce na reálné situace. Nejde totiž jenom o dodržování norem a předpisů zacílených na spolehlivost našich opatření a činností, protože tím můžeme přehlédnout jevy, které normy a předpisy nevidí. Jde o chování založené na řízení znalostí [14].

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie. Analýzy havárií: rozlomení plošiny Alpha v r. 1988 v Severním moři; havárie skladu leteckého petroleje v Buncefieldu 11. 12. 2005; neobjasněné námořní, vlakové a letecké havárie v posledních letech; havárie v jaderné elektrárně Fukushima 11. 3. 2011 (pozn. – byla podceněna velikost tsunami, nebyly respektovány vypočtené scénáře havárií), ukázaly, že řada odborníků bývá postižena provozní slepotou a po splnění požadavků norem a standardů nevidí zbylá rizika nebo rizika spojená s různými vazbami a spřaženími s okolím.

Proto v kapitole 5 ukážeme specifické nástroje rizikového inženýrství pro zajištění bezpečnosti kritických objektů a ochrany lidí, které používají specifické postupy založené na principu integrální bezpečnosti s tím, že při změně podmínek, a to zvláště náhlé, se aplikují specifické nástroje, které jsou předem připravené k okamžité aplikaci. Jde především o připravený způsob provedení odezvy pro možné případy, které nelze odhalit pravděpodobnostními přístupy, a hlavně pro tuto odezvu mít vybudované náhradní zdroje vody či jiného chladiva a energie, specifické systémy odezvy a specifický výcvik inženýrů a záchranářů.

Dosažení požadované úrovně bezpečnosti znamená dobře řídit a správně rozhodovat. Dobré / správné řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici a uděláme vše pro to, abychom zabránili provozní slepotě. Data musí být: správná, tj. zná se jejich velikost a přesnost; a musí mít vypovídací schopnost pro řešený problém, tj. musí být validovaná. Datové soubory musí být reprezentativní, tj.: úplné; obsahovat správná data; mít dostatečný počet dat; data musí být rozprostřena homogenně v celém sledovaném intervalu a musí být validovaná. Při aplikaci modelů musí být správně zváženy nejistoty a neurčitosti v datech [31,35].

Je si nutno uvědomit, že v reálném světě při zajišťování bezpečnosti složitých sociotechnologických objektů řešíme netriviální problémy, tj.: je více chráněných aktiv, jejichž cíle jsou v řadě případů konfliktní; aktiva se mění v čase a prostoru; a prostředí, ve kterém jsou aktiva, tj. lidský systém se dynamický vyvíjí.

4.6.6. Nástroj pro posouzení bezpečnosti technického díla

Jak již bylo výše řečeno, bezpečnost a riziko nejsou komplementární veličiny, i když spolu určitým způsobem souvisí. Práce s riziky je velmi náročná na znalosti, data i kvalifikovanost personálu, který ji provádí. Protože v praxi jde o bezpečnost, a ta závisí na úrovni práce s riziky, je třeba měřit tento vztah.

Údaje a zkušeností z práce s riziky, které jsou shromážděné v pracích [2-4] a v pracích v nich citovaných, jasně ukazují, že čím lépe rizika entity vypořádáme (tj. čím lepší postup pro jejich zvládnutí použijeme), tím dosáhneme vyšší úroveň bezpečnosti entity. Proto jsme při konstrukci nástroje pro posuzování míry bezpečnosti technického díla použili všeobecně použitelné metody inženýrství rizika [69], tj. kontrolní seznam, a teorie maximálního užitku [65]. To znamená, že hodnocení kontrolního seznamu je navrženo způsobem, že nejvyšší hodnocení u každého hodnoceného aspektu, připadá nejlepšímu způsobu zvládnutí daného aspektu (tj. validita techniky je nejvyšší) na základě současných znalostí a zkušeností. Stupnice pro posuzování celkového výsledku kontrolního seznamu je zvolena v souladu s doporučeními v práci [4].

Vytvořený specifický kontrolní seznam je v tabulce 20. Kontrolní seznam obsahuje 72 otázek a stupnice pro jeho celkové vyhodnocení (tj. míry bezpečnosti) podle zásad uvedených v [4], je v tabulce 21 Nástroj byl úspěšně odzkoušen v praxi a byl prezentován na mezinárodních setkáních odborníků z oblasti bezpečnosti technických děl [96].

Tabulka 20. Kontrolní seznam pro posuzování bezpečnosti technického díla na základě posouzení práce s riziky.

Otázka	**Odpověď**		**Poznámka**
	ANO	**NE**	
Jsou v dokumentaci technického díla odlišovány pojmy nebezpečí, ohrožení a riziko?			
Je dokumentace technického díla založena na kontextu, který zvažuje jen aktiva technického díla?			
Je dokumentace technického díla založena na kontextu, který			

zvažuje aktiva technického díla a vybraná veřejná aktiva (zaměstnanci, kontraktoři, návštěvních, lidé v okolí, pracovní a životní prostředí)?			
Je dokumentace technického díla založena na kontextu, který zvažuje aktiva technického díla a všechna veřejná aktiva?			
Jsou zvažovány zdroje rizik, které stanovuje zkušenost experta?			
Jsou zvažovány zdroje rizik, které stanovuje legislativa a zkušenost experta?			
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle?			
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle a lidský faktor spojený se špatně provedenými pracovními úkony?			
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle a lidský faktor v nejširším pojetí?			
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle, zdroje určené BOZP a zdroje spojené s ochranou pracovního prostředí?			
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle, zdroje určené BOZP a zdroje spojené s ochranou pracovního prostředí i s ochranou životního prostředí vně technického díla?			
Jsou zvažovány zdroje rizik, které představují zdroje v technickém díle, zdroje určené BOZP a zdroje spojené s ochranou pracovního prostředí i s ochranou životního prostředí vně technického díla v systémovém pojetí (tj., že všechny zdroje rizik jsou vzájemně propojené)?			
Jsou zvažovány zdroje rizik dle přístupu All-Hazard-Approach (tj. systémové pojetí i vnější zdroje)?			
Je zvažováno jen dílčí riziko?			
Jsou zvažována dílčí rizika i integrované riziko?			
Jsou zvažována dílčí rizika, integrovaná rizika i integrální riziko?			
Jsou rizika v technickém díle systematicky sledována?			
Jsou rizika technického díla systematicky sledována až po výstavbě technického díla?			
Jsou rizika technického díla systematicky sledována po celou dobu životnosti technického dílu už od jeho projektu?			
Jsou rizika technického díla systematicky sledována po celou dobu životnosti technického dílu už od jeho projektu a v jeho projektu a provozu je uplatněn přístup Defence-In-Depth?			
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky?			
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik?			
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přija-			

telnosti rizik, která respektují veřejný zájem (tj. mají sociální rozměr)?			
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik a cíle řízení rizik?			
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik a cíle řízení rizik s ohledem na veřejný zájem?			
Je při práci s riziky technického díla systematicky použit procesní model práce s riziky, který má jasně určen kritéria přijatelnosti rizik, cíle řízení rizik s ohledem na veřejný zájem a nápravná opatření v monitoringu pro případ, že riziko se stane nepřijatelné?			
Je při práci s riziky technického díla systematicky určen a sledován soubor prioritních rizik?			
Zajišťuje technika řízení rizik technického díla v každé fázi práce s riziky přezkoumání přínosů a nákladů spojených s opatřeními na vypořádání rizik, aby se zajistilo hospodárné nakládání se silami, zdroji a prostředky technického díla?			
Zajišťuje technika řízení rizik technického díla v každé fázi práce s riziky přezkoumání přínosů a nákladů spojených s opatřeními na vypořádání rizik, aby se zajistilo hospodárné nakládání se silami, zdroji a prostředky technického díla a veřejné správy?			
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to jen některých?			
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech prioritních?			
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu?			
Jsou v technickém díle prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu a nepřijatelné dopady na okolní životní prostředí?			
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení největších dopadů rizik, a to jen některých?			
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení rizik, a to všech prioritních?			
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení dopadů rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu?			
Jsou v technickém díle prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení dopadů rizik, a to všech, které by mohly způsobit závažné ztráty technickému dílu a mít nepřijatelné důsledky pro okolní životní prostředí?			

Je technické dílo pojištěno pro případ realizace rizik?			
Má technické dílo rezervy finanční, materiální, technické, personální a organizační pro odezvu v případě realizace závažného rizika?			
Má technické dílo rezervy finanční, materiální, technické, personální a organizační pro obnovu v případě realizace závažného rizika?			
Má technické dílo rezervy finanční, materiální, technické, personální a organizační pro odezvu a obnovu v případě realizace extrémního neočekávaného rizika?			
Jsou při práci s riziky v technickém díle zohledněny jen výsledky předběžných analýz rizik?			
Jsou při práci s riziky v technickém díle upřednostněny výsledky standardních, rychlých a méně přesných analýz rizik před výsledky předběžných analýz rizik?			
Jsou při práci s riziky v technickém díle upřednostněny výsledky detailních analýz rizik v souhrnném kontextu před výsledky standardních, rychlých a méně přesných analýz rizik a před výsledky předběžných analýz rizik?			
Jsou při práci s riziky v technickém díle upřednostněny výsledky individuálních a specifických analýz rizik před výsledky detailních analýz rizik v souhrnném kontextu, standardních, rychlých a méně přesných analýz rizik a předběžných analýz rizik?			
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení?			
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení technické a ekonomické?			
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení technické a ekonomické, externí a interní?			
Jsou při práci s riziky v technickém díle stanoveny kritéria pro hodnocení technické a ekonomické, externí a interní a sociálně – politické?			
Jsou při práci s riziky v technickém díle stanoveny požadavky pro zajištění bezpečnosti?			
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti?			
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti a dílčí cíle?			
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle a metody a postupy?			
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle, metody a postupy a také limity a podmínky?			
Jsou při práci s riziky v technickém díle stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle, metody, postupy, limity a podmínky, a kompetence osob či institucí?			
Má správce technického díla systém řízení bezpečnosti, který je postaven na zásadách procesního řízení a systematické			

práci s riziky?			
Má správce technického díla systém řízení bezpečnosti, který obsahuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v technickém díle a v okolním území?			
Má správce technického díla systém řízení bezpečnosti (SMS), který má proces řízení, který obsahuje šest procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií?			
Má SMS správce technického díla proces koncepce a řízení, který obsahuje podprocesy pro: celkovou koncepci; dosahování dílčích cílů bezpečnosti; vedení / správu bezpečnosti; systém řízení bezpečnosti; personál a zahrnuje úseky pro: řízení lidských zdrojů, výcvik a vzdělání, vnitřní komunikaci / informovanost a pracovní prostředí; revize a hodnocení plnění cílů v bezpečnosti?			
Má SMS správce technického díla proces administrativní postupy, který obsahuje podprocesy pro: identifikaci ohrožení od možných pohrom a hodnocení rizika; dokumentaci postupů (včetně systémů pracovních povolení); řízení změn; bezpečnosti ve spojení s kontraktory; a dozor nad bezpečností výrobků?			
Má SMS správce technického díla proces technické záležitosti, který obsahuje podprocesy pro: výzkum a vývoj; projektování a montáže; inherentně bezpečnější procesy; technické standardy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů?			
Má SMS správce technického díla proces vnější spolupráce, který obsahuje podprocesy pro: spolupráci se správními úřady; spolupráci s veřejností a dalšími zúčastněnými (včetně akademických pracovišť); a spolupráci s dalšími podniky?			
Má SMS správce technického díla proces nouzová připravenost, který obsahuje podprocesy pro: plánování vnitřní (on-site) připravenosti; usnadnění plánování vnější (off-site) připravenosti (za kterou odpovídá veřejná správa); a koordinaci činností resortních organizací při zajišťování nouzové připravenosti a při odezvě?			
Má SMS správce technického díla proces dokumentace a šetření havárií, který obsahuje podprocesy pro: zpracování zpráv o pohromách, haváriích, skoro nehodách a dalších poučných zkušenostech; vyšetřování škod, ztrát a újmy a jejich příčin; a odezvu a následné činnosti po pohromách (včetně aplikace poučení a sdílení informací)?			
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém jsou stanoveny role zúčastněných, pravidla pro zvyšování kultury bezpečnosti (tzv. zlatá pravidla) a příslušné odpovědnosti?			
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém jsou: bezpečnostní plány (strategická, taktická, operativní a technická úroveň); vnitřní a vnější nou-			

zové plány, plány kontinuity a krizové plány?			
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi?			
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje jen technická rizika?			
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická a organizační rizika?			
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická, organizační a vnější rizika?			
Je v SMS správce technického díla program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická, organizační, vnější a kybernetická rizika?			
Je v SMS zajištěn kvalitní monitoring integrálního rizika a závažných dílčích rizik a nápravná opatření pro případ nepřijatelných rizik?			
CELKEM			

Tabulka 21. Hodnotová stupnice pro míru bezpečnosti.

Míra bezpečnosti	**Hodnoty v %**	**Počet odpovědí „ANO“ v tabulce 19**
Extrémně vysoká – 5	Více než 95 %	Více než 68
Velmi vysoká – 4	70 - 95 %	51 - 68
Vysoká – 3	45 - 70 %	33 - 50
Střední – 2	25 – 45 %	19 - 32
Nízká – 1	5 – 25 %	4 - 18
Zanedbatelná – 0	Méně než 5 %	Méně než 4

Předmětný kontrolní seznam byl otestován v praxi [96]. Vedlejším produktem testů bylo zjištění, že velkým problémem při práci s riziky technických děl je, že experti z různých oblastí spojených s technickými díly spolu nespolupracují; důkazem jsou záznamy o řešení konfliktů, které nemusely vzniknout, kdyby experti spolu komunikovali.

4.6.7. Shrnutí poznatků spojených s prací s riziky ve prospěch bezpečnosti technických děl

Základní nástroje pro zajištění bezpečného území, bezpečného technického díla i jejich dobré koexistence s okolím zajišťují specifické nástroje, kterými jsou bezpečnostní plán (strategický plán zacílený na rozvoj) a jeho dílčí plány jako je územní plán; nouzové plány, tj. plány odezvy na konkrétní pohromy; a krizové plány, tj. plány odezvy na extrémní pohromy [1-3,11,12], jejichž nedílnou součástí u technologických objektů jsou plány kontinuity, jejichž cílem je zajistit schopnost obnovit dostatečně rychle činnost technického díla, aby nedošlo ke ztrátě obslužnosti území, produktů, konkurenceschopnosti území, zaměstnanosti, které logicky vedou ke snížení rozvojového potenciálu daného území [1,3,4].

Pro posuzování rizik byl vyvinut bezpočet pomocných pracovních pomůcek, metodických návodů, uživatelských příruček a softwarů, které zajišťují odpovědi na otázky:

1. Jaké ohrožení představuje pohroma?
2. Jaké dopady na aktiva mohou nastat?
3. Jaký je scénář ohrožení?, tj. jak jsou rozloženy dopady?
4. Jaká je pravděpodobnost výskytu takto veliké pohromy?
5. Jak je riziko veliké, tj. pokud některý nepřijatelný dopad nastane, jaké budou škody a újmy na chráněných zájmech?

Postupy pro určení rizika vychází ze vztahu ***R = H x Z***, tj. závisí na určení ohrožení ***H*** (Hazard) a zranitelnosti ***Z*** (vulnerability); u teroristických útoků tam ještě přibývá úmysl útočníka ***I*** (*tj. R = H x Z x I*). Při určování ohrožení používáme jednoduché odhady, výpočty založené na scénářích pohrom a také velmi náročné postupy založené na teorii extrémních hodnot a na různých modelech entity: lineární (liniové); stromové; síťové; a vícekriteriální, pro něž vytváříme systémy pro podporu rozhodování [2,9]. Důležité je jakou hodnotu ohrožení určujeme, používá se: střední, očekávaná na nějaké úrovni četnosti výskytu; a maximální možná. Je zřejmé, že při zvážení každé hodnoty zajistíme jinou úroveň ochrany.

Pro stanovení rizika lze použít postupy s různou náročností, tj. postupy: jednoduché pro identifikaci rizika; obtížné pro stanovení hodnoty rizika, ve kterém jde o přesný údaj – pro strategické rozhodování; a středně náročné pro stanovení hodnoty rizika pro potřeby kontroly rizika konkrétního procesu, při kterém lze použít míru (a to i verbální) – pro taktické a operativní rozhodování.

Riziko je třeba identifikovat, analyzovat, ocenit a pochopit v souvislostech, aby s ním bylo možno vyjednávat. Hodnocení dopadů pohrom v konkrétním území je základní součástí jakéhokoliv pokusu o kvantifikaci a hodnocení rizika. Hodnocení rizika je strukturovaná procedura, která se pokouší odpovědět na dále uvedené otázky: jaké ztráty, škody a újmy budou na chráněných aktivech?; jak často se to stane?; jak zareagují bezpečnostní systémy v území?; a jaké ztráty, škody a újmy budou na chráněných aktivech, když selžou bezpečnostní systémy v území? Aby hodnoty rizika měly jasnou vypovídací hodnotu, tak je důležité mít nejenom nástroj, ale také jasně definovanou hodnotovou stupnici jak pro klasifikaci dílčích položek, tak pro souhrn položek. *Poznámka:* nejčastější chyba v českých poměrech – nedefinuje se stupnice, tj. veškeré údaje o riziku jsou subjektivní.

Řízení rizik je proces určení opatření a činností vedoucích k ochraně před riziky; člověk ho prováděl od samého počátku uvědomělého konání. Dnes podle položek, které sleduje a podle stanoveného cíle, používá nástroje, jejichž efektivita záleží na kvalitě dat a metody zpracovatele, a také na čase, ve kterém je nutné provést rozhodnutí; nezanedbatelné jsou náklady na samotné zpracování podkladů pro rozhodnutí.

Inženýrství (inženýring)***rizika*** je realizace opatření a činností k vypořádání rizik způsobem stanoveným řízením rizik, dle disponibilních možností a dle podmínek v místě řešení.

Úkolem řízení rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet.

Zvládnutí rizika znamená buď snížení rizika, anebo provádění opatření a činností, aby se riziko udrželo na podmíněně přijatelné úrovni, kterou v případě realizace lze zvládnout připravenou odezvou.

Konkrétní technická opatření závisí na typu technického díla, jeho stavbě a vybavení. Vzhledem k velké rozmanitosti technických děl je opatření velmi mnoho; je třeba respektovat požadavky uvedené v příslušných zákonech, normách a standardech. Např. specifickou pozornost je třeba věnovat tlakovým nádobám, regulačním ventilům, potrubím, kontejnmentům či jiným ochranným obálkám.

Snižování rizika je prakticky vždy spojeno se zvyšováním nákladů. Řízení rizika je tedy vedeno snahou najít hranici, na kterou je únosné riziko ještě snížit, aby vynaložené náklady byly společensky přijatelné. Proto je třeba se dohodnout na tom, jaké požadavky bude výstup z hodnocení rizika splňovat. Při hodnocení rizik je nutné se snažit tyto požadavky dodržovat a případné nedodržení odůvodnit. Jedná se především o splnění požadavků:

- provedení hodnocení v požadované šíři a kvalitě v souladu s přijatou metodikou hodnocení,
- úplnost hodnocení,
- zahrnutí nejnovějších poznatků vědy,
- odhad nejistot v případě použití extrapolací,
- jednotné vyjádření charakteristik rizika
- průhlednost provedení procesu hodnocení rizik.

Dosažení cíle znamená dobře řídit a správně rozhodovat, přičemž dobré řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici [2,9]**.** *Poznámka:* nejčastější chyba v českých poměrech – neprověřuje se kvalita datových souborů a vzájemný vztah mezi přesností dat a citlivostí metody.

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

S vnímáním rizika souvisí přijatelnost rizika, která musí mít sociální rozměr. Je třeba zvažovat:

1. Pro koho má být riziko přijatelné?; pro původce rizika, pro politiky nebo pro veřejnou správu?

2. Kdo stanoví přijatelnost?; politici rozhodují o tom, co je zákonné, a tudíž by neměli rozhodovat o tom, co je přijatelné,
3. Zda při stanovení přijatelnosti rizik byla diskutována aktuálně tolerovatelná rizika, netolerovatelné prahové hodnoty a postoje veřejnosti k rizikům.

Rizika byla, jsou a budou a neustále se budou objevovat nová. Řízení rizika, které způsobují pohromy, vyžaduje rozměr a měření rizika, které berou v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Řada současných technik na určování rizika nereprezentuje holistický přístup a většina z nich nezvažuje vazby a toky mezi prvky systému za zranitelné položky, které zvyšují škody, ztráty a újmy. Je si třeba uvědomit, že riziko je rozdělené na lokální, regionální i státní úrovni.

Je zřejmé, že nejsme-li schopni riziko identifikovat a analyzovat, nejsme schopni se proti němu účinně bránit.

Chyba, které se dopustíme při analýze rizika, se přenáší do nouzových a krizových plánů, do plánů kontinuity a snižuje jejich hodnotu ve vztahu k plánovaným opatřením směřujícím především k ochraně lidských životů a zdraví, ale i v oblasti akceschopnosti záchranných složek podílejících se na realizaci záchranných operací.

Na závěr je třeba připomenout, že ignorování či podceňování řízení rizik je důvodem většiny problémů lidské společnosti.

Dle prací [97,98] kritéria přijatelnosti rizik jsou obvykle obsažena v národních zákonech. Kritéria přijatelnosti rizika označovaná jako ALARP jsou kritéria pro měření každého rizika; a nezávisí na ohrožení. Etický základ spočívá v aplikaci metody CBA na výsledky hodnocení rizika.

Hodnocení rizika je důležitou činností, když stanovujeme požadavky na bezpečnost důležitého technického díla. Kromě hodnoty rizika se v praxi posuzuje ještě úroveň integrity bezpečnosti SIL (Safety Integrity Level), definovaná normou ČSN EN 61508-X, 61511-X [100]. Uvedená veličina charakterizuje úroveň schopnosti systému identifikovat závažnou odchylku od požadovaného stavu systému. V praxi se rozlišují 4 úrovně, tabulka 22. ***PFD*** označuje střední pravděpodobnost výskytu nebezpečné poruchy, která zabrání plnění bezpečnostní funkce na vyžádání a ***PFH*** označuje střední pravděpodobnost výskytu chyby bezpečnostní funkce za hodinu.

Vzhledem ke skutečnosti, že dosud u technických děl se v praxi odlišuje provozní (funkční) bezpečnost a integrální bezpečnost, definovaná jako vrcholová vlastnost systému, je třeba si uvědomit, že výše uvedená veličina SIL se vztahuje k provozní bezpečnosti, tj. ne k celkové (integrální) bezpečnosti systému. Provozní bezpečnost systému je zajištěná řízením rizik zacíleným na spolehlivost systému [4]. Proto veličina SIL definovaná výše uvedeným způsobem je spojená se spolehlivostí systému, tj. ne s integrální bezpečností, která je zvažována v tabulce 3.

Tabulka 22. Úrovně SIL [100].

SIL	(PFD_{AVG})	(PFH)
SIL 1	$\geq 10^{-5}$ až $<10^{-4}$	$\geq 10^{-9}$ až $<10^{-8}$
SIL 2	$\geq 10^{-4}$ až $<10^{-3}$	$\geq 10^{-8}$ až $<10^{-7}$
SIL 3	$\geq 10^{-3}$ až $<10^{-2}$	$\geq 10^{-7}$ až $<10^{-6}$
SIL 4	$\geq 10^{-2}$ až $<10^{-1}$	$\geq 10^{-6}$ až $<10^{-5}$

Úroveň SIL ovlivňuje jak konstrukci systému (např. zálohování funkcí pomáhajících zajistit bezpečnost), tak procesy během konstrukce technického díla. Na základě výsledků v praxi [101] zajištění

- SIL 1 – SIL 2 znamená zvýšení nákladů o 20-50%
- SIL 2 – SIL 3 znamená zvýšení nákladů o 50-150%

Opatření používaná v řízení bezpečnosti (a to provozní i integrální) jsou pasivní a aktivní; pasivní jsou technické povahy a aktivní závisí na činnostech člověka.

Pro podporu systému řízení bezpečnosti je třeba dle údajů jak v pracích [1-4,17], tak v pracích v nich citovaných, zpracovat řadu podpůrných nástrojů jako jsou: bezpečnostní plány, vnitřní a vnější nouzové plány, plány kontinuity a krizové plány. V praxi se velmi osvědčily plány řízení prioritních rizik [4]. Předmětné plány mají tabelární formu, která obsahuje: oblast rizika; popis rizika; ocenění rizika; a opatření pro zvládnutí rizika. Oblast rizika se zpravidla dělí na podoblasti: organizační; technickou; personální; vnějších faktorů; a kybernetickou. Popis rizika obsahuje zásadní dopady a jejich důsledky na sledovaná aktiva. Oblast ocenění rizika obsahuje výsledek hodnocení pravděpodobnosti výskytu a výsledek ocenění dopadů na aktiva dle stanovených stupnic (právě zde je v praxi nejvíce chyb – stupnice jsou jen verbální a není vyznačen vztah ke škodám na aktivech [4]). Oblast opatření na zmírnění rizika obsahuje taxativně: opatření, které se udělá při realizaci rizika; stanovení jak a podle čeho se opatření udělá; a kdo opatření udělá (tj. odpovědnost za provedení). Příklad je dále v odstavci 5.4.2.

5. POSTUPY PRÁCE S RIZIKY ZACÍLENÉ NA KOEXISTENCI TECHNICKÉHO DÍLA A JEHO OKOLÍ

Jak již bylo několikrát uvedeno, technické dílo je přínosem pro území, ale zároveň je zdrojem rizik pro území, a proto je důležitá koexistence technického díla s okolním územím.

5.1. Kontexty pro řízení a vypořádání rizik

Při práci s riziky technického díla s cílem zajistit bezpečí a rozvoj lidí je třeba dle současného poznání shrnutého v prací [2,3] zvažovat řadu aspektů:

1. Vnímání reality. Pro řešení současných problémů je nutné systémové pojetí technického díla a jeho okolí [3]. V současné praxi se při řešení konkrétních problémů používají modely reality předpokládající: uzavřený systém; otevřený systém; soubor několika otevřených systémů; systém systémů [3].
2. Pojetí zdrojů rizik. Dle poznatků, o které se opírá publikace, rozlišujeme případy, ve kterých zdroji rizik, tj. pohromami jsou: jen vnitřní jevy v systému; jen vnitřní jevy v systému a lidský faktor; vnitřní a vnější jevy a lidský faktor; vnitřní a vnější jevy, lidský faktor a tzv. interdependences, tj. indukovaná škodlivá propojení a škodlivé toky v systému a v propojení systému s okolím; a vnitřní a vnější jevy, lidský faktor a tzv. interdependences, tj. indukovaná škodlivá propojení a škodlivé toky v systému systémů a v jeho propojení s okolím.
3. Systematická práce s riziky zacílená na jejich redukci je doložena od 30. let minulého století. Na základě kritického vyhodnocení současných poznatků, jehož výsledky jsou shrnuty v pracích [3,4,17], rozlišujeme pět konceptů, ze kterých vycházíme při vyjednávání s riziky, a to: klasické řízení a inženýrství rizika; klasické řízení a inženýrství rizika zahrnující lidský faktor; řízení a inženýrství zaměřené na bezpečí (zabezpečovací řízení a inženýrství); řízení a inženýrství zaměřené na bezpečnost, tj. takové ovládání a vypořádání rizika, které zajistí jak zabezpečený systém, tak jeho bezpečné okolí; a řízení a inženýrství zaměřené na bezpečnost systému systémů (SoS); obrázek 21. Charakteristiky konceptů a praktické aplikace jsou popsány v citovaných pracích a konkrétní výsledky jsou uloženy v archivu [62].

   Z výsledků výzkumu shrnutého v práci [17], založeného na aplikaci teorie maximálního užitku, který se zabýval hodnocením míry kritičnosti konceptů současného řízení a vypořádání rizik objektů, vyplývá, že žádný z dnes používaných konceptů pro řízení a vypořádání rizik nemá zanedbatelnou míru kritičnosti; tj. míra kritičnosti při aplikaci:
   - klasického konceptu řízení a inženýrského vypořádání rizik je extrémně vysoká,
   - konceptu řízení a inženýrského vypořádání rizik zvažujícího lidský faktor, je velmi vysoká,
   - konceptu řízení a inženýrského vypořádání rizik zaměřeného na zabezpečený systém je vysoká,

- konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém je střední,
- konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém systémů je nízká.

Obr. 21. Koncepty řízení a inženýrského vypořádání rizik; TZ = technologické zařízení, technické dílo.

Uvedený výsledek také znamená, že ani progresivní koncept, kterým je řízení bezpečnosti systému systémů, nezaručuje zanedbatelnou míru kritičnosti. Důvodem jsou rizika napříč systémů náležejících do systému systémů (SoS) a do propojení SoS s okolím, která nejsme schopni na základě současných znalostí a zkušeností předem všechna odhalit.

Z výše uvedených fakt vyplývají základní principy pro práci a riziky, a to: být proaktivní; domýšlet možné důsledky; správně určovat priority z pohledu veřejného zájmu; myslet na zvládnutí nepřijatelných dopadů; zvažovat synergie; a být ostražitý [6], což odpovídá filosofii prosazované v pracích [3,4,17]. Proto při stanovení rizika pro strategické rozhodování je nutno používat hierarchický multikriteriální postup; recentní odborné práce používají pojem hierarchické holografické modelování (HHM).

4. Cíl práce s riziky: snížení rizika; zabezpečený systém; bezpečný systém; a bezpečný systém systémů.
5. Práce s riziky. Nejprve si musíme uvědomit, že pro kvalitní práci musíme: mít kvalitní data o objektu a procesech, které uvnitř i vně něho probíhají [3,4]; a zvolit správný kontext řešení (obrázek 3). Na základě každého konceptu chápání rizik je třeba rizika identifikovat, analyzovat, hodnotit, posuzovat, řídit, vypořádat a stále sledovat; obrázek 14. Model platí pro práci s riziky za normálních a abnormálních

podmínek a platí pro všechny typy rizik, tj. dílčí, integrovaná i integrální (dílčí – zvažuje se jedno aktivum; integrovaná – zvažuje se agregace pro více aktiv; integrální – zvažují se aktiva i vazby a toky mezi nimi).

V případě výskytu kritických podmínek je třeba zvážit příčinu kritických podmínek, tj. odhalit přispěvatele k riziku, který způsobil kritické podmínky a absolvovat proces od počátku. Z obrázku 14 je zřejmá zásadní role monitoringu. V případě, že se zjistí, že riziko je nepřijatelné, je třeba provést změny, jak naznačují zpětné vazby na obrázku 14. Protože změny vyžadují zdroje, síly a prostředky, tak na základě zajištění hospodárnosti se nejprve realizuje zpětná vazba 1, a teprve, když nepřinese žádoucí stav, tak se realizuje zpětná vazba 2; poté zpětná vazba 3, a když ani po ní není žádoucí výsledek, tak zpětná vazba 4. V případě výskytu extrémních jevů s katastrofickými dopady se přikračuje okamžitě k realizaci zpětné vazby 4.

Je třeba také poznamenat, že kritický je také výběr kvalitativního nebo kvantitativního přístupu při oceňování rizik, protože s kvantifikací rizika se musí zacházet obezřetně, jelikož výpočty rizika vytváří falešný pocit jistoty a bezpečí [2]. Použití postupů při práci s riziky, které jsou založeny na příliš jednoduchých postupech, vede k chybám, jejichž důsledky mohou být velké havárie či velká selhání, jak ukazují analýzy reálných havárií [62], které dle výše uvedené terminologie označujeme jako organizační havárie. Proto je třeba vždy porovnat pro a proti při použití kvantitativní a kvalitativní analýzy. Pokud se hovoří o kvantifikaci, je třeba zmínit a porovnat úrovně kvantifikace: verbální (velký, malý), ordinální (např. od 1 do 10), bodové hodnocení, intervalové hodnocení, výpočet pravděpodobnosti, výpočet na základě důkazů (Bayesův teorém). Předmětný výpočet je náročný na data a je zdlouhavý.

Na základě dosavadních znalostí a zkušeností, shrnutých v práci [17], platí:

- důvody podporující kvantitativní analýzu jsou: stanovení rizika je výsledkem objektivních metod a postupů včetně statistické analýzy dat; výsledky analýzy rizika jsou také v „manažerském jazyce“ – procenta, finance apod.; poskytují se dostatečné podklady pro analýzu nákladů a přínosů; a je možné sledovat a kontrolovat výkonnost řízení rizik,
- důvody proti kvantitativní analýze jsou: výpočty mohou být někdy složité a mohou pro nezasvěceného vypadat jako černá skříňka; a ke kvantitativní analýze jsou potřebné znalosti a počítačové programy,
- několik doporučení ke kvantitativní analýze: riziko jako číslo často fascinuje, ale současně omezuje vnímání souvislostí. Z hlediska komunikace s veřejností, je třeba upozornit na to, že velmi nízké pravděpodobnosti se obtížně vztahují ke každodenním zkušenostem. Například jeden/jedna z miliónu v čase znamená 30 sekund za rok. Proto je žádoucí jistá míra analogie; údaje typu 10^{-5} nevyjadřují aktuální riziko, nýbrž jsou statistickou horní hranicí možnosti, že riziko by se mohlo vyskytnout. Díky mocnině deseti se věří, že snížení rizika o řád nebo o dva řády je pouhým násobkem deseti. Snížení rizika 10^{-3} na 10^{-4} znamená, že riziko se sníží o devadesát procent. Následné snížení z 10^{-4} na 10^{-5} je desetkrát menší, a tudíž devíti procentní. Proto se doporučuje vyjadřovat snížení rizika graficky; a kvantitativní přístup k riziku musí tudíž vycházet z prosté zásady: spíše měřit to, co je měřitelné, než měřit to, co je důležité. Pokud důležité je současně měřitelné, tím lépe,
- důvody pro použití kvalitativní analýzy jsou: výpočty, pokud se dělají, jsou jednoduché a snadno pochopitelné; není nutné kvantitativně určit četnost výskytu

pohrom; není nezbytné určit náklady na opatření zmírňující působení rizikových faktorů; kvalitativní analýza uspořádá a doporučí oblasti pro hlubší a detailnější posouzení,

- důvody proti použití kvalitativní analýzy jsou: výsledky včetně stanovení rizika jsou převážně subjektivní; nepracuje se s žádnou hodnotou a hodnotovými ukazateli; pro návrh protiopatření jsou poskytnuty pouze náznaky problému; není možné sledovat účinnost a výkonnost procedur řízení rizika, protože chybí objektivní měřítko,
- několik doporučení ke kvalitativní analýze: kvalitativní přístup k riziku by se měl zabývat jen potenciálem / možností výskytu; kvalitativní přístup je založen na popisných hodnotách s relativní důležitostí, takže nelze opomenout následující problémy kvalitativního přístupu: Jak vysoké je vysoké riziko nebo jaká je porovnatelnost různě vysokých rizik? Jaké jsou rozdíly mezi vysokým–středním, vysokým–nízkým, středním–nízkým?; a skórování rizika může vést k chybnému rozhodnutí, které znamená, že opatření se dělají tam, kde by se dělat nemusela, a naopak kde by se měla dělat, se nedělají.

6. Orientace na kritické položky. Protože nikdy není dostatek zdrojů, sil a prostředků, tak se v inženýrské praxi orientujeme jen na kritické atributy, tj. jen na nepřijatelná a podmíněně přijatelná rizika [3] a ISO normy založené na projektovém řízení typu TQM (Total Quality Management), tj. ISO 9000, 14000, 18000 a 30000 (seznam vyhodnocených rizik; seznam rizik vyžadujících nejvyšší pozornost; seznam neaktuálních / vyřešených rizik).
7. Počet sledovaných aktiv. V praxi se používají modely: jedno aktivum; více aktiv, jejichž hodnotu lze vyjádřit jednou proměnnou, nejčastěji penězi; více nesouměřitelných aktiv – lidský systém [2]. Tj. zvažujeme buď dílčí riziko, anebo složené, které je buď integrované, anebo integrální. Integrované je definovaný součet dílčích rizik a nezahrnuje zpravidla vlivy vazeb a toků v systému. Integrální či komplexní vychází ze systémového pojetí reality, tj. zahrnuje i vlivy vazeb a prvků [2], což je případ lidského systému i složitých technologických objektů.
8. Závislost na místě. Riziko je místně specifické a určuje se z velikostí místních ohrožení, která vytváří možné pohromy v daném místě s ohledem na míry zranitelnosti místa a jeho aktiv vůči konkrétním možným pohromám.

5.2. Model pro zajištění koexistence technického díla a jeho okolí v čase

V případě několika nesouměřitelných aktiv v otevřeném systému, což je u každého technického díla, je nutno použít multikriteriální přístup a hledat optimum [2]. Přitom je pravdou, že optimum pro systém s více nesouměřitelnými aktivy nemusí ležet těsně u optim pro jednotlivá aktiva. Specifikum manažerských a inženýrských metod, nástrojů a technik spočívá v tom, že od sebe nelze oddělit charakteristiky jevů, před kterými předmětný objekt musí být chráněn, vlastnosti materiálů, území konstrukcí a zařízení, které tvoří objekt, provozní podmínky a limity, detekci narušení objektů při překročení stanovených limitů a korekční opatření podporující bezpečnost objektu a jeho okolí. Protože jejich cílem je kvalitní řešení v daných podmínkách, musí kloubit exaktní výsledky s výsledky dobré inženýrské praxe, a to především znamená používat pouze ověřené postupy a ověřená data. Vlastní inženýrské řešení a výběr metod,

nástrojů a technik pro práci s riziky je závislé na: počtu a charakteru sledovaných aktiv; volbě konceptu řešení problému; a fázi řízení – prevence, připravenost, odezva, obnova. Jelikož rizika mají různé zdroje, tj. závisí jak na pohromách, tak na místních zranitelnostech, tak na metodách jejich zvládání a řízení, které odráží chyby na straně všech zúčastněných, je třeba postupovat obezřetně a dodržovat postup:

- určit pohromy, které mohou systém postihnout a přitom respektovat All-Hazard-Approach [99] ve formě popsané v [1,16,18],
- možné pohromy rozdělit na relevantní, specifické a kritické [1,2],
- aplikovat procesní model pro práci s riziky nebo jeho pokročilé modifikace, jejichž přehled je v práci [2], a určit, pro která rizika se budou dělat opatření a činnosti pro: prevenci; zmírnění; odezvu; obnovu; a která RIZIKA zůstanou nezajištěná [2],
- provést realizaci opatření a zajistit monitoring s důrazem na údržbu, opravy a včasnou aplikaci nápravných opatření [2].

Celkový postup, který zajišťuje koexistenci území a technického díla během jeho životnosti je popsaný v práci [3] je zobrazen na obrázku 22.

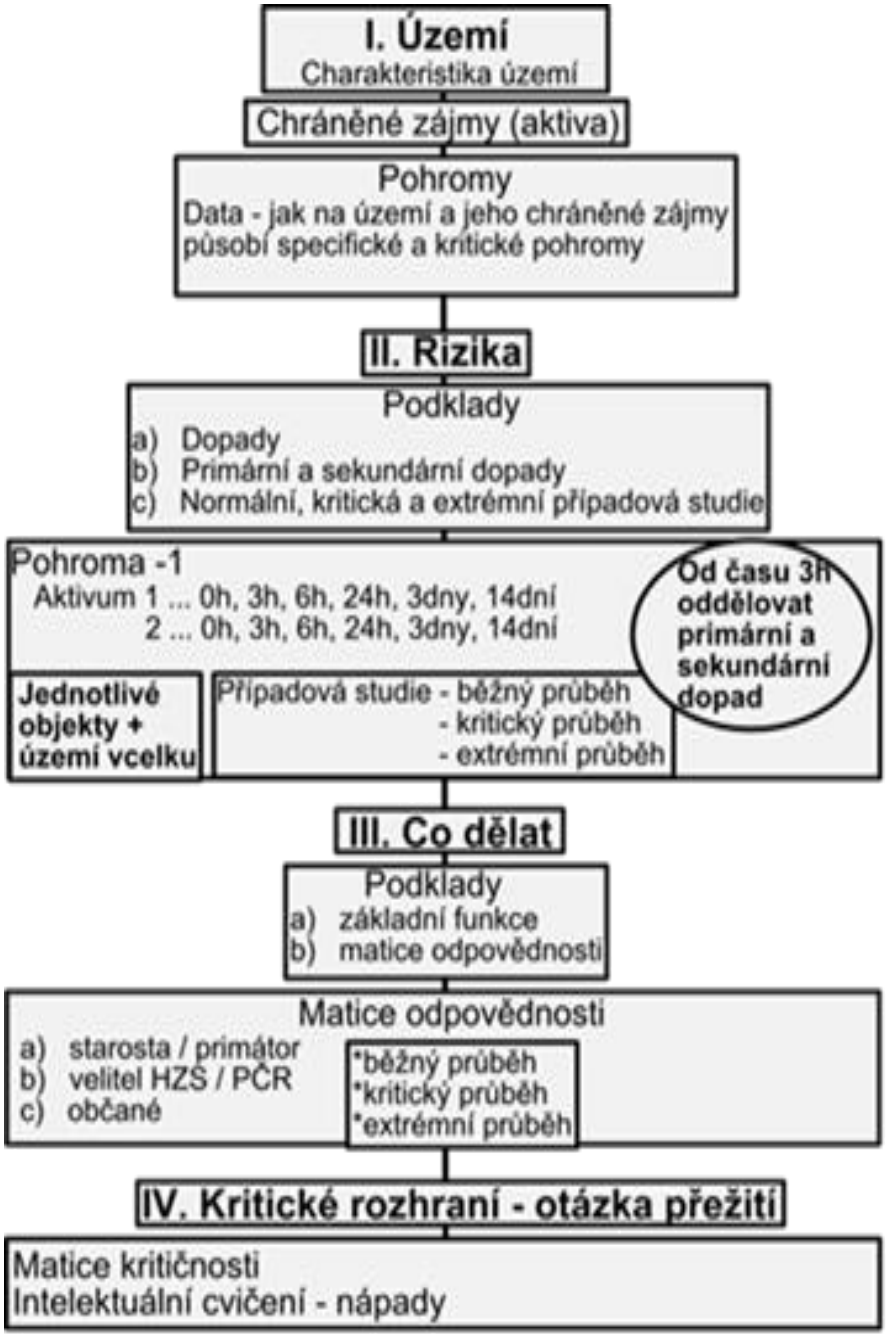
Obrázek 22 ukazuje, že v první fázi se stanoví charakteristiky území a charakteristiky možných pohrom (v ČR pro oblast územního plánování existují jednotným způsobem zpracované územně analytické podklady obcí v grafické podobě, které jsou pro stát v archivu v Brně, a které lze použít pro běžné potřeby; pro kritické objekty je nutno dělat vlastní detailní průzkum a studie); v druhé se určí rizika na základě zvážení ohrožení, které představují možné pohromy dle možné velikosti, a zvážení místních zranitelností, a to území i veřejných aktiv; ve třetí se zváží jednak účinnost aplikovaných preventivních, zmírňujících, reaktivních a obnovovacích opatření a činnosti, a jednak zajištění odpovědností a kvalita podpor pro kvalitní odezvu; ve čtvrté části se hledají způsoby řešení možných situací, které mají rysy, jež mohou ohrozit přežití lidí a nejsou řešeny v předchozích krocích. V případě vložení technologických objektů do území je právě v části III třeba řešit koexistenci objektu s územím, tj. provádět prevenci domino efektů a jiných dopadů, které mohou za jistých podmínek nastat.

Za normálního stavu SoS je obtížné identifikovat průřezová rizika, a proto se použila známá skutečnost, že průřezová rizika se projevují sekundárními a vyššími dopady na aktiva SoS při výskytu pohrom, jejichž velikost přesahuje úroveň projektových pohrom (tj. velikost pohrom, do které se dělají systematicky preventivní opatření na zabránění nebo zmírnění dopadů možných pohrom na aktiva) [2,3]. Specifickým přístupem, který požaduje zpracování extrémních scénářů pohrom, by měly být odhaleny atypické scénáře pohrom, které se nevyskytují za normálních podmínek, a proto nejsou odhaleny při běžných analýzách rizika [2,3].

Navržený nástroj de facto představuje sestavení místních scénářů, které v případě jednotlivých pohrom zahrnují obojí, jak místní projevy pohrom (tj. akce), tak i lidské reakce. Analytickým způsobem nástroj odhaluje slabiny v lidských reakcích na možné pohromy, a to v oblasti prevence, připravenosti, odezvy i obnovy, pomocí specifických technik dovoluje určit závažnost slabin a za pomocí praktik dobré inženýrské praxe navrhuje zlepšení v lidských reakcích s cílem zvýšit bezpečí pomocí zvýšení úrovně bezpečnosti. Nástroj se skládá ze 4 částí:

1. Screening technického díla a jeho okolí.
2. Vyhodnocení rizik technického díla i jeho okolí.

3. Screening existujících opatření a činností pro řízení rizik technického díla a pro zvyšování bezpečnosti technického díla a vyhodnocení úrovně vyjednávání s riziky.
4. Identifikace kritických položek řízení rizik technického díla a návrh řešení gapů spojených s přežitím či kontinuitou aktiv při kritických pohromách.



Obr. 22. Procesní model fází řízení bezpečnosti území. Fáze: I- charakteristika území, tj. aktiv, zdrojů domino efektů a možných pohrom; II-stanovení rizik pro 3 velikosti každé možné pohromy; III-souhrnné posouzení zacílené na identifikaci konfliktů, nepokrytých závažných problémů a chybějících odpovědností; IV-stanovení kritických situací a opatření pro přežití lidí.

V prvním kroku se provádí screening SoS, který se skládá z následujících částí:
- stanovení charakteristiky SoS (v případě území charakteristika v rozsahu územně plánovací dokumentace, jak ji požaduje územní plánování),
- klasifikace SoS (v případě území – průmyslová oblast, zemědělská oblast, les…),
- aplikace propojení přístupu All-Hazard-Approach ve formě [16] vytvořené pro Evropu a dokumentace o SoS, kterou se stanoví soubor pohrom, které mohou mít na SoS nepřijatelné nebo podmíněně přijatelné dopady, tj. jsou nebezpečné pro SoS,
- identifikace zranitelných míst SoS (např. pomocí SWOT analýzy se stanoví slabé a silné stránky, rizika a možnosti řídícího mechanismu SoS).

V druhém kroku se ocení rizika SoS spojená se všemi pohromami identifikovanými jako nebezpečné v prvním kroku. S ohledem na existenci náhodných a znalostních nejistot v datech se:
- zpracují variantní scénáře realizace rizik v SoS pro jednotlivé nebezpečné pohromy (např. pomocí propojení modifikované formy metody What, If [2,9] a cíleně zaměřené metody případové studie [8]); s ohledem na poznání se vytvoří scénáře pohrom normální, kritické a extrémní, ve kterých jsou odděleně sledovány dopady na jednotlivá aktiva SoS ve stanovených časových intervalech (např. u území se osvědčily simulace pro časové úseky měřené od vzniku pohromy 0h: 0h, 3h, 6h, 24h, 3 dny, 14 dní, 1 měsíc),
- u jednotlivých nebezpečných pohrom se vyhodnotí sekundární a vyšší dopady na aktiva SoS, pozorovatelné v časech 3h, 6h, 24h, 3 dny, 14 dní, 1 měsíc, a to především u scénářů nebezpečných pohrom kritických a extrémních a odhalí se místa vzniku kaskádovitých selhání a možné kaskády dopadů,
- celkovým vyhodnocením údajů získaných pro pohromy identifikované jako nebezpečné pro SoS se určí zranitelné položky SoS,
- stanoví se četnost selhání jednotlivých zranitelných položek SoS s ohledem na pohromy identifikované jako nebezpečné pro SoS,
- sestaví se matice kritičnosti pro SoS (pro jednotlivé zranitelné položky SoS se skóruje četnost selhání a závažnost selhání oceněná velikostí ztrát na aktivech SoS) a dle vhodné hodnotové stupnice se určí vysoce kritické, středně kritické a běžně kritické položky SoS.

V třetím kroku se na základě existující dokumentace pro řízení bezpečnosti SoS, což v současné době znamená, že se zváží opatření a činnosti pro řízení rizik platné pro jednotlivé systémy a provede se ocenění jejich účinnosti v oblasti řízení rizik SoS – pro jednotlivé položky řízení rizik (akty řízení, technická oblast, znalostní oblast, finanční oblast, personální oblast, odpovědnosti) se:
- provede screening existujících opatření a činností pro řízení rizik dílčích systémů SoS a posoudí se jejich vhodnost pro zvyšování bezpečnosti SoS,
- provede ocenění úrovně vyjednávání s riziky u všech pohrom, které byly identifikovány jako nebezpečné pro SoS, a to zvláště pro vysoce kritické a středně kritické položky SoS, a pro potřeby řízení bezpečnosti SoS se úroveň oklasifikuje dle vhodné stupnice,
- sestaví matice odpovědností a jejich úroveň se posoudí z hlediska příslušných kompetencí na úrovni jednotlivých systémů i celého SoS; logicky odpovědnosti za řízení bezpečnosti SoS musí být primární,
- posoudí postupy a režimy řízení SoS, které vzniknou agregací postupů a režimů řízení dílčích systémů, pozornost se soustředí na odhalení konfliktů a gapů při

implementaci v praxi a na to, jak jsou zajištěny znalostně, materiálně, technicky, personálně a finančně,
- posoudí dostatečnost a přístupnost zdrojů, sil a prostředků s ohledem na zvládnutí selhání středně a vysoce kritických položek SoS s přijatelnými ztrátami a škodami,
- posoudí účinnost specifických postupů jako je varování, schopnost reakce na varovací instrukce apod.

Na závěr se identifikují oblasti, ve kterých se rizika SoS řídí nedostatečně nebo vůbec neřídí.

Ve čtvrtém kroku zaměřeném na identifikaci kritických položek řízení rizik SoS a na návrh řešení gapů spojených s přežitím či kontinuitou aktiv při kritických pohromách se určují rozhraní, která vedou k rozpadu až zániku některého z aktiv nebo celého SoS. Postup je následující:
- posoudí se závažnost oblastí, ve kterých se rizika SoS řídí nedostatečně nebo se neřídí vůbec a pro vysoce závažné oblasti z pohledu veřejného zájmu se navrhnou reálná opatření a činnosti proti rozpadu až zániku některého z aktiv nebo celého SoS, zpracuje se plán jejich realizace (většinou dlouhodobý) a zajistí se jeho implementace po všech stránkách,
- na základě kritického pohledu na extrémní a kritické scénáře možných nebezpečných pohrom se s ohledem na základní veřejná aktiva (životy a zdraví lidí, kvalitní životní podmínky a možnost rozvoje) prověří znovu možná opatření a činnosti pro přežití či kontinuitu veřejných aktiv, aby nedošlo k přesahu prahu kritičnosti podmínek jejich existence.

SMS pro SoS se tudíž skládá ze systému řízení bezpečnosti, který řídí průřezová rizika a předurčuje cíle systémů řízení bezpečnosti pro jednotlivé systémy SoS. To znamená, že SMS každého dílčího systému SoS se změní následujícím způsobem:
- vstupní položka „monitoring vnitřních a vnějších procesů a jevů“ se změní na položku „monitoring vnitřních a vnějších procesů a jevů a pokyny pro řízení dílčího systému z pohledu řízení bezpečnosti SoS,
- výstupní položka „projev bezpečnosti“ se změní na položku „projev bezpečnosti a možné dopady na okolí, tj. na další systémy SoS“ a celé okolí SoS.

Vstupní položka SMS pro SoS je položka „monitoring vnitřních a vnějších procesů a jevů a chování jednotlivých dílčích systémů“. Výstupní položka je „projev bezpečnosti SoS“.

5.3. Zásady pro řízení rizik technických děl

Podle Mezinárodní organizace pro standardizaci (ISO) kvalifikované řízení rizik technického díla musí:
- být součástí systému řízení sledovaného technického díla.
- být součástí každého procesu rozhodování sledovaného technického díla,
- explicitně zvažovat nejistoty a neurčitosti v procesech a podmínkách sledovaného technického díla a jeho okolí,
- být systematické a strukturované,
- vycházet z nejlepších dostupných informací,
- být dynamické a vhodně reagovat na různé změny,
- být uzpůsobeno místním podmínkám a legislativním požadavkům,

- respektovat vliv člověka (lidský faktor) na technické dílo,
- mít schopnost neustálého zlepšování.

Systém řízení technického díla je tudíž zároveň ***systém řízení bezpečnosti*** **(SMS)** technického díla. Má cíl zvyšovat bezpečnost a provádí to na základě snižování rizik na úroveň přijatelného rizika. Má široko akceptované priority jak zvládnout nebezpečí, kterými jsou:
- eliminovat zdroje nebezpečí,
- redukovat (omezit) možné dopady, tj. možná nebezpečí pro chráněná aktiva,
- zvládnout rizika,
- lokalizovat a zmírňovat škody.

Znovu shrneme základní hlediska pro řízení rizik technických děl dle [4]:

1. Jde o složité socio-kyber-technologické systémy typu SoS, které musí být bezpečné po celou dobu životnosti, a proto řízení rizik musí být zacíleno na integrální bezpečnost a být ve všech aspektech ucelené, systémové a proaktivní.
2. Technická díla po celou dobu životnosti musí plnit kvalitně úkoly a ani při svých kritických podmínkách neohrozit sebe ani své okolí (tj. aplikuje All-Hazard-Approach, Defence-In-Depth, má program na neustálé zvyšování bezpečnosti a kultury bezpečnosti).
3. Složitá technologická zařízení (jaderné elektrárny, dálnice, přehrady, velká letiště, velké výrobní celky apod.) jsou důležitá pro zajištění základních funkcí státu, a mnohá i celé EU, a proto se povinnosti při vypořádání rizik se rozdělují mezi všechny zúčastněné.

Proto na základě výzkumu popsaného v [4] z pohledu bezpečí a rozvoje lidí, území i státu je řízení rizik těchto složitých technologických zařízení důležité ve dvou oblastech:

A. Oblast propojující veřejnou správu a management technického díla.

B. Oblast věcná zabývající se daty, metodami, materiálovými a technickými záležitostmi, organizačními, právními, finančními a personálními záležitostmi přímo v technickém díle.

Zásady pro řízení rizik technického díla na úseku propojení veřejné správy a managementu technického díla jsou stanoveny pro úrovně ŘÍZENÍ:

1. A1 - politickou (parlament, vláda, veřejná správa).
2. A2 - strategickou (veřejná správa, vlastník, investor, provozovatel).
3. A3 - taktickou (veřejná správa, vlastník, investor, provozovatel).
4. A4 - operativní / funkční (provozovatel).
5. A5 - technickou (provozovatel).

Výsledky kritické analýzy a kritického posouzení způsobů řízení rizik spojených s technickými díly v praxi [4] ukázaly počty zásad uvedené v tabulce 23; konkrétní zásady jsou v [4].

Tabulka 23. Zásady pro řízení rizik technického díla na úseku propojení veřejné správy a managementu technického díla

Úroveň řízení	**Počet zásad**
A1 - Politická (parlament, vláda, veřejná správa)	4
A2 - Strategická (veřejná správa, vlastník, investor, provozovatel)	8
A3 - Taktická (veřejná správa, vlastník, investor, provozovatel)	4
A4 - Operativní / funkční (provozovatel)	5
A5 - Technická (provozovatel)	19
CELKEM	40

Zásady pro řízení rizik technických děl ve věcné oblasti na úsecích jsou pro úseky:

1. B1 - Koncepce technického díla a způsob řízení technického díla.
2. B2 - Požadavky na data, metody a techniky, které zajišťují kvalitní rozhodování a řízení technického díla.
3. B3 - Postupy pro správné umístění, kvalitní projekt, výstavbu a provoz technického díla.
4. B4 - Zajištění kontinuity provozu technického díla a podpory základních funkcí státu, tj. veřejného zájmu.

Výsledky kritické analýzy a kritického posouzení způsobů řízení rizik spojených s technickými díly v praxi [4] ukázaly počty zásad uvedené v tabulce 24; konkrétní zásady jsou v [4].

Tabulka 24. Zásady pro řízení rizik technického díla ve věcné oblasti pro: vlastníka, investora, provozovatele, odborný management, zaměstnance, inspektory, kontraktory, participující odborníky a další zúčastněné.

Oblast řízení rizik technického díla	**Počet zásad**
B1 - Koncepce technického díla a způsob řízení technického díla	21
B2 - Požadavky na data, metody a techniky, které zajišťují kvalitní rozhodování a řízení technického díla	9
B3 - Postupy pro správné umístění, kvalitní projekt, výstavbu a provoz technického díla	13
B4 - Zajištění kontinuity provozu technického díla a podpory základních funkcí státu, tj. veřejného zájmu	23
CELKEM	66

Protože zdrojů, sil a prostředků na bezpečnost, tj. na řízení rizik, není nikdy dostatek, je třeba z důvodů hospodárnosti postupovat následovně:

- rizika určovat jen pomocí dat a metod, které zajistí kvalitní podklady pro rozhodování o vypořádání rizik na příslušné úrovni řízení,
- na strategické úrovni řízení a inženýrského vypořádání rizik je nutné řešit rizika technického díla tak, že ho chápeme jako SoS - jde o zajištění dlouhodobé existence a rozvoje technického díla i jeho okolí,
- na taktické a funkční úrovni řízení a inženýrského vypořádání rizik je nutné řešit rizika technického díla způsobem zaměřeným na bezpečný systém,
- na technické a funkční úrovni řízení a inženýrského vypořádání rizik lze řešit rizika technického díla způsobem zaměřeným na zabezpečený systém**, *jen tehdy, když*** výskyt možných škod v okolí systému je málo pravděpodobný, anebo škody jsou přijatelné (např. manipulace s nádrží s vysoce nebezpečnou látkou již do předmětné kategorie nepatří).

Pro řízení a vypořádání rizik technického díla je důležitá motivace rizika skutečně snižovat ve prospěch veřejného zájmu a odpovědnost za provádění činností, které vedou ke snížení rizik. Je třeba si uvědomit, že akademická sféra dává řadu sofistikovaných doporučení, která však v praxi ztroskotávají na tom, že není jasně určená odpovědnost a nejsou stanovená jasná pravidla [34].

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie (popularizované jako ***černé labutě, dračí králové*** atd.).

Proto nyní při řízení bezpečnosti technických děl víme, že složitá technická díla jsou z různých důvodů čas od času v nestabilním stavu a vznikají organizační havárie, kaskády selhání bez zjevné příčiny, neobvyklé jevy apod., tj. připouštíme existenci nejistot jak náhodných, tak i epistemických (znalostních) v jejich chování.

Z důvodu zajištění jejich bezpečnosti a ochrany lidí musíme připravovat řešení odezvy pro možné případy, kdy se realizují rizika z příčin, které nelze odhalit pravděpodobnostními přístupy, a pro kvalitní odezvu budovat náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik inženýrů a záchranářů.

5.4. Vypořádání rizik technických děl

Člověk se snaží vytvářet technická díla tak, aby:
- fungovaly, co nejdéle, a to bez závad nebo jen s malým počtem závad,
- co nejlépe plnily požadované funkce,
- byly co nejlevnější,
- spotřebovávaly, co nejméně energie a co nejméně nedostatkových surovin,
- měly, co nejmenší hmotnost (omezené požadavky na materiál),
- zabíraly, co nejmenší prostor,
- neohrožovaly ani sebe, ani okolí,
- nevyžadovaly vysoce kvalifikovaný personál
- neprodukovaly velké množství nebezpečného odpadu
- apod.

Každé technické dílo zahrnuje technické prostředky, technické postupy, člověka, znalosti a dovednosti vytvářet cíleně nové produkty. Jeho vazby jsou povahy technické

„stroj-stroj“, povahy smíšené „člověk-stroj“ a v posledních letech významnou roli hrají vazby „člověk-PC" a „stroj-PC“. Toky v systému jsou energetické, materiálové, informační, finanční a instrukční aj.

Na základě poznatků a zkušeností shrnutých v [3,4,11,17] pro bezpečnost technických děl platí následující pokyny:

1. Opatření pro podporu bezpečnosti musí vycházet z jasného chápání primárních výrobních procesů, ze všech jejich přidružení a ze všech důležitých možných scénářů jevů vedoucích ke škodě a ztrátám.
2. Řízení bezpečnosti technických děl se musí provádět v celém životním cyklu infrastruktury, tj. při projektování, konstruování, instalování, provozování, udržování, pozměňování, vyřazení z provozu. Analýza rizika musí pokrývat všechny uvedené fáze, při kterých technické dílo působí dopady na své okolí (viz rizika uvedená v kapitole 4).
3. Způsob zajištění bezpečnosti technického díla musí zahrnovat identifikaci, ovládání a monitorování scénářů řízení na 3 úrovních:
   - přímé řízení rizik technického díla za normálního, abnormálního a kritického stavu,
   - plány, postupy a předpisy pro optimální přímé ovládání rizika technického díla,
   - struktura kontrol činnosti systému řízení bezpečnosti a provádění jeho vylepšení.
4. Smyčky, zpětná vazba a monitoring, které jsou mezi činnostmi na výše uvedených 3 úrovních, spouštějí revize a vylepšení systému řízení technického díla.
5. Systémy řízení technického díla na hierarchicky vyšší úrovni řídí kritické bezpečnostní úlohy na nižší úrovni. Předmětný přístup zajišťuje:
   - vždy dostupné lidské reservy,
   - kompetentnost provozovat bezpečně za všech situací,
   - zaměření a motivování na zajištění bezpečnosti,
   - komunikaci vně i uvnitř o propletených úkolech,
   - existenci postupů, plánů a pravidel pro dosažení bezpečnosti,
   - výběr vhodného technického projektu pro zajištění optimální bezpečnosti,
   - použití uživatelsky příjemných a ergonomických rozhraní stroj-člověk,
   - existenci systému na řízení konfliktů mezi bezpečností a ostatními cíli společnosti při výrobě a údržbě, projektování apod.

Zajištění bezpečnosti technického díla vyžaduje systematický přístup. Je nutné, aby iniciativy související s uvedeným problémem byly v souladu se začleněním ČR do mezinárodních společenství a aktivit. Proto je vhodné aplikovat následující model:
- stanovit co a proč je nutné chránit,
- stanovit minimální úroveň ochrany,
- posoudit současnou úroveň ochrany,
- v případě zjištění, že ochrana je nedostatečná navrhnout opatření,
- zajistit prostředky pro další ochranu a aplikovat opatření pro ochranu,
- periodicky kontrolovat stav,
- udržovat ochranu na odpovídající úrovni,
- revidovat opatření v závislosti na vývoji.

Rozdělení kompetencí a odpovědností je zásadní a důležité v každé složitější činnosti lidské společnosti i u každého složitějšího technického díla. Za bezpečnost technic-

kého díla odpovídají vlastníci a provozovatelé, ale i veřejná správa, která musí provádět dohled nad bezpečností technického díla ve veřejném zájmu.

S ohledem na zajištění bezpečí a rozvoje lidí je třeba jasně právně vymezit dílčí odpovědnosti za zajištění celkové bezpečnosti. Pro všechny důležité činnosti v technickém díle je třeba mít závazné matice odpovědnosti [8]. Nedostatečně stanovené odpovědnosti vedou ke ztrátám, jak ukazují zprávy ze zásahů při haváriích [3,4]. Podle verdiktů soudů o určení viny u několika havárií (např. dopravní nehoda vlaku ve Studénce v r. 2008) je zřejmé, že odpovědnost za bezpečnost technických děl je vágně stanovena v českém právu. Možná je to problém národních legislativ, jak ukazuje hodnocení železniční nehody v roce 2013, která se stala několik kilometrů od španělské železniční stanice Santiago de Compostela – španělská vyšetřovací komise obvinila strojvedoucího a Evropská drážní agentura, používající moderní způsoby vyšetřování havárií našla kořenovou příčinu této dopravní nehody v chybách řídicího systému drah [101].

5.5. Nástroje pro vypořádání rizik technických děl

Na základě poznatků shrnutých v pracích [1-4,11,13,17,25-39] rizika vypořádáme na základě aplikace technických nebo organizačních opatření. Technická opatření provedená v rámci prevence jsou velmi účinná (až 80%) [1,3]. Organizační opatření jsou účinná méně, ale pro ochranu lidí a dalších veřejných aktiv jsou velmi důležitá.

5.5.1. Technická opatření

Technická opatření se aplikují ve všech fázích řízení bezpečnosti, tj. při přípravě i výstavbě (zadávací podmínky, limity a podmínky, preventivní opatření, průkazy odolnosti apod., dohled ze strany státu stanovený legislativou), provozu provozní předpisy pro normální, abnormální a kritické podmínky, plány odezvy na projektové havárie (nouzové, havarijní), plány kontinuity a plány odezvy na nadprojektové havárie) [1,3].

Pro důležité technické objekty se používá koncept bezpečnosti kritických objektů založený na komplexním přístupu, zvaném obrana do hloubky [48,49], který byl vyvinut odborníky z oblasti jaderné energetiky s cílem, aby veřejnost i životní prostředí byly ochráněny před veškerými riziky spojenými s provozem energetických jaderných zařízení. Koncept obrana do hloubky a kultura bezpečnosti sloužily jako základní filozofie pro bezpečný projekt a bezpečný provoz kritických objektů. Podle údajů v uvedených citacích správně použita obrana do hloubky zajišťuje, že žádná jednotlivá lidská chyba nebo jednotlivé selhání zařízení na jedné úrovni obrany, ani kombinace selhání na více než jedné úrovni obrany, nemůže ohrozit obranu v hloubky na následující úrovni nebo vést poškození veřejnosti nebo životního prostředí.

Podle INSAG-10 [49] obrana v hloubky tvoří hierarchické rozmístění různých úrovní vybavení a postupů s cílem zachovat efektivitu fyzických bariér, které jsou umístěné mezi radioaktivní materiál a pracovníky, veřejnost nebo životní prostředí, při běžném provozu, předpokládaných provozních událostech, a u některých bariér i při havárii. Obrana do hloubky je obecně rozdělena do pěti úrovní. Když jedna úroveň selže, vstupuje do hry následná úroveň.

Tabulka 25 shrnuje cíle každé úrovně a odpovídající prostředky, které jsou nezbytné k jejich dosažení [48]. Úrovně jsou určeny jako nezávislé v rozsahu použití. Obecným cílem obrany do hloubky je zajistit, aby jednotlivá porucha, selhání zařízení nebo selhání lidského faktoru na jedné úrovni obrany, a dokonce i kombinace selhání na více než jedné úrovni obrany, se nešířily do dalších úrovní obrany do hloubky. Nezávislost různých úrovní obrany je rozhodující pro splnění uvedeného cíle [50].

Tabulka 25. Úrovně obrany do hloubky (zpracováno dle [48]).

Úrovně obrany do hloubky	**Cíl**	**Podstatné prostředky pro dosažení cíle**
1	Prevence abnormálního provozu a selhání.	Konzervativní projekt a vysoká kvalit výstavby a provozu.
2	Zvládnutí abnormálního provozu a detekce selhání.	Ovládání, omezovací a ochranné systémy a další kontrolní (dozorné) rysy.
3	Řízení projektových havárií.	Zavedeny (naprojektovány a zabudovány) prvky zajišťující bezpečnost a postupy pro řízení havárií.
4	Řízení neprojektových podmínek objektu včetně prevence rozšiřování havárie, a zmírňování důsledků krutých havárií.	Zavedení doplňujících opatření pro řízení havárií.
5	Zmírnění radiologických důsledků významných úniků radioaktivních materiálů.	Vnější nouzová odezva.

Pomocí kvalitních zadávacích podmínek je třeba vybudovat kvalitní technické dílo (umístění, materiál a konstrukce stavby, zařízení a jejich propojení). Pak je třeba mít způsob ovládání technického díla při:

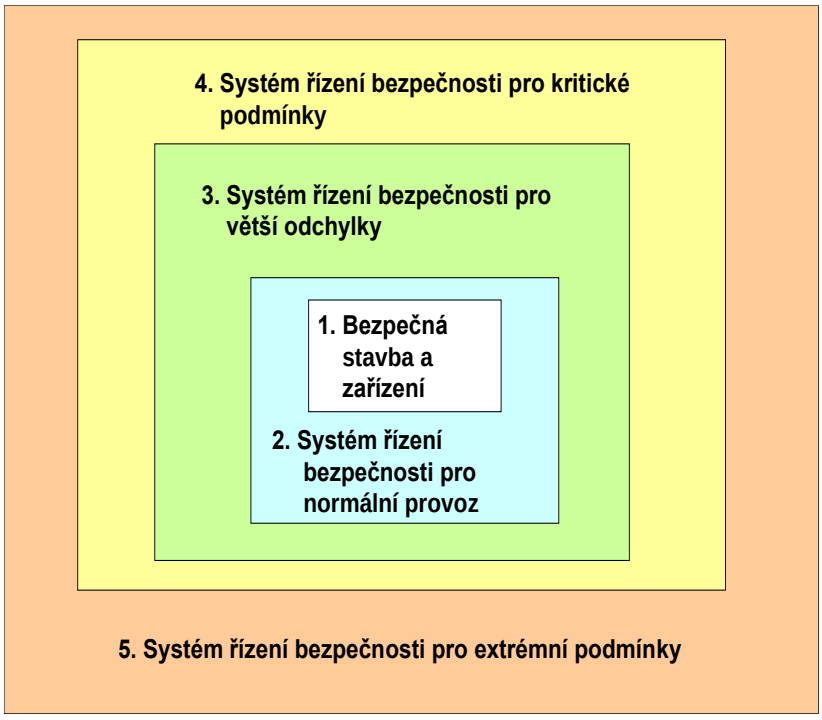
- normálních podmínkách; jde o způsob prevence abnormálního provozu a selhání technického díla,
- abnormálních podmínkách; jde o způsob ovládání abnormálního provozu a detekce selhání technického díla,
- kritických podmínkách; jde o ovládání havárií technického díla pomoci projektových opatření,
- extrémních (nadprojektových) haváriích technického díla, a to včetně prevence dalšího rozvoje havárie a zmírnění dopadů havárie vně technického díla.

Základní prostředky pro splnění požadovaných nároků jsou:

- konzervativní návrh objektu a vysoká kvalita konstrukce a provozu,
- zabudování ovládacích, omezovacích a ochranných systémů a další typické znaky dohledu nad provozem,
- naprojektovány (inherentní) vlastnosti podporující bezpečnost,
- alternativní opatření a řízení havárie – vnitřní plán odezvy,
- vnější plány odezvy.

Protože složitá technická díla jsou základem pro život a rozvoj lidí, je nutné i při nadprojektových podmínkách zajistit, aby objekty bylo možno zprovoznit v jisté dohledné

době po havárii. Proto na základě zkušeností z praxe, autorka metodou analogie uspořádala základní principy pro řízení bezpečnosti objektů a infrastruktur typu systém systémů [3] (obrázek 23) takto:



Obr. 23. Pětistupňový systém řízení bezpečnosti složitého objektu.

1. V návrhu, výstavbě a konstrukci technického díla je třeba používat principy bezpečného projektu (přístupy: All-Hazard-Aproach, proaktivní, systémový aplikující integrální riziko, a také významná dílčí rizika spojená s vazbami a toky hmotnými, energetickými, finančními a informačními v dílčích systémech i napříč nich; správná práce s riziky; a monitoring, ve kterém jsou zabudovány korekční opatření a činnosti). Důležité je sestavení zadávacích podmínek spojených s daným územím, které vyjadřují způsob ocenění místních zranitelností vůči všem relevantním pohromám, které mohou postihnout dané místo, a také ocenění všech místně specifických rysů, které mohou způsobit specifické dopady. Na základě recentního poznání, shrnutého v pracích [17,48], je třeba u kritických složitých objektů zohlednit nejistoty náhodné i znalostní, tj. neurčitosti v datech, aby se předešlo atypickým haváriím, které jsou důsledkem nepředvídatelných jevů, které nelze odhalit běžnými stochastickými metodami.
2. Řídicí systém technického díla musí mít základní řídicí funkce, alarmy a reakce operátora zpracované tak, aby objekt byl udržen v normálním (stabilním) stavu za normálních podmínek.
3. Technické dílo musí mít speciální řídicí systémy orientované na bezpečnost a ochranné bariéry, které ho udržují v bezpečném stavu i při větší změně provozních podmínek (tj. při abnormálních podmínkách) a zabraňují vzniku nežádoucích jevů (havárií či selhání), což znamená, že musí mít dobrou resilienci. Předmětné systémy udržují bezpečný provoz i za změny podmínek nebo mají schopnost zajistit normální provoz po aplikaci nápravných opatření (vyčištění, oprava…).

4. Pro případ, že se vyskytnou kritické podmínky, které způsobí, že dojde ke ztrátě ovládání technického díla, musí mít technické dílo systém opatření pro vnitřní nouzovou odezvu, zmírnění dopadů, a pro návrat do normálního provozu (plán kontinuity a vnitřní nouzový / havarijní plán).
5. Pro případ, že dopady ztráty ovládání technického díla postihnou okolí technického díla, musí mít technické dílo ve spolupráci se správou území opatření i pro vnější odezvu, zmírňující opatření pro prevenci ztrát v technickém díle; a kapacitu pro překonání obtíží, aby byla schopnost technické dílo obnovit.

V odborné oblasti se výše zmíněné vrstvy považují za ochranné bariery (tzv. ochrana do hloubky (Defence-In-Depth) a při rozlišení objektů z hlediska bezpečnosti se používá bezpečnostní charakteristika, že objekt má jednostupňovou nebo až pětistupňovou ochranu do hloubky. Jednotlivé systémy řízení bezpečnosti zajišťují aplikaci technických, provozních a organizačních opatření a činnosti, které jsou navrženy tak, aby buď zabránily iniciaci řetězce škodlivých jevů, anebo tento řetězec zastavily [51].

Protože deterministický přístup k ochraně do hloubky nezvažuje explicitně pravděpodobnost výskytu výzev ani mechanismů, ani nezahrnuje kvantifikaci pravděpodobnosti úspěchu spojeného s provedením prvků a systémů na každé úrovni obrany do hloubky, je deterministický přístup doplňován pravděpodobnostní analýzou bezpečnosti (PSA) v oblasti spolehlivosti systémů, pravděpodobných cílů apod. s cílem zajistit adekvátní úroveň bezpečnosti, která zajišťuje dobře vybalancovaný projekt.

Z důvodu existence neurčitostí, které nelze postihnout stochastickým přístupem [52], se v dnešní praxi kombinují stochastické postupy s expertními údaji získanými vyhodnocením řady případových studií [17].

Pro úspěšné zvládnutí rizik u složitých technologických systémů je dle [51] třeba:
- udržovat provoz technického díla ve středních provozních podmínkách, což lze zajistit tím, že provozní personál: je řádně vycvičený; má potřebné dovednosti; a chápe podstatu řízení základních provozních funkcí,
- zajistit bezpečný provoz technického díla za proměnných podmínek, což lze zajistit tím, že provozní personál: je řádně vycvičený; zná plány provozu za proměnných podmínek; a respektuje požadavky kultury bezpečnosti,
- ovládnout kritický stav zařízení technického díla pomocí preventivních mechanismů (např. pomocí kritických systémů bezpečnosti), což lze zajistit: aplikací pracovních postupů podle jistých přijatých standardů; a výcvikem ve vypořádání odchylek od normálního provozu,
- při ztrátě ovládání technického díla (nadprojektová havárie či nadprojektové selhání) je třeba znovu získat nadvládu nad technickým dílem, k čemuž je třeba vzdělat personál, aby byl schopen: získat povědomí o situaci; pochopit podstatu problému; porozumět omezení základních stejně jako preventivních funkcí ovládání; improvizovat,
- při neschopnosti zvládnout zařízení technického díla, je třeba vzdělat personál, aby byl schopen: odstavit technologii tak, že zajistí, co nejmenší ztráty u technologie; a aktivovat vnější nouzový plán (tj. aplikovat ochranná opatření a činnosti, uvolnit rezervy, provést evakuaci).

Z výše uvedených skutečností vyplývá, že čím vyšší velikost projektové pohromy zvolíme pro umístění, projektování, výstavbu a konstrukci technického díla, tj. zajistíme jeho větší schopnost zvládat dopady pohrom, tj. zajistíme pasivní ochranu, tím vyšší bezpečnost dosáhneme, protože účinnost organizačních opatření v oblasti řízení je vždy nižší než u opatření technických, u kterých dosahuje až 80%.

Zvážení poznatků shrnutých v [3] ukazuje, že požadavky kladené na zařízení, systémy a komponenty technických děl:

- dosud nezvažuji systematicky kaskádová selhání a skutečnost, že ani použití nejlepšího současného konceptu pro zajištění bezpečnosti objektů nemá zanedbatelnou kritičnost (tj. po jeho aplikaci některé zdroje rizika zůstávají nezajištěná) kvůli kaskádovým selhání způsobeným znalostními nejistotami [17],
- příliš spoléhají na účinnost PSA, která hodnotí rizika spojená s procesním modelem výroby a neuvažuje selhání bezpečnostních prvků, tj. ochranných bariér, což přes všechna dosud aplikovaná opatření vede k realizaci zdrojů rizik, které mohou mít extrémní dopady.

Kromě toho mnoho příkladů ukazuje, že řada expertů je postižena provozní slepotou, je uchlácholena splněním požadavků norem a standardů a nevidí rizika spojená s různými vazbami a spřaženími s okolím. Například jednoduché srovnání intervalů používaných v pravděpodobnostních hodnoceních ukazuje, že: interval $(\mu-\sigma, \mu+\sigma)$ pokrývá 68,5 % případů; interval $(\mu-2\sigma, \mu+2\sigma)$ pokrývá 85.4 % případů; a interval $(\mu-3\sigma, \mu+3\sigma)$ pokrývá 99,8 % případů [17], kde μ je medián a σ standardní odchylka.

Konkrétní technická opatření, jako je výběr materiálů pro výrobní zařízení, specifické konstrukce, zálohování, ochranné systémy apod. jsou předmětem technických norem, standardů, a nebudou zde uváděny.

5.5.2. Organizační opatření

Systém řízení bezpečnosti pak musí být založen na dobré kultuře bezpečnosti, tj. na dobré úrovni systematicky prováděných lidských opatření. V práci [102] autoři ukazují tři hlavní příčiny havárií a selhání technologií. První příčinou jsou lidské chyby mající původ ve špatné komunikaci a spolupráci zúčastněných. Druhou příčinou je nereagování na situaci mající původ v selhání zařízení a v nedostatečné reakci zúčastněných na vzniklou situaci. Třetí příčinou je přijatelnost vysokého rizika a nedostatečné povědomí o dopadech (tj. škodách a ztrátách na aktivech), které s ním souvisí. Autoři citované práce ukazují, že máme řadu nástrojů pro identifikaci a analýzu pohrom a havárií, a přesto se tyto vyskytují. K jejich výskytu přispívají:

- neadekvátní standardy a postupy,
- nedostatek zdrojů,
- chybné audity a revize,
- práce pod tlakem,
- velké pracovní zatížení,
- resty,
- nedostatek kompetence,
- nepřiměřený projekt výrobního procesu,
- neadekvátní monitoring a opravy,
- příliš velká orientace technického díla na výkon,
- nejasné role a odpovědnosti,
- neadekvátní řízení,
- nedostatečný dohled.

Představu předmětné situace vytváří model organizační havárie, tzv. Swiss Cheese“ (obrázek 2), kdy za určitých podmínek se projeví propojení nedostatků v řízení bezpečnosti systému a dojde k havárii či selhání. Autoři zdůrazňují, že jedinou obranou proti haváriím a selháním technických děl je rozvíjení situačního povědomí v organizaci u všech jejich členů. Je třeba umět: rozlišovat normální, abnormální a

kritické podmínky; a rozpoznat, když dochází k rozhraním mezi uvedenými podmínkami, a správně a včas reagovat na změny podmínek. Předmětní autoři používají označení pro tento postup „pravidlo tří“.

Obrana bezpečnosti technického díla vyžaduje znát nebezpečné podmínky a realizovat jak proaktivní opatření ke snížení jejich výskytu, tak mít připraveny adekvátní reakce. Bezpečnost organizace je výsledkem toho, jak jednotlivci i organizace rozumí rizikům a jak s nimi nakládají.

Autoři rozlišují pět typů organizací podle způsobu práce s riziky:

1. Nakládání s riziky v organizaci je patologické, když v organizaci chybí systém, jak s nimi vyjednávat.
2. Reaktivní nakládání s riziky provádí organizace, které mají systém odezvy na rizika, která se v organizaci již vyskytla.
3. Formální řízení rizik mají organizace, které berou v úvahu i rizika, která se ještě u nich nevyskytla, ale jsou možná.
4. Proaktivní řízení rizik mají organizace, které provádí nejen formální řízení rizik, ale přihlíží i k místním podmínkám.
5. Generativní způsob práce s riziky je proaktivní řízení rizik, které zvažuje možná vzájemná propojení v čase. Vždy je důležité stanovení toho, co je třeba v dané situaci provést a odpovědnost za provedení, tj. plán řízení rizik; a to na úrovni konkrétních pracovníků, liniového managementu a senior managementu.

Organizační opatření pro zajištění a zvyšování bezpečnosti technických děl zajišťují plány, které již byly zmíněny výše. Zásadní organizační opatření pro oblast zvládání rizik, která patří mezi prioritní rizika, obsahují plány řízení rizik [4].

Řízení rizik je nedílnou součástí vnitřního řídícího a kontrolního systému každé entity i každé činnosti. Čím je výrobní technologie složitější, tím podrobnější informace jsou potřebné pro zajištění bezpečnosti. Pan Fawcett v práci [103] prohlásil „Vědět znamená přežít, ignorovat znamená říkat si o zničení“. Ignorování či podceňování řízení rizik je důvodem většiny problémů, nezdarů, katastrof, a proto je důležité mít vždy předem připravený nástroj, jak zvládnout očekávaná rizika, k čemuž slouží plán řízení rizik, a dokonce, co udělat v případě neočekávaných rizik, k čemuž slouží plány pro zvládnutí nečekaných situací (contingency plans) [1,3,17].

Plán řízení rizik se opírá o způsob řízení TQM [56], tj. zvažují se prioritní rizika, která nebylo možno vypořádat, a při realizaci mají potenciál významně poškodit technické dílo. Samotný plán se zpracovává ve formě tabulky, která zvažuje rizika z oblastí:

- řízení technického díla,
- vnitřní zdroje rizik technického díla spojené s jeho stavbou, konstrukcí, zařízeními a provozem,
- personál technického díla,
- vnější zdroje rizik technického díla spojené s živelními pohromami,
- vnější zdroje rizik technického díla spojené s chováním veřejné správy, konkurencí, trhem apod.,
- útoky na technické dílo,
- kybernetické zdroje rizik spojené se sítěmi,
- válka.

Pro každou oblast rizika se v tabulce uvádí:

- příčiny rizika,
- pravděpodobnost výskytu realizace rizika a dopady rizika,
- opatření na zvládnutí nebo alespoň zmírnění rizika, které jsou jasně stanoveny, a u každého z nich je uvedena odpovědnost za jejich provedení.

Příklad plánu z oblasti řízení letového provozu je v tabulce 26, převzaté z práce [104].

Tabulka 26. Příklad plánu řízení rizik pro letadlo. Použité zkratky: IATA = International Air Transport Association; NTSB = National Transportation Safety Board; ŘLP = Řízení letového provozu; SAS = Skybrary Aviation Safety. Citace dokumentů, uvedených ve čtvrtém sloupci jsou v práci [104], neuvádíme je proto, že patří do jiné odborné oblasti, než je práce s riziky.

Oblast rizika	**Popis příčin rizika**	**Pravděpodobnost výskytu a dopady rizika**	**Opatření pro zmírnění rizika a odpovědnosti**
Organizační	Ztráta orientace	*Pravděpodobnost:* malá *Dopady:* velké	*Opatření:* použití náhradních tzpůsobů orientace - dle reliéfu terému a požádání o pomoc řízení letového provozu (NTSB 2010) *Odpovědnost:* pilot (NTSB 2010)
	Chybné vyhodnocení situace	*Pravděpodobnost*: střední *Dopady*: velké	*Opatření:* provedení opravného manévru (NTSB 2000) Odpovědnost: pilot (NTSB 2000)
	Špatná spolupráce posádky	*Pravděpodobnost:* malá *Dopady:* střední	*Opatření:* okamžité zavedení pořádku a později změna posádky (NTSB 2000) *Odpovědnost:* velitel letadla (NTSB 2000)
	Nezvladatelný cestující	*Pravděpodobnost:střední* *Dopady:* střední	*Opatření:* pohovor, přikurtování k sedadlu, popř. oddělení od ostatních, přistání na vhodném letišti (IATA 2016) *Odpovědnost:* velitel letadla (IATA 2016)
Technické	Výpadek motoru	*Pravděpodobnost:* malá *Dopady:* střední	*Opatření:* zahájit nouzové klesání a vyslání zprávy na řízení letového provozu (Mika 2016, SAS 2009, 2014) *Odpovědnost:* pilot „letící" (Mika 2016, SAS 2009, 2014)
	Nefunkční výškoměr	*Pravděpodobnost:* malá *Dopady:* střední	*Opatření:* použití záložních systémů určení polohy (SAS 2009) *Odpovědnost:* pilot (SAS 2009)
	Úbytek kyslíku na palubě	*Pravděpodobnost:* malá *Dopady:* vysoká	*Opatření:*spuštění kyslíhových masek, vyslání zpráva na řízení letového provozu (SAS 2005) *Odpovědnost:* pilot (SAS 2005)
Narušení bezpečnosti z vnitřních	Požár v kabině	*Pravděpodobnost: malá* *Dopady:* velmi vysoké	*Opatření:* použití hasících přístrojů na palubě , vyslání zprávy na řízení letového provozu, snaha o rychlé přistání (ŘLP 2016) *Odpovědnost:* velitel letadla (ŘLP 2016)

	Požár v zavazadlovém prostoru	*Pravděpodobnost:*lmalá *Dopady:* velmí vysoké	*Opatření:* nouzové přistání na nejbližším vhodném letišti (NTSB 2010) *Odpovědnost:* velitel letadla (NTSB 2010)
Narušení bezpečnosti z vnějších příčin	Velké propadnutí letounu	*Pravděpodobnost:* malá *Dopady:* střední	*Opatření:* opravný zásah v řízení letadla(NTSB 2004) *Odpovědnost:* pilot „letící" (NTSB 2004)
	Velký elektrický výboj	*Pravděpodobnost:* malá *Dopady:* vysoké	*Opatření:* okamžité převzetí manuálního řízení (ŘLP 2016) *Odpovědnost:* pilot (ŘLP 2016)
	Útok cizího letadla	*Pravděpodobnost:* malá *Dopady:* velmi vysoké	*Opatření:* nouzové přistání na nejbližším vhodném letišti (DSB 2014) *Odpovědnost:* pilot „letící" (DSB 2014)
Kybernetické	Ztráta spojení	*Pravděpodobnost:* střední *Dopady:* střední	*Opatření:* nastavení nouzového kódu odpovídače letadla (ŘLP 2014, 2015) *Odpovědnost:* pilot „letící" (ŘLP 2014, 2015)
	Hackerský útok na systém řízení letadla	*Pravděpodobnost:* malá *Dopady:* velmi vysoké	*Opatření:* aplikace manuálního řízení (IATA 2016) *Odpovědnost:* pilot „letící" (IATA 2016)
	Podivné hlášení – neobvyklá aktivace senzorů	*Pravděpodobnost:* malá *Dopady:* velmi vysoké	*Opatření:* prověření varovných sstémů, vyslání zpráva na řízení letového provozu (SAS 2014) *Odpovědnost:* velitel letadla (SAS 2014)

Pro sestavení plánu řízení rizik, který odpovídá nárokům řízení vyžadovaným TQM, je potřeba důkladně znát: pohromy, tj. zdroje rizik; místní zranitelnosti, které předurčují krutost (kritičnost, závažnost) kritických situací; a možnosti odezvy za kritických situací.

Protože bylo ukázáno, že rizika jsou spojená i se samotnou prací s riziky, tak byl vypracován a v praxi otestován kontrolní seznam (tabulka 27) pro posuzování kritičnosti plánu řízení rizik; přičemž při posuzování jednotlivých položek byl použit princip „čím vyšší, tím horší" podle teorie [65] a stupnice:

0 bodu – naplnění kritéria má zanedbatelné nedostatky ve sledované oblasti (nižší než 5 %), tj. má zanedbatelnou kritičnost,

1 bod - naplnění kritéria má nízké nedostatky ve sledované oblasti (5-25 %), tj. má nízkou kritičnost,

2 body - naplnění kritéria má střední nedostatky ve sledované oblasti (25-45 %), tj. má střední kritičnost,

3 body - naplnění kritéria má vysoké nedostatky ve sledované oblasti (45-70 %), tj. má vysokou kritičnost,

4 body - naplnění kritéria má velmi vysoké nedostatky ve sledované oblasti (70-95 %), tj. má velmi vysokou kritičnost,

5 bodů - naplnění kritéria má extrémně vysoké nedostatky ve sledované oblasti (vyšší než 95 %), tj. má extrémně vysokou kritičnost.

Tabulka 27. Kontrolní seznam pro posuzování plánu řízení rizik.

Otázka	**Hodnocení**
Je plán pro zvládnutí rizik veden jasnou představou a sledovanými cíli?	
Uplatňuje se v plánu pro zvládnutí rizik princip celistvosti (tj. uvážení prosperity sociálního, ekologického a ekonomického subsystému; vyjádření nákladů a užitků; dopadů a přínosů ekonomické aktivity pomocí peněžních i nepeněžních hodnot)?	
Jsou v plánu pro zvládnutí rizik zváženy podstatné elementy (např. spravedlivá dělba využívání zdrojů mezi současnou generací a generacemi budoucími; nadměrná spotřeba a chudoba; lidská práva; ekologické poměry podmiňující život; prosperita umožněná ekonomickým rozvojem a mimotržními činnostmi)?	
Má plán pro zvládnutí rizik přiměřený rozsah (např. vhodné měřítko času a prostoru)?	
Je plán pro zvládnutí rizik prakticky zaměřen (např. explicitně definované kategorie, které spojují vytyčenou představu s indikátory a kritérii; omezený počet klíčových cílů; omezený počet indikátorů; standardizovaný způsob měření a porovnávání; referenční hodnoty indikátorů, prahové hodnoty, vývojové trendy)?	
Je plán pro zvládnutí rizik otevřený (např. všeobecně přijaté metody a databáze; explicitní věrohodnost, vyloučení nejistoty)?	
Je v plánu pro zvládnutí rizik zahrnuta efektivní komunikace v zájmové společnosti?	
Podílí se na plánu pro zvládnutí rizik široká veřejnost?	
Počítá se v plánu pro zvládnutí rizik s následným posuzováním (např. upřesňování postupných cílů vlivem vývoje systému)?	
Jsou v plánu pro zvládnutí rizik zabezpečeny kapacity institucí (např. určení odpovědnosti za dodržení cílů rozhodovacího procesu, sběr a uchovávání údajů, dokumentace)?	
CELKEM	

Stupnice pro celkovou kritičnost plánu řízení rizik se jako v dříve uvedených případech určuje analogicky k principům používaným od 80. let v normách ČSN. Výsledná míra kritičnosti za předpokladu, že všechna kritéria mají stejnou váhu, může nabýt hodnot 0 až 50; prahové hodnoty pro míru kritičnosti plánu pro řízení rizik, odpovídající použité stupnici jsou uvedené v tabulce 28, která platí pro míru rizika.

Tabulka 28. Stupnice pro určení míry kritičnosti plánu pro řízení rizik.

Stupeň kritičnosti plánu pro řízení rizik	**Kritičnost v %**	**Počet bodů pro stupeň kritičnosti**
Extrémně vysoká – 5	Více než 95 %	Více než 47.5
Velmi vysoká – 4	70 - 95 %	35 – 47.5
Vysoká – 3	45 - 70 %	22.5 – 35

Střední – 2	25 – 45 %	12.5 – 22.5
Nízká – 1	5 – 25 %	2.5 – 12.5
Zanedbatelná – 0	Méně než 5 %	Méně než 2.5

6. VARIANTY PRÁCE S RIZIKY TECHNICKÝCH DĚL POUŽÍVANÉ V PRAXI A JEJICH VALIDITA

Je skutečností, že v současné technické praxi jsou opomíjeny pokrokovější přístupy a postupy práce s riziky zacílené na bezpečnost technických děl. Důvodem jsou: neznalosti nároků na data; nestanovené nároky na metody zpracování dat; nezvažování změn v čase. Náročnost není vyžadována legislativou, ani státním dohledem a dozorem nad technickými díly. Proto v předložené kapitole uvedeme výsledky srovnání modelu řízení a vypořádání rizik technických děl, který je nastíněn v předchozích kapitolách a údajů zjištěných v praxi, z odborných publikací, zpráv o haváriích a selháních technických děl, specifického výzkumu a zkušeností autorky.

6.1. Souhrnná charakteristika normativu určujícího bezpečné technické dílo

Bezpečnost technických děl je vyžadovanou vlastností od lidské společnosti. Je skutečností, že ji narušuje mnoho známých rizik a také mnoho nově poznávaných rizik, která souvisí se stále rostoucí složitostí technických děl i celého světa. Na základě současných znalostí shrnutých v pracích [1-4,10-39], jež jsou shrnuté v pracích [3,4], chápeme každé technické dílo jako otevřený složitý systém systémů, tj. jako několik otevřených systémů, které se vzájemně prolínají, a jsou propojené s okolím. Propojení zajišťují plnění důležitých úkonů a zároveň způsobují závislosti, které jsou příčinami specifických zranitelností. Za jistých podmínek vznikají propojení vysoce nežádoucí, která vedou k selhání technických děl, která za jistých okolností výrazně poškozují i okolí. Proto při zajišťování bezpečnosti technických děl je třeba zvažovat, že technická díla mají rozmanitá aktiva, která se v dynamicky proměnném světě mění. Rozmanitost a proměnnost aktiv způsobuje, že za jistých podmínek jsou požadavky na opatření, která zajišťují bezpečnost jednotlivých aktiv, konfliktní, což znamená, že metody používané k řízení rizik, které je zacílené na bezpečnost technických děl, musí být multikriteriální [4].

V současné době je v pokrokových inženýrských disciplínách ***bezpečnost chápaná jako vlastnost, která vystupuje na úrovni systému*** [3,4,25-34]. Představuje soubor opatření a činností, které zajistí, že systém je bezpečný. Jak již bylo několikrát uvedeno, bezpečnost a riziko spolu jistým způsobem souvisí, ale nejsou komplementární veličiny. Snížení rizika znamená zvýšení bezpečnosti, ale obráceně to neplatí [3,4].

Na základě výše uvedených faktů jsou technická díla složitá, což znamená, že chování celku nelze odvodit z chování jednotlivých částí a za jistých podmínek dochází k výskytu neočekávaných jevů, které vedou ke zničení nebo selhání funkčnosti daného zařízení. Proto se v praxi sledují specifické vlastnosti, jako:

- interoperabilita (tj. schopnost technického zařízení jako celku plnit kvalitně dané úkoly za normálních, abnormálních i kritických podmínek),
- integrita bezpečnosti (SIL), která se většinou sleduje ve spojení s lidskými chybami (při specifikaci, návrhu, instalaci, údržbě, modifikaci apod.),
- kritičnost (tj. míra s jakou může dojít k úrazu osob, zničení materiálu, škodě či jiným ztrátám na aktivech - jde o prahovou hodnotu, pod níž je stav sledovaného

zařízení žádoucí a opačně); kritičnost závisí přímo úměrně na zranitelnosti aktiv [4],
- provozní spolehlivost, která zajišťuje, že systém plní stanovené požadavky a jeho provoz vyhovuje stanoveným podmínkám (rozkládá se na dvě základní vlastnosti, kterými jsou zranitelnost a odolnost) [3,17].

Problémy složitých technických děl, které způsobují neplánovaná a nežádoucí propojení [3,4,17], která jsou důsledkem:
- náhle vynořeného rysu chování, který nelze odvodit ze znalostí o chování komponent (jde o tzv. emergenci),
- hierarchičnosti,
- samo organizovanosti,
- rozmanitých řídících struktur,

což vše dohromady připomíná chaos. Proto při zajištění bezpečnosti složitých technických děl a zařízení je nutný mnoho oborový a mezioborový přístup, kterým se musí zařídit jejich:
- existence (schopnost zajistit rovnováhu),
- efektivnost (schopnost vyrovnat se s nedostatkem zdrojů),
- volnost (schopnost dobře zvládat výzvy z okolí),
- bezpečí (schopnost ochránit se před jevy uvnitř i vně),
- adaptace (schopnost přizpůsobit se vnějším změnám),
- koexistence (schopnost měnit své chování tak, aby chování reagovalo na chování a orientaci dalších systémů a aby je daný systém neohrožoval a ony neohrožovaly jeho).

Z hlediska současného poznání před námi dnes stojí minimálně dva úkoly:
- řešit problém funkčnosti souboru vzájemně propojených (tj. závislých) objektů a infrastruktur za normálních, abnormálních a kritických podmínek,
- vyhledat kritické stavy složitého zařízení, které jsou nepředvídatelné, anebo jsou důsledkem závažné chyby obsluhy, a za jistých podmínek mohou přejít do vysoce nežádoucích, tj. vysoce nepřijatelných stavů, tj. do stavů, ve kterých je ohrožena samotná existence zařízení, anebo dokonce lidí, a které obvykle označujeme jako krizové.

Jak již bylo dříve řečeno, technická díla a zařízení mohou být poškozena vnitřními i vnějšími škodlivými jevy (pohromy), a to včetně chování lidí, kteří je vytváří a provozují. Časté příčiny škod na technickém díle a jeho okolí způsobují tzv. organizační havárie, které spočívají v tom, že se buď se nezváží všechny pohromy, anebo se podcení jejich velikost.

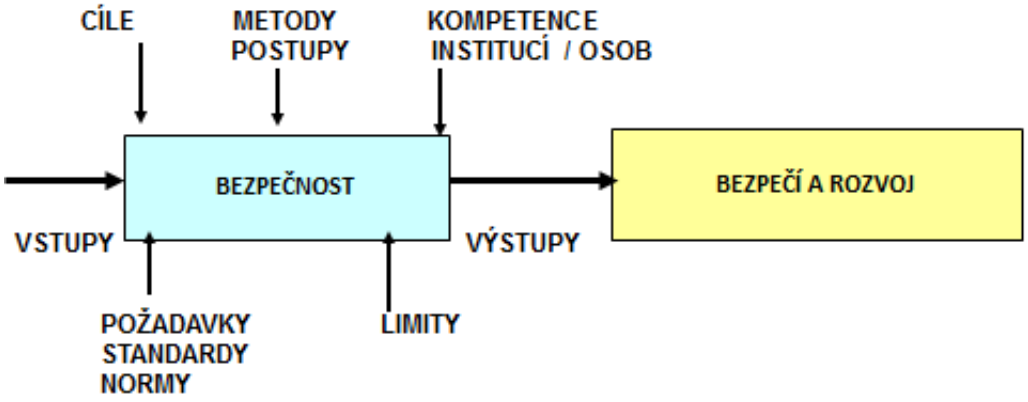
Protože složitá technická díla jsou obvykle vybavena drahou technologií, dochází při odezvě na nouzové situace často ke konfliktu mezi provozními inženýry a bezpečnostními složkami zacílenými na ochranu lidí, protože inženýři jsou vzdělávání i cvičení ke zvládání normálních, abnormálních i kritických podmínek a k respektování ochrany technologií, protože provoz technologií jim poskytuje práci, tj. i obživu. Na základě pro-aktivního přístupu, který je vlastní projektovému a procesnímu řízení, se řešení konfliktů předem připravuje, a to: sestavením plánu pro řízení rizik, který je odsouhlasen předpokládanými zúčastněnými stranami.

Při zajišťování bezpečnosti kritických objektů rozlišujeme v praxi podle cíle práce s riziky dva koncepty, a to řízení rizik a řízení bezpečnosti, přičemž je skutečností, že druhý jmenovaný naplňuje cíle lidí lépe [2,3]. Je to způsobeno tím, že riziko a bezpečnost jsou sice v určitém vztahu, ale nejsou komplementárními veličinami [8],

protože bezpečnost lze zvýšit aniž bychom snížili riziko, např. aplikací varovacích systémů zvýšíme bezpečnost, ale riziko nesnížíme. Komplementární veličinou k bezpečnosti je kritičnost. Kritičnost je chápaná jako mezní stav systému, který je významný pro stabilitu systému [11] a posuzuje se podle:

- možných škod na životech a zdraví lidí. Usuzuje se na ní dle škod možných při haváriích, v jaderných nebo chemických provozech,
- ztráty funkčnosti cílené činnosti, která má jisté poslání (mission). Usuzuje se na ni dle rozsahu postiženého území, např. při selhání navigačního systému,
- ekonomických škod při podnikání. Usuzuje se na ni např. dle ztrát, které způsobí nefunkčnost bank.

Ze systémového hlediska je zajištění bezpečnosti základním požadavkem na systém jako celek, nikoli jen požadavkem na jeho komponenty, a poměrně snadno se dá odvodit systémové schéma řízení bezpečnosti v určité situaci uvedené na obrázku 24. Z obrázku je zřejmé, že tím jaká opatření používáme k zajištění bezpečnosti, tím určujeme výsledek, tj. bezpečí jako stav systému.



Obr. 24. Procesní model vytváření aktuální bezpečnosti, jeho vstupy a výstupy.

Normativ určující bezpečné technické dílo je model technického díla, který respektuje principy All-Hazard-Approach i Defence-In-Depth, má plán na zvyšování bezpečnosti, plány pro řízení rizik, plány odezvy, plány kontinuity a podklady pro plány krizové, aby byly zajištěny kvalitní plány odezvy v okolí technického díla. To znamená, že má všechna rizika zvládnuta na takové úrovni, že jejich realizace neohrozí ani jeho existenci, ani významně nepoškodí jeho okolí. Z pohledu vývoje to znamená, že nepředpokládáme náhlou velkou změnu (skok) podmínek. Při takovéto změně by došlo k extrému, na jehož zvládnutí se dosud nepřipravujeme.

Úkolem vypořádání rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Snižování rizika je vždy spojeno se zvyšováním nákladů. Proto řízení rizika je vedeno snahou najít hranici, na kterou je únosné riziko ještě snížit, aby vynaložené náklady byly společensky přijatelné. Z pohledu praxe je třeba se dohodnout na tom, jaké požadavky bude výstup z hodnocení rizika splňovat. Při hodnocení rizik je nutné se snažit stanovené požadavky dodržovat a případné nedodržení odůvodnit. Jedná se především o splnění požadavků: provedení hodnocení v požadované šíři a kvalitě v souladu s přijatou metodikou hodnocení; úplnost hodnocení; zahrnutí nejnovějších

poznatků vědy; odhad nejistot i neurčitostí v případě použití extrapolací; jednotné vyjádření charakteristik rizika; a průhlednost provedení procesu hodnocení rizik.

Svět je však složitý systém systémů ve vertikální i horizontální rovině, a proto jeho chování je heuristické, tj. je značně proměnné v závislosti na vnitřních a vnějších podmínkách, což znamená, že za určitých situací vznikají neočekávané jevy, které v reálném životě mohou přinést citelné ztráty a škody, protože jsou důsledky jevů, se kterými člověk na základě svých znalostí nepočítá [1,3,4,11,17], protože nejsou detekovatelné stochastickými metodami, které pracují s náhodnými nejistotami. Teprve dnes u zvláště složitých systémů hledáme způsoby, abychom zabránili: atypickým haváriím; kaskádovitým selháním infrastruktur; eskalaci dopadů na chráněná aktiva; nebo nežádoucím propojením v kritických objektech, tj. snažíme se vyrovnat s riziky, jejichž zdroji jsou neurčitosti (tj. znalostní nejistoty). Používáme k tomu multikriteriální přístupy [1,3].

Na základě komplexní analýzy a kritického posouzení několika tisíc odborných prací a výsledků z praxe, jejichž výsledky jsou v pracích [1-4,11,17], je nutné při řešení problémů bezpečnosti kritických objektů použít systémový přístup (tj. zaměřit se na integrální riziko) a nejprve vybrat správný koncept práce s riziky (tj. kontext, v němž rizika sledujeme) a poté respektovat logický model práce s riziky. Klíčové koncepty inženýrství zaměřených na bezpečnost jsou:

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

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

Rizika byla, jsou a budou a neustále se budou objevovat nová. Řízení a vypořádání rizik, které způsobují pohromy, vyžaduje rozměr a měření rizika, které berou v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Většina technik na určování rizika nereprezentuje holistický přístup a nerespektuje, že riziko je rozdělené na lokální, regionální i státní úroveň [3].

Je zřejmé, že nejsme-li schopni riziko identifikovat a analyzovat, nejsme schopni se proti němu účinně bránit. Chyba, které se dopustíme při identifikaci, analýze a hodnocení rizika, se přenáší do nouzových a krizových plánů, do plánů kontinuity a sni-

žuje jejich hodnotu ve vztahu k plánovaným opatřením směřujícím především k ochraně lidských životů a zdraví, ale i v oblasti akceschopnosti záchranných složek podílejících se na realizaci záchranných operací.

Při práci s riziky si je třeba uvědomit, že úkolem řízení rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Základní principy při práci s riziky jsou:

- být proaktivní,
- domýšlet možné důsledky,
- správně určovat priority veřejného zájmu,
- myslet na zvládnutí problémů,
- zvažovat synergie,
- být ostražitý.

V případě, že sledované riziko není přijatelné, tak je třeba zvážit situaci a vybrat některou z dále uvedených činností [2]:

- vyhnutí se riziku (tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika, když to jde – u přírodních pohrom to nejde a mnohdy to nejde ani u technologií, které ještě nejsou plně odzkoušeny v praxi),
- odstranění zdrojů rizik (tj. zabránění vzniku pohrom, když to jde – u přírodních pohrom to nejde a u technologických procesů, např. těch, které pracují s nebezpečnými látkami, to také mnohdy nejde),
- snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom (např. snížením množství nebezpečných chemických látek v podnicích, když to jde – u přírodních pohrom to nejde),
- 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.

U technických děl jde především o snížení pravděpodobnosti výskytu prioritních (kritických) rizik a o snížení závažnosti jejich dopadů.

Proto u strategických řešení problémů technických děl je nutné používat systémové pojetí a integrální riziko, které zohledňuje také znalostní nejistoty. Bezpečnost založená na vypořádání dílčích rizik či integrovaného rizika nezajišťuje dostatečně bezpečné technické dílo. Vzhledem k dynamickému vývoji světa, je třeba prioritní rizika monitorovat a vypořádávat v čase, a také příslušnou bezpečnost měřit.

Při návrhu míry úrovně bezpečnosti jsme použili známou zkušenost, že čím lépe vypořádáme příslušná rizika, tak tím vyšší je bezpečnost entity. Proto pomocí logického uspořádání požadavků jednotlivých technik, používaných při práci s riziky v technickém díle, rozdělených do 7 oblastí, a teorie maximálního užitku [65], jsme sestrojili kontrolní seznam a stupnici pro stanovení úrovně bezpečnosti. Práce [96] ukazuje výsledek aplikace předmětného kontrolního seznamu a předmětné stupnice na 5 běžných technických děl, která nepatří mezi kritické objekty České republiky a mají charakter SME. Souhrnné hodnocení bezpečnosti provedené na základě reálných dat ukazuje střední úroveň bezpečnosti. Z hlediska úrovně poznání je největším nedostatkem v praxi skutečnost, že se stále dostatečně nezvažuje systémová povaha technických děl a dynamika vývoje, a že chybí soustavná spolupráce expertů z různých oblastí, kteří rozhodují o dílčích aspektech technického díla od jeho přípravy až k ukončení jeho životnosti.

Na základě současného poznání shrnutého v pracích [3,4] a v předchozích kapitolách, normativ určující úroveň práce s riziky má sedm položek (obrázek 25), které ovlivňují výsledek práce s riziky technického díla, tj. jeho bezpečnost, a to:

1. Kontext, do kterého jsou zasazena rizika spojená inherentně s technickými díly.
2. Seznam zvlažovaných zdrojů rizik.
3. Typ rizika.
4. Způsoby vypořádání rizik.
5. Procesní model práce s riziky, aplikaci TQM a Coaseho teorému.
6. Techniku řízení a vypořádání rizik technického díla.
7. Způsob řízení rizik v čase.

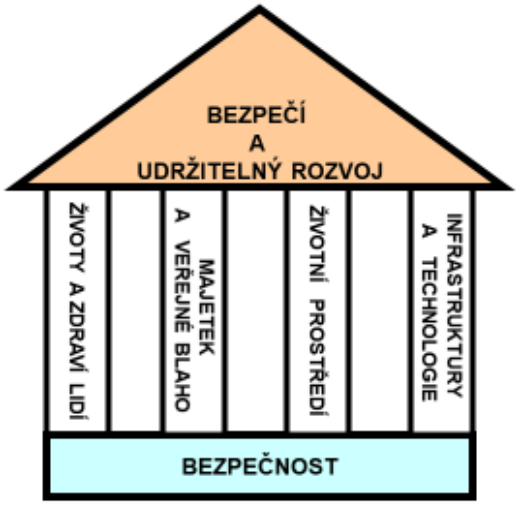
Obr. 25. Položky, které ovlivňují výsledek práce s riziky technického díla.

6.2. Varianty práce s riziky technických děl používané v praxi a výsledky jejich porovnání s normativem

Dále uvedeme postupně varianty, které se u položek uvedených na obrázku 25 používají pro zvládnutí rizik technických děl s cílem zajistit, aby technické dílo bylo bezpečným systémem a abychom přitom znali zanedbání, kterých jsme se dopustili při výběru modelu řešení. Je třeba začít určením kontextu, ve kterém chápeme rizika a pak pokračovat přes postupy jejich identifikace, analýzy, hodnocení, řízení až k postupům jejich vypořádání.

6.2.1. Údaje o variantách práce s riziky používané v praxi

Na základě analýzy údajů v pracích [25-34], šetření, která byla provedená při shromažďování podkladů pro práce [3,4,58], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [63] se v technickém sektoru často zvažuje jen kontext technického díla nebo kontext podniku, který technické dílo spravuje a v řadě případů jen kontext výrobního zařízení. To znamená, že nejobecnější kontext (označovaný jako All-Hazard-Approach [99] a pro Evropu rozpracovaný v [16,18]), který je založen na zvažování technického díla jako součásti lidského systému, který má aktiva a procesní model, jež je znázorněn na obrázku 26, obvykle zvažován není; pouze u vybraných jaderných zařízení a nebezpečných chemických provozů je k uvedeným aktivům přihlíženo integrovaným způsobem [3,4].



Obr. 26. Aktiva lidského systému a procesní model pro zajištění jeho bezpečí [1].

Je pochopitelné, že čím užší kontext při chápání rizik je použit, tím větší jsou zanedbání reálné skutečnosti, což v praxi znamená, že příslušná řešení nezvažují některé zdroje rizik a jejich dopady na všechna veřejná a podniková aktiva; velmi často se dle údajů v [4,63] jedná o:

- vyloučení škodlivých jevů: z okolí sledované entity; a jevů, které jsou vyvolané špatnými rozhodnutími managementu podniku či správních orgánů,
- nezvažování dopadů rizik na lidi, majetek a životní prostředí v okolí technického díla.

Rizika spojená s technickými díly se sledují od 30. let minulého století, nejprve se sledovaly je technické aspekty, které se postupně doplňovaly s růstem poznání a s růstem požadavků na bezpečnost [3,4,17]. V současné době se vyžaduje bezpečný systém systémů, ale ani ten nezajišťuje stoprocentní bezpečnost, jak ukazuje hodnocení, jehož výsledky jsou uvedené v práci [3].

Na základě analýzy údajů v pracích [25-34], šetření, která byla provedená při shromažďování podkladů pro práce [3,4,17], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [64] se v technické praxi používají dále uvedené výběry zdrojů rizik:

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

Z uvedeného vyplývá, že v řadě případů jsou zanedbány mnohé zdroje rizik pro technická díla. Je to způsobeno skutečností, že:
- při stanovení rizik nejsou zvažována všechna veřejná aktiva a všechna aktiva technického díla (tj. není respektován přístup All-Hazard-Approach [1,2,96]), který je velmi náročný na data, metody, znalosti, zkušenosti a dobu provedení,
- je zanedbána systémová podstata technického díla,
- nezvažují se dynamické dopady vnějšího prostředí na technické dílo, které následně ovlivní konkurenceschopnost technického díla a zajištění obslužnosti území v delším časovém intervalu (např. špatné postupy veřejné správy jsou zdrojem rizik pro technické dílo).

Je zřejmé, že velikost rizika pro dané technické dílo závisí mnoha faktorech; velmi na potenciálu škodlivého jevu (velikosti ohrožení) a na zranitelnosti aktiv technického díla. Na základě analýzy údajů v pracích [25-34], šetření, která byla provedená při shromažďování podkladů pro práce [3,4,17], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [63] se v technické praxi určuje velikost ohrožení:
- odhadem na základě historických údajů nebo tabulek v normách,
- inženýrským úsudkem.

Předmětné metody nepostihují fakt, že extrémní pohromy se vyskytují sporadicky a nepravidelně v čase, a proto nezaručují bezpečnost technického díla v dlouhodobém časovém měřítku. Výpočty náročné na data, znalosti a čas na základě teorie extrémních hodnot či baeysovských metod, které dovolují postihnout neurčitosti, se dosud používají jen u kritických jaderných zařízení.

Na základě analýzy údajů v pracích [25-34], šetření, která byla provedená při shromažďování podkladů pro práce [3,4,17], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [63] se se v technické praxi používají rizika dílčí a integrovaná, protože u nich nejsou velké nároky na kvalitu dat a použitých metod;]; nejméně náročné je určení dílčích rizik, a proto se dílčí rizika nejvíce používají, i když jejich vypovídací schopnost s ohledem na celkovou bezpečnost má velká omezení.

Jen u technických děl velké důležitosti (jaderná zařízení, kosmické koráby, vojenská zařízení apod.) se provádí expertně opatření pro zvládnutí integrálního rizika. Je zřejmé, že pro dlouhodobé zajištění bezpečného technického díla je třeba zvažovat integrální riziko. Jelikož ve výše uvedeném vzorci je neznámá ztrátová funkce, tak v pracích [3,4] jsou uvedené postupy používané v praxi.

Dle dnešních požadavků, specifikovaných v předchozích kapitolách, je třeba, aby technické dílo bylo bezpečný systém, tj. aby se zvažovalo vzájemné působení objektů a infrastruktur a území, v němž se technické dílo nachází, tj. synergentní a kumulativní účinky. Podle současného poznání je třeba propojit přístup All-Hazard-Approach a Defence-In-Depth,

Na základě analýzy údajů v pracích [25-34], šetření, která byla provedená při shromažďování podkladů pro práce [3,4,17], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [63] se v technické praxi používají způsoby:

- rizika se určují a vypořádávají až po vytvoření produktu [3]. Předmětný způsob má nebezpečí, že některá závažná rizika, která lze snížit jen specifickými technickými opatřeními v zadání projektu technického díla, již lze snížit jen organizačními opatřeními, která jsou však méně účinná než opatření technická [3,4,17,63] (např. problémy dálnice D8),
- vyjmenovaná rizika se zvažují od začátku projektu technického díla až do jeho odstavení z provozu. Předmětný způsob závisí na požadavcích legislativy, znalostech projektantů, konstruktérů a provozovatele.

Pokrokový přístup, ve kterém se rizika zvažují od začátku projektu technického díla a používá se v praxi ověřená strategie založená na přístupu Defence-In-Depth, je používán korektně jen u nebezpečných jaderných technických zařízení. U jiných technických děl (např. železniční doprava) je používán jen částečně, protože vyžaduje systémové myšlení, mnoha oborové a mezioborové znalosti a zkušenosti [3,4,63].

Důsledné propojení přístupů All-Hazard-Approach a Defence-In-Depth je potřebné pro zajištění integrální bezpečnosti, je zatím snem.

Zajištění bezpečnosti technických děl a všech dalších entit závisí na kvalitě práce s riziky a na disponibilních možnostech jak managementu a personálu technických děl, tak veřejné správy [1,4]. Zvládání rizik v čase a místě vyžaduje znalosti, schopnosti, finanční, materiální, technické a lidské zdroje. Proto se dále zabýváme nejenom samotnou prací s riziky, ale i praktickými postupy, které se používají při rozhodování o vypořádání rizik.

Základní model práce s riziky zacílený na bezpečná technická díla lze popsat procesním modelem, který je na obrázku 15; další modely jsou uvedeny v práci [2], popř. v pracích, které jsou v předmětné práci citovány. Je zřejmé, že nejsme-li schopni riziko identifikovat a analyzovat, tak nejsme schopni se proti němu účinně bránit. Chyba, které se dopustíme při analýze rizika, se přenáší do provozních předpisů, nouzových a krizových plánů, do plánů kontinuity a snižuje jejich hodnotu ve vztahu k plánovaným opatřením směřujícím především k ochraně lidských životů a zdraví, ale i v oblasti akceschopnosti záchranných složek podílejících se na realizaci záchranných operací.

Je si třeba uvědomit, že úkolem řízení rizika je najít optimální způsob, jak zjištěná rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Úkolem inženýrství rizika je pak navržená opatření a činnosti pro vypořádání rizik způsobem stanoveným řízením rizik, dle disponibilních možností a dle podmínek v místě řešení realizovat a zajistit jejich spolehlivost a funkčnost. Snižování rizika je prakticky vždy spojeno se zvyšováním nákladů a s nároky na znalosti. Řízení rizika je tedy vedeno snahou najít hranici, na kterou je únosné riziko ještě snížit, aby vynaložené náklady byly společensky přijatelné.

Důležitou roli v práci s riziky hraje jak hodnocení rizika, tak posouzení rizika. Dle požadavků uvedených v pracích [2,8,9] u hodnocení jde o splnění požadavků: provedení hodnocení v požadované šíři a kvalitě v souladu s přijatou metodikou hodnocení; úplnost hodnocení; zahrnutí nejnovějších poznatků vědy; odhad nejistot v případě použití extrapolací; jednotné vyjádření charakteristik rizika; a průhlednost provedení procesu hodnocení rizik.

U posouzení rizika jde o správné ocenění přijatelnosti rizika a o volbu správné reakce na riziko. Přijatelnost rizika je ve skutečnosti výsledkem porovnávání několika typů přijatelnosti – technická přijatelnost (spolehlivost a složitost technologií, strojů a zařízení), ekonomická přijatelnost (náklady) a socio-politická přijatelnost (vnímání rizik) [2-4,17]. K posouzení rizika se v praxi používá nejčastěji matice rizika ve tvaru na obrázku 27.

		Kategorie závažnosti dopadů nehod				
		5	4	3	2	1
Kategorie závažnosti četností výskytu nehod	A					
	B					
	C					
	D					
	E					

Obr. 27. Matice rizika; plocha: bílá – přijatelné riziko; světle šedá – tolerovatelné riziko s využitím ALARP; tmavě šedá – podmíněně přijatelné riziko (vyžaduje připravené postupy a opatření pro odezvu; černá – nepřijatelné riziko (vyžaduje okamžitá preventivní a zmírňující opatření).

V souladu s veřejným zájmem je třeba, aby přijatelnost rizika měla sociální rozměr. Proto je třeba zvažovat:

1. Pro koho má být riziko přijatelné?; pro původce rizika, pro politiky nebo pro veřejnou správu?
2. Kdo stanoví přijatelnost?; politici rozhodují o tom, co je zákonné, a tudíž by neměli rozhodovat o tom, co je přijatelné,
3. Zda při stanovení přijatelnosti rizik byla diskutována aktuálně tolerovatelná rizika, netolerovatelné prahové hodnoty a postoje veřejnosti k rizikům.

Protože rizika jsou inherentní součástí lidského systému i každého jeho podsystému, řízení rizika vyžaduje používat rozměr a měření rizika, které berou v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory.

Řada současných technik na určování rizika nereprezentuje holistický přístup a většina z nich nezvažuje vazby a toky mezi prvky systému za zranitelné položky, které zvyšují škody, ztráty a újmy. Často se při alokací úkolů spojených s vypořádáním rizika zapomíná na skutečnost, že zvládání rizik spojených s technickým dílem je rozdělené na všechny úrovně řízení technického díla a také na lokální, regionální i státní úroveň veřejné správy [2,4].

Pro správce a provozovatele technických děl se jeví vhodná kategorizace přijatelnosti rizik, kterou používá OSN; její popis je v práci [1]. Na závěr je třeba připomenout, že ignorování či podceňování řízení rizik je důvodem většiny problémů lidské společnosti.

V našich podmínkách se používají ISO normy třídy 9000, 14000 apod., ve kterých je zakotven typ řízení Total Quality Management (TQM) [56], který spočívá na požadavku, že na procesu zlepšování kvality entity se podílí všichni zaměstnanci, od řadových zaměstnanců až po nejvyšší řídící pracovníky entity. Proces zlepšování jakosti (tj. v jeho nejvyšší úrovni jde de facto o zvyšování integrální bezpečnosti) vychází z impulsů, které vychází z potřeb zákazníka / občana.

TQM vychází z předpokladu, že trvalá kvalita (jakost) 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]; de facto jde o jistou kulturu bezpečnosti (jinými slovy způsob aplikace opatření a činností lidí). Pozornost se zaměřuje na procesy probíhající v entitě. Při implementaci TQM se přihlíží na specifika entity, protože z důvodu účinnosti všechna opatření musí odpovídat struktuře entity, tj. musí být místně specifická.

Výstupy z procesu řízení rizik pro potřeby správného řízení podle TQM jsou:

1. *Seznam vyhodnocených rizik* (risk assessment document) - zde se zaznamenávají veškeré informace o příslušném riziku.
2. *Seznam rizik vyžadujících nejvyšší pozornost* (top risks list) - obsahuje seznam vybraných rizik, jejichž řešení má nejvyšší nároky na zdroje a čas.
3. *Seznam neaktuálních / vyřešených rizik* (retired risk list) - slouží jako historický odkaz pro budoucí rozhodování**.**

Technika samotného řízení rizik z důvodu hospodárného nakládání se silami, zdroji a prostředky před každou fází práce s riziky formálně přezkoumává řízení a vypořádání rizik v kontextu přínosů a nákladů na výstupy. Coaseho teorém [95] se používá pro stanovení ekonomického optima v nákladech na vypořádání rizik.

Na základě analýzy údajů v pracích [25-34], šetření, která byla provedená při shromažďování podkladů pro práce [3,4,17], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [63] se v technické praxi z důvodu neznalosti nepoužívá ani rozdělení rizik do kategorií, jak navrhuje TQM, ani hospodárné využívání nákladů podle Coaseho teorému vyznačeného na obrázku 18.

Další problém při práci s riziky technických děl vzniká v důsledku tradičního oddělování zdrojů rizik na rizika spojená s člověkem a rizika jiná. Vyvinuly se dvě oddělené disciplíny [4], a to řízení a inženýrství na vytváření:
- zabezpečených technických děl,
- bezpečných technických děl.

Oba typy pracují s riziky a spoléhají na princip ochrana do hloubky (Defence-In-Depth), požadují řízení pomocí systému řízení bezpečnosti technického zařízení jako celku (SMS) [4]. Na základě analýz v citované práci dochází k tomu, že když se aplikují odděleně, tak vznikají zmatky ve stanovení priorit, což vede k existenci konfliktů a je nutno provádět optimalizaci opatření. Nesprávně stanovené priority přináší škody, např. v důkladně zabezpečeném objektu uhořeli lidé, protože při požáru nemohli objekt opustit; pilot Andreas z Germanwings mohl navést letadlo do horského masívu Alp, protože pancéřové dveře nešly zvenku otevřít aj.). Proto je východiskem použití konceptu integrální bezpečnosti, který vychází ze zvažování všech jevů, které mohou území i technologické zařízení poškodit (tzv. přístup All-Hazard-Approach), který oba typy řízení a inženýrství inherentně propojuje [4].

Z výše uvedených údajů je zřejmé, že řízení a vypořádání rizik technického díla není úkolem jednotlivce, ani úkolem jedné organizace či jednoho sektoru (obr. 15-17). Jde o kolektivní zacílené úsilí všech zúčastněných. Z obrázků 15 a 16 vyplývá, že:
- stanovit riziko mohou odborníci, kteří mají znalosti, data a schopnost aplikovat vhodné metody,
- rozhodnout o riziku mohou jen ti, co mají příslušné oprávnění (tj. právně určený subjekt veřejné správy nebo v případě objektu (tj. technického díla) právně určený subjekt podniku, jemuž entita patří,
- řízení a zmírňování, tj. vlastní aplikace opatření a činností vedoucí ke zvládnutí rizika mohou jen odborníci, kteří mají příslušné znalosti, schopnosti, vybavení, zdroje a prostředky.

Veřejnost je platným účastníkem při vypořádání rizik, protože jde o její bezpečí a kvalitu života. Protože zdrojů rizik je zpravidla více a opatření na jejich zvládnutí jsou často konfliktní, je třeba použít řízení rizika zacílené na bezpečnost, tj. tzv. řízení bezpečnosti [2].

Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá v rozdělení opatření a činností na vypořádání rizik do kategorií, ve kterých se příslušná část rizika zajistí tak, že:
- preventivními opatřeními se sníží nebo odvrátí realizace rizika,
- účelovými preventivními (zmírňujícími) opatřeními odezvy a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se zmírní dopady, tj. sníží se nebo se odvrátí nepřijatelné dopady při realizaci rizika,
- pojištěním se pokryje část možných ztrát a škod při realizaci rizika,
- vytvořením rezervy na odezvu a obnovu a záloh se zajistí přežití lidí, kontinuitu provozu technického díla, objektu a území,

- přípravou plánu pro odezvu na nepředvídané situace (Contingency Plan) se zajistí provedení reakce na realizaci rizik neřiditelných nebo příliš nákladných, anebo málo častých.

K tomu se rovněž připojuje rozdělení zvládání rizik mezi všechny zúčastněné [2-4]. Rozdělení provedení konkrétních opatření a činností ve správném řízení se provádí tak, že se vychází z toho, že za zvládání rizik odpovídají všichni zúčastnění a že zvládání konkrétního rizika je nejlépe přidělit tomu subjektu, který je na to nejlépe připraven [2]. Je zřejmé, že toto je však možné jen v organizaci, ve které je kvalifikované projektové a procesní řízení, tj. činnosti a opatření se aplikují na základě znalostí, a to věcných i z oblasti řízení (tj. činnosti jsou vzájemně provázané, nejsou chyby v komunikaci, každý zúčastněný ví, co má dělat a jak to má dělat) [2].

Na základě šetření, která byla provedená při shromažďování podkladů pro práce [3,4,17], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [62] v technické praxi platí:

- při výběru zdrojů rizik, jejich analýze a hodnocení se nepožaduje použití kvalifikovaných dat a kvalifikovaných metod zpracování,
- neberou se v úvahu všechny zdroje rizik v daném území,
- provádí se jen rychlé a méně přesné analýzy rizik,
- hodnocení rizik technických děl, která jsou spojená se strategickými cíli a operacemi obvykle nezahrnují všechny důležité faktory: externí a interní; sociálně – politické; technické a ekonomické,
- při posuzování rizik technických děl managementem technického díla (i veřejnou správou při udělování důležitých rozhodnutí) se často některá rizika zanedbávají. Jde např. o sociálně – politická rizika jsou obtížně kvantifikovatelná, např. politická stabilita, dopad teroristického útoku apod. Často se interní sociálně – politické faktory odlišují od externích (viz názor české a rakouské veřejnosti na jadernou elektrárnu Temelín). V dosavadní praxi se při jejich sledování nepoužívá:
  - sociologický přístup, který spočívá v tom, že se vytváří popis povahy rizika z pohledu sociálních skupin a vztahů se zaměřením na ekologická a sociální rizika a na aktivizaci veřejného mínění,
  - politická analýza, která tato rizika hodnotí pragmaticky a hledá jejich ekonomické dopady,
  - analýza rozložení rizik ve společnosti, která spočívá v identifikaci původce (zdroje) rizika, způsobu „šíření“ (realizace) rizika a „spotřebitele“ (skupiny lidí, která je postižena ***dopady r***ealizace) rizika.
- při řízení rizik se často neprosazuje prevence, tj. snížení zranitelnosti technického díla, a tím i snížení jeho rizik, a spoléhá se jen na odezvu,
- neprovádí se pravidelné hodnocení rizik a sledování jejich aktuálnosti; prosadit změny specifických úprav určité činnosti; a revidovat adekvátnost hodnocení rizik,
- nezajišťují se odpovídající zdroje, síly a prostředky pro kvalifikovanou odezvu na havárie a selhání,
- nezajišťují se odpovídající zdroje, síly a prostředky pro kvalifikovanou obnovu (dokonce jen výjimečně existují plány kontinuity pro důležité části technického díla).

Technické dílo i jeho okolí se dynamicky vyvíjí, a proto je třeba, aby se technické dílo systematicky přizpůsobovalo změnám. Na základě současného poznání, shrnutého v pracích [2,14,17,47,48], systém řízení bezpečnosti (tzv. SMS – Safety Management System) komplexního objektu v čase je postaven na zásadách procesního řízení a zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje

pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v území. Zpravidla se týká řady otázek, kromě jiného i organizace, pracovníků, identifikace a hodnocení ohrožení a z nich plynoucích rizik, řízení chodu organizace, řízení změn v organizaci, nouzového a krizového plánování, monitorování bezpečnosti, auditů a přezkoumávání [1,14,47]. Jak bylo uvedeno v odstavci 4.6.5 a na obrázku 20, ***systém řízení bezpečnosti se skládá z šesti procesů.*** Na základě skutečnosti, že v čase dochází ke změnám, které jsou pro technické dílo příznivé i nepříznivé, je třeba sledovat vývoj v čase.

Na základě analýzy údajů v pracích [25-34], šetření, která byla provedená při shromažďování podkladů pro práce [3,4,17], údajů z odborných prací, které jsou citované v pracích [1-4,17] a zkušeností získaných přímo z šetření v praxi [62], se v technické praxi:

- nezvažují rizika, která mohou vyústit v organizační havárii; např. se předpokládá, že celková koncepce bezpečnosti je perfektní, tj. bez chyb,
- systém řízení bezpečnosti neobsahuje pravidelná hodnocení cílů bezpečnosti v technickém díle,
- jen u jaderných zařízení nejvyšší kategorie nebezpečnosti provádí systematický monitoring stavu technického díla v čase,
- jsou prováděny změny, aniž by se uvažovalo o tom, že mohou ovlivnit bezpečnost technického díla,
- není posuzována bezpečnost v souvislosti s chováním kontraktorů v technickém díle,
- je slepá důvěra v platnost standardů a norem, tj. počítá se pouze s provozními podmínkami, pro které platí standardy, tj. nepřipouští se jejich změny v důsledku vnějších pohrom nebo lidských chyb,
- zanedbává se údržba technických zařízení a nedbá se na bezpečnost technického díla jako celku,
- chybí konkrétní postupy pro zvládání havárií a selhání a příslušný odborný personál pro odezvu,
- nevyhodnocují se skoro nehody a často ani větší poruchy a havárie,
- opatření přijatá po haváriích jsou často jen slohová cvičení.

6.2.2. Výsledky srovnání variant požívaných v praxi s normativem

Údaje uvedené v předchozím odstavci ukazují, že požadavky normativu jsou splněny jen v zásadních aspektech; tj. obvykle se zanedbávají některá významná fakta, která patří do současného poznání bezpečnosti technických děl. Pro zjištění míry zanedbání byl proveden specifický výzkum, jehož výsledky jsou v práci [96].

Pomocí kontrolního seznamu v tabulce 20 a hodnotové stupnice v tabulce 21 byl proveden bezpečnostním audit [2,9] v pěti běžných technických dílech, která nepatří mezi kritické objekty České republiky; mají charakter SME (malý a střední podnik - Small and Medium Enterprise); konkrétně: chemický podnik, strojírenský podnik, tepelná elektrárna, letiště, dálnice [63]. Při auditu odpověď na každou otázku vypracovalo samostatně 5 hodnotitelů (technický ředitel, bezpečnostní expert technického díla, bezpečnostní expert místní veřejné správy, bezpečnostní expert regionální správy, autor) dle dokumentace technického díla a výsledné hodnocení byl stanoven jako medián z údajů hodnotitelů. V případě významných pochybností při hodnocení konkrétní otázky byla učiněna poznámka ve vyhrazeném sloupci kontrolního sezna-

mu, a výsledky šetření v těchto případech byly nakonec získány na základě panelové diskuse hodnotitelů.

Přístup k podnikové dokumentaci byl podmíněn tím, že konkrétní údaje o technickém díle nebudou zveřejněny. Proto je uveden jen konečný výsledek v dále uvedeném tvaru:

1. Počet hodnocení „ANO“ se pohyboval mezi 20 – 29; střední hodnota (medián) je 24.
2. Nejvýše dosažená validita techniky práce s riziky:
   - jsou sledována jen aktiva technického díla,
   - jsou sledovány pouze zdroje rizik, které se nachází v technickém díle a lidský faktor spojený se špatně provedenými pracovními úkony,
   - jsou zvažována dílčí rizika a většinou i integrované riziko spojené s BOZP,
   - rizika jsou sledována až po výstavbě technického díla,
   - při práci s riziky technického díla je systematicky použit procesní model práce s riziky, který má jasně určena kritéria přijatelnosti rizik a ojediněle cíle řízení rizik zohledňující veřejný zájem,
   - jsou prováděna preventivní opatření na snížení nebo odvrácení rizik, a to jen prioritních,
   - je zajištěno pojištění technického díla pro případ realizace známých rizik,
   - jsou upřednostněny výsledky standardních, rychlých a méně přesných analýz rizik před výsledky předběžných analýz rizik,
   - při práci s riziky jsou stanovena kritéria jen pro hodnocení technické a ekonomické,
   - jsou stanoveny a aplikovány požadavky, standardy a normy pro zajištění bezpečnosti,
   - správce technického díla má systém řízení bezpečnosti sestavený na zásadách procesního řízení.

Srovnání počtu hodnocení „ANO“ se stupnicí v tabulce 21 ukazuje, že míra bezpečnosti je u běžných technických děl střední. Posouzení úrovně dosažených validit technik práce s riziky [96] ukazuje, že v praxi chybí systémový přístup a že v běžných technických dílech se respektují pouze požadavky legislativy a vlastní zkušenosti s riziky.

Vedlejším produktem studia dokumentace zmíněných technických děl, a těch dalších v [63] je zjištění, že experti z různých oblastí spojených s technickými díly spolu nespolupracují; důkazem jsou záznamy o řešení konfliktů, které nemusely vzniknout, kdyby experti spolu komunikovali.

Uvedený příklad potvrzuje, že tam, kde jde o zajištění bezpečných technických děl, tam je třeba používat techniky pro práci s riziky, které jsou založené na systémovém pojetí a kritickém hodnocení všech vlivů, které mohou působit na technické dílo dnes i v budoucnosti. Provedené šetření problémů spojených s prací s riziky technických děl ukázalo, že u běžných technických děl je míra bezpečnosti střední. Posouzení validity metod a procedur práce s riziky, které jsou používané v praxi, ukazuje, že dosud v české praxi převládají techniky, které nerespektují systémovou povahu technických děl a dynamiku vývoje. Ze studia dokumentací sledovaných technických děl je zřejmé, že při vytváření jejich bezpečnosti experti z různých oborů pracují odděleně, což pochopitelně nezaručuje ani optimální bezpečnost, ani optimální náklady.

6.3. Standardy a normy pro práci s riziky a jejich validita

Je pravdou, že bez standardů a legislativy bychom byli odsouzení k opakování chyb z minula, ale bez vložení bezpečnosti do jejich vylepšení a schopnosti udržitelně odpovědět na neočekávané události nebudeme připraveni na budoucnost.

6.3.1. Norma ČSN ISO 31000

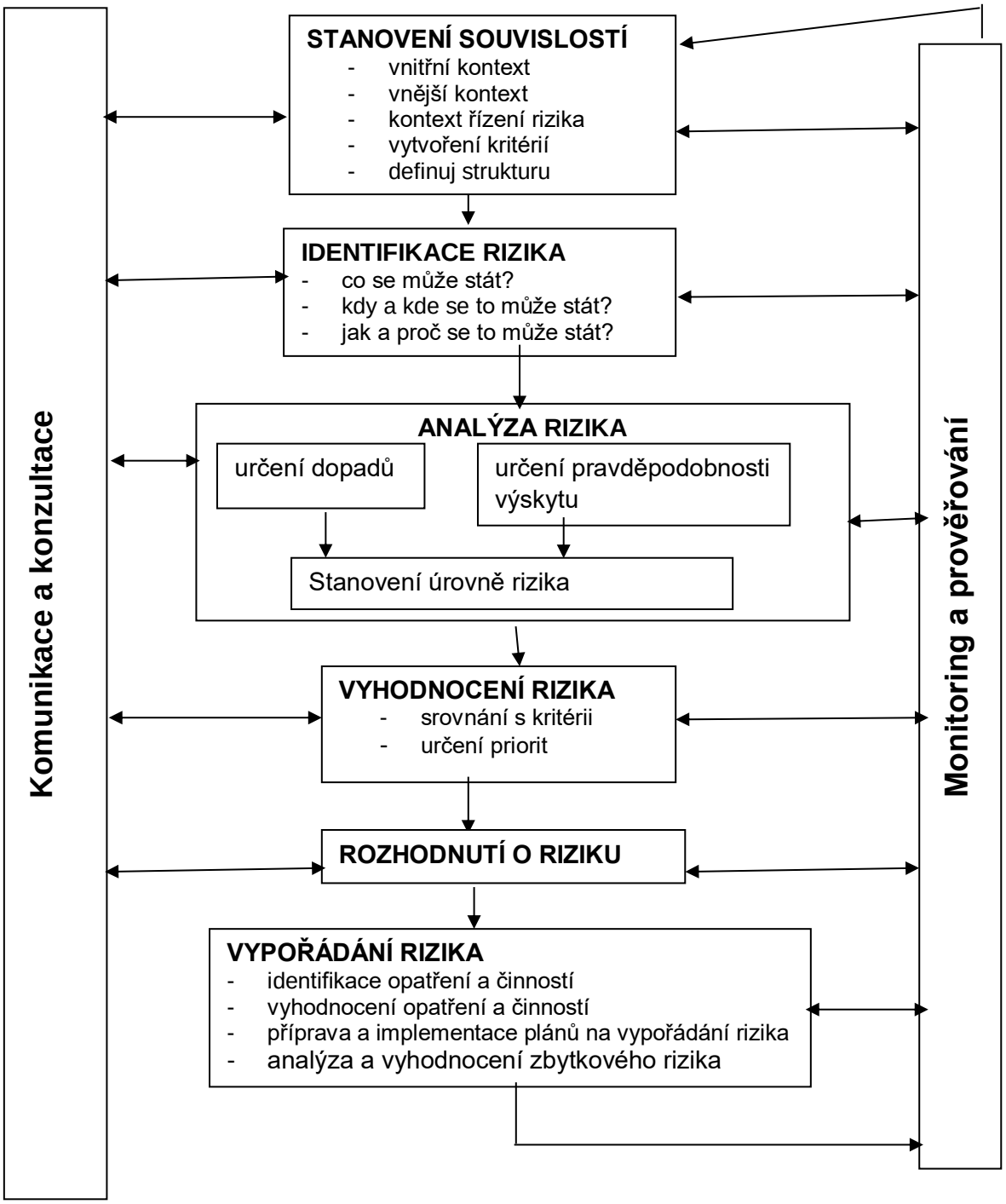
Základní systém pro řízení rizika stanovuje norma ČSN ISO 31000 [7]. Předmětná norma je mezinárodní a stanovuje řadu principů, které je třeba naplnit, aby bylo řízení rizik efektivní. Doporučuje, aby organizace rozvíjely, implementovaly a kontinuálně zlepšovaly rámec, jehož účelem je integrovat proces pro řízení rizik do svého celkového vedení, strategie a plánování, managementu, procesů podávání hlášení, politik, hodnot a kultury. Norma se opírá o projektové a procesní řízení v entitě. Její model je na obrázku 28.

Podle citované normy kvalifikované řízení rizik:

- vytváří hodnoty, protože přispívá k prokazatelnému dosahování cílů jako zlepšení zdraví, bezpečí, kvality životního prostředí, účinnosti procesů a činností atd.,
- je nedílnou součástí procesů, které probíhají v systému, protože za ní odpovídá řídící struktura systému a je nedílnou součástí všech procesů, z nich složených projektů v objektu i řízení změn,
- je součástí rozhodovacích procesů v systému, čímž pomáhá rozhodovat podle důležitosti a rozpoznávat alternativní způsoby řešení problémů,
- je realistické, protože se explicitně zabývá nejistotou i neurčitostí jak v podmínkách, v nichž se systém nachází, tak v procesech, které v objektu i vně probíhají,
- je systematické, uspořádané a včasné, čímž zajišťuje účinnost opatření a činností,
- je založeno na nejlepších dostupných informacích, což zajišťuje aktuální řešení založené na znalostech,
- je přizpůsobené systému, tj. je místně specifické, což zaručuje jak hospodárnost, tak účinnost,
- bere v úvahu lidské a kulturní faktory v systému, což ovlivňuje jeho přijatelnost u zúčastněných,
- je transparentní a komplexní, což zvyšuje jeho spolehlivost,
- je dynamické, opakovatelné a reaguje na změny v systému, což zaručuje jeho aktuálnost a napomáhá neustálému zlepšování a rozvoji systému.

Rámec řízení rizik zahrnuje:

1. Pochopení systému a jeho souvislostí. V oblasti vně systému je třeba sledovat především kulturní, politické, právní, finanční, technologické, ekonomické, přírodní a konkurenční aspekty prostředí. V oblasti vnitřní se jedná především o kvalitu zdrojů a znalostí (např. kapitál, čas, lidé, procesy, systémy a technologie), informační systémy, informační toky a rozhodovací procesy (jak oficiální, tak neoficiální), vnitřní zainteresované strany, hodnoty, kultura a řídící struktura systému..



Obr. 28. Schéma pro řízení rizika [2].

2. Politiku řízení rizik. Politika řízení rizik určuje vazby mezi řízením rizik, cíli systému a dalšími politikami (je upřednostněna nebo je na posledním místě při rozhodování; jak se řeší konflikty; jaké metody řízení se používají; jaké nástroje podporují řízení rizik atd.

3. Integraci výsledků řízení rizik do řídících procesů. Aby řízení rizik bylo efektivní a účinné, musí být obsaženo ve všech směrnicích a realizačních procesech, které v systému probíhají. Patří do strategického plánování a do politiky rozvoje.
4. Stanovení odpovědnosti za opatření a činnosti spojené s řízením rizik.
5. Zdroje nutné pro řízení rizik včetně znalostí, dovedností, zkušeností a kompetencí.
6. Stanovení mechanismů pro interní komunikaci a podávání zpráv o rizicích a jejich zvládání.
7. Stanovení mechanismů pro externí komunikaci a podávání zpráv o rizicích a jejich zvládání.

Pro implementaci řízení rizik je nutné:

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

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

Analýza rizika znamená kritické studium kauzálního vztahu příčiny – dopady. Hodnocení rizik znamená porovnání úrovní rizik získaných analýzou rizik s kritérii pro posuzování rizik. Hodnocení rizika z pohledu prevence, připravenosti, odezvy a obnovy musí obsahovat:
- identifikaci ohrožení; specifikaci jevů (nebo scénářů), které ohrožují; specifikaci četnosti výskytu jevů (nebo scénářů), které ohrožují; odhad důsledků jevů (nebo scénářů), které ohrožují (ve kterých je zahrnuto i působení místní zranitelnosti); odhad rizika z kombinace důsledků jevů (nebo scénářů), které ohrožují a četností výskytu; ocenění kroků pro odhad rizika a provedení odhadu rizika; ocenění výsledků odhadu rizika pro potřeby rozhodnutí,
- standardy a normy pro regulaci projektování a provozování lidských činností; postupy a systémy řízení bezpečnosti; a popř. další,
- jakým způsobem jsou cíle řízení rizika nastaveny, zda: cíle o úrovni rizika jsou kvalitativní nebo kvantitativní; splňují technické standardy; standardy řízení jsou systémové; a další.

Zvládání rizik dle podkladů uvedených v [2] znamená v případě, že riziko není přijatelné, provést:
- vyhnutí se riziku (tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika), když to jde – u přírodních pohrom to nejde,
- odstranění zdrojů rizik, tj. zabránění vzniku pohrom, když to jde – u přírodních pohrom to nejde,
- snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom (např. snížením množství nebezpečných chemických látek v podnicích), když to jde – u přírodních pohrom to nejde,

- 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,
- retenci rizika.

Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika.

Pro posuzování účinnosti řízení rizika se používá index, který hodnotí výkonnost řízení rizika – RMI (Risk Management Index). Jedná se o kvalitativní míru, která je založená na cílech, které si řízení rizik vytyčilo. Někdy se též používají indikátory, u kterých se požaduje, aby byly transparentní, robustní, reprezentativní a snadno pochopitelné pro uživatele (veřejnost, politici, veřejná správa apod.).

Řízení rizik je třeba aplikovat na celé technické dílo, celou organizaci, která technické dílo spravuje, a to v mnoha oblastech a na mnohých úrovních, v kteroukoli dobu a také při řízení projektů a činností.

6.3.2. Validita zvládnutí rizika při použití norem a standardů

Další používané normy spojené s rizikem v technické praxi jsou: ČSN IEC 300-3-9; ČSN OHSAS 18001; ČSN EN ISO 12100; ČSN EN ISO 12 100-1; ČSN EN ISO 14121-1; ČSN EN 1050:2001; ČSN EN ISO 12100-1; ČSN EN ISO 12100-2; ČSN EN ISO 9000 atd.

Normy a standardy ukládají požadavky, které jsou oprávněné. Nestanovují však často způsob, jak požadavky splnit, tj. jaká data a jaké metody použít. Platí jen pro jisté podmínky, což znamená, že existují rizika spojená s jejich využitím, jak ukazují obrázky 6 a 8.

Proto při aplikaci norem a standardů si musíme uvědomit, co standardy pokrývají. V daném směru jsou obvykle založené na zásadách teorie pravděpodobnosti. Proto si musíme uvědomovat, že v žádném případě nepokrývají všechny možné varianty. Při použití normálního rozdělení platí, že interval (medián-σ, medián +σ) pokrývá 68.5 % případů; interval (medián -2σ, medián +2σ) pokrývá 95.4 % případů; interval (medián -3σ, medián+3σ) pokrývá 99.8 % případů. To znamená, že neplatí pro celý rozsah možných podmínek. Proto u důležitých technických děl je nutno provádět všechna hodnocení spojená s riziky a bezpečností jako místně specifická, tj. vycházet z logických základů metod a systémového pojetí entity; aplikace různých kódů a software, které nejsou místně specifické, mohou za kritických podmínek vést k selhání technických děl [4,64].

V praxi při práci s riziky spojenými s technickými díly se stále používají jen tradiční metody, jako jsou Kontrolní seznam, HAZOP, FMEA, FMECA, QRA apod. [2,9], protože pro ně existuje řada software. Jak již bylo dříve řečeno, předmětné metody při práci s riziky nerespektují systémový charakter technického díla při dopadech vnějších pohrom, úmyslných vnějších aktů (např. korupce na správních úřadech s cílem oslabit konkurenceschopnost technického díla), teroristických činů apod., což potvrzují šetření US EPA [69], která již byla zmíněna. To znamená, že platí, že předmětné metody lze použít s ohledem na bezpečnost technických děl jen při řešení některých úloh, ve kterých nejde o integritu bezpečnosti technického díla; všeobecně použitelné metody jsou správně aplikované metody What, If [2,9] a místně specifické kontrolní seznamy, které jsou sestavené experty.

6.3.3. Poznámka k výběru expertů

Jestliže vezmeme v úvahu složitost světa a jeho komponent, tak vzniká otázka, jaká je přesnost jeho modelování za účelem řešení jeho problémů. Současné poznání ukazuje, že analytické metody mají mnohá omezení, a proto při řešení zásadních otázek se používají heuristické metody. To znamená, že při řešení problémů je třeba používat zkušenosti, které mají experti. Úsudek experta je používán v případech, kdy nejistoty existující při chápání a popisu řešeného problému jsou vysoké; tj. existuje mnoho neurčitostí.

V práci [105] je ukázáno, že predikce expertů se ne vždy potvrdí, což potvrzují i záležitosti z běžného života např. z oblasti předpovědi počasí nebo analýzy havárií [63]. Proto je třeba řešit zavedení a použití expertů. V případě prvním jde o záležitosti: jak experta vybrat; zda vybrat jednoho nebo několik expertů; jak stanovit výsledek na základě dat od více expertů, tj. jak agregovat jejich názory několika expertů. V druhém případě jde o problém využití: informace od experta; a informace o expertovi. Kvalitu výsledků totiž ovlivňují faktory: kvalifikace experta; postup odhadu; proces výběru expertů; metoda agregace výsledků; a dostupné informace o výkonu experta.

Proto např. nařízení US NRC z r. 1997 používá při výběru expertů průkazy požadavků: akademické vzdělání a zkušenosti pomocí recenzovaných publikací; obeznámenost a znalost různých aspektů spojených s řešeným problémem; snaha prosazovat nezaujatě názor; dostupnost a ochota věnovat čas a úsilí při řešení problému; specifické znalosti a odbornost v předmětné oblasti; ochota efektivně se účastnit diskusí a poskytovat hodnocení a interpretace; schopnost komunikace, flexibilita nestrannost, schopnost generalizovat i zjednodušovat. Pro získání kvalitního výsledku při použití několika expertů je třeba experty motivovat a sjednotit hladiny jejich pohledů na problém (např. hierarchie pohledů od špatného k dobrému). Pro získání kvalitních výsledků je důležitá agregace vyjádření expertů. Lze ho provést matematicky, anebo na základě kritérií, tj. heuristicky např. metodou DELPHI; podobný systém pravidel používá i EU [2]. .

Autor práce [105] ukazuje na příkladech, že u problémů, které lze popsat tvrdými modely, lepší výsledky dávají matematické analytické postupy. Avšak u problémů, které lze popsat pouze měkkými modely, jsou výsledky heuristických přístupů lepší než analytické metody. Aby nedošlo k přecenění nebo podcenění některých aspektů rozhodovaného problému, je důležité vybrat experty, kteří jsou:

- obeznámeni s technickým problémem,
- mají znalosti:
  - v širší oblasti než je rozhodovaný problém,
  - z matematiky, fyziky a technických disciplín,
  - analýzy rizik,
  - rozhodování a příbuzných disciplín,
  - z oblasti prosazující veřejný zájem.

Stejné závěry vyplývají z diskusí na odborných setkáních [3] a nakonec i ve sdělovacích prostředcích v poslední době je otázka, kdo je expert.

Podle nároků na experty, jež jsou shrnuté v práci [3] se expertem míní osoba, která je uznávaná odbornou komunitou, má experimentální zkušenosti v dané oblasti, určitý počet kvalitních odborných publikací, zná podstatu nejistot různých konceptů, roz-

manitost podmínek, způsoby kompenzace škod a má zájem o řešení předmětného problému. Mnoho příkladů z praxe však ukazuje, že řada odborníků, kteří se považují za experty je postižena provozní slepotou, je uchlácholena splněním požadavků norem a standardů a nevidí rizika spojená s různými vazbami a spřaženími s okolím [3,63,64].

Praxe [3,63,64] také ukázala, že u složitých technických děl nestačí jeden expert, ale je třeba kombinovat znalosti několika expertů. Velký důraz je kladen na kvalifikovanost expertů (průkaz znalostí, zkušeností, objektivity a schopnosti hledat konsensus). Kombinaci návrhů lze dle povahy rozhodovaného problému zajistit pomocí analytických metod nebo heuristik, např. metody DELPHI, panelová diskuse [9]. Systematické zapojení expertů snižuje potřebu improvizace při zvládání kritických situací.

Rozvoj technologií směřuje stále více ke kombinaci jednotlivých zařízení a aplikací do komplexních (složitých) systémů s cílem dosáhnout zvýšení výroby a vysoké ziskovosti. Vytvářené systémy nejsou výsledkem expertů z jedné disciplíny (oboru), nýbrž jsou výsledkem interdisciplinárního týmu. Zvláště pro síťové technologie platí, že jednotlivý expert není schopen kompletně posoudit a ovládat velké technické systémy, a proto je nutná spolupráce expertů z řady disciplín, která vyžaduje vzájemné pochopení cílů a schopnost hledání konsensu.

Dodnes je skutečností, že při sestavování technických děl a při vytváření jejich bezpečnosti experti z různých oborů pracují odděleně, což nezaručuje ani optimální bezpečnost, ani optimální náklady. Často se stává, že jednotlivé dílčí systémy jsou bezpečné, protože pro ně existují standardy a normy (např. jednotlivé technické části určitého provozu), ale bezpečnost celku, který vznikl jejich propojením s kybernetickými a jinými infrastrukturami již sledovaná není, protože se hodnocení a prokázání bezpečnosti nepožaduje relevantní legislativou a navíc k danému účelu není dosud k dispozici relevantní odborný postup. Právě uvedená skutečnost znamená slabinu pro bezpečnost technických děl. Dosavadní řešení jsou prováděná na základě dobré inženýrské praxe a jejich dlouhodobá bezpečnost a spolehlivost se těžko prokazuje.

7. ZÁVĚR

Svět, ve kterém žijeme je proměnný. Jeho okamžitý stav je určen rozmanitými procesy, jejichž převážnou část lidé neovládají, i když jsou obdařeni inteligencí, která jim dovoluje svět pozměňovat. Výsledky předmětných procesů nejsou vždy pro člověka přijatelné. Mírou jejich přijatelnosti pro člověka je veličina riziko, která je velmi ovlivněná náhodností a neurčitostí procesů, které probíhají ve světě kolem nás. Když chceme s předmětnou veličinou u technických děl pracovat s cílem zajistit bezpečí lidí i bezpečná technická díla, tak musíme:

- pochopit, co riziko znamená (tj. jde o normované očekávané škody, ztráty a újmy na chráněných aktivech, přičemž z hlediska lidské společnosti je třeba zvažovat jak chráněná aktiva technického díla, tak veřejná aktiva),
- znát ohrožení, která pro technické dílo představují všechny možné pohromy, tj. zdroje rizik všeho druhu, a to dnes i v budoucnosti (tzv. All-Hazard-Approach v provedení rozpracovaném pro Evropu, které bylo výše zmíněno),
- umět pracovat s pravděpodobností,
- uvědomit si existenci neurčitostí spojených s podmínkami, ve kterých je technické dílo, a které se v čase mění, protože okolní svět i samo dílo se dynamicky vyvíjí,
- udělat vše pro bezpečnost technických děl i jejich okolí (zde hraje zásadní roli motivace a odpovědnost).

Modelem světa a modelem každé jeho důležité entity (tj. i každého složitého technického díla) je soubor otevřených a vzájemně propojených systémů, které jsou uspořádány do řady hierarchických úrovní, jež jsou také propojené. V reálném světě chování hierarchicky vyššího souboru systémů určuje chování systémů na nižší úrovni hierarchie, ale také platí, že výrazný jev, který se vyskytne na nižší úrovni hierarchie, může mít potenciál narušit soubor systémů na vyšší úrovni hierarchie. Příkladem druhého faktu je, že lidská činnost poškozuje jak životní prostředí, tak planetární systém exhalacemi. Proto je třeba sledovat nejenom dílčí rizika, ale i rizika spojená s vazbami a toky v systémech a napříč systémů (tj. interdependences), tj. snažit se odhadnout integrální riziko.

Shromážděné poznatky ukázaly, že technická díla by měla být konstruována a provozována s vědomím, že:

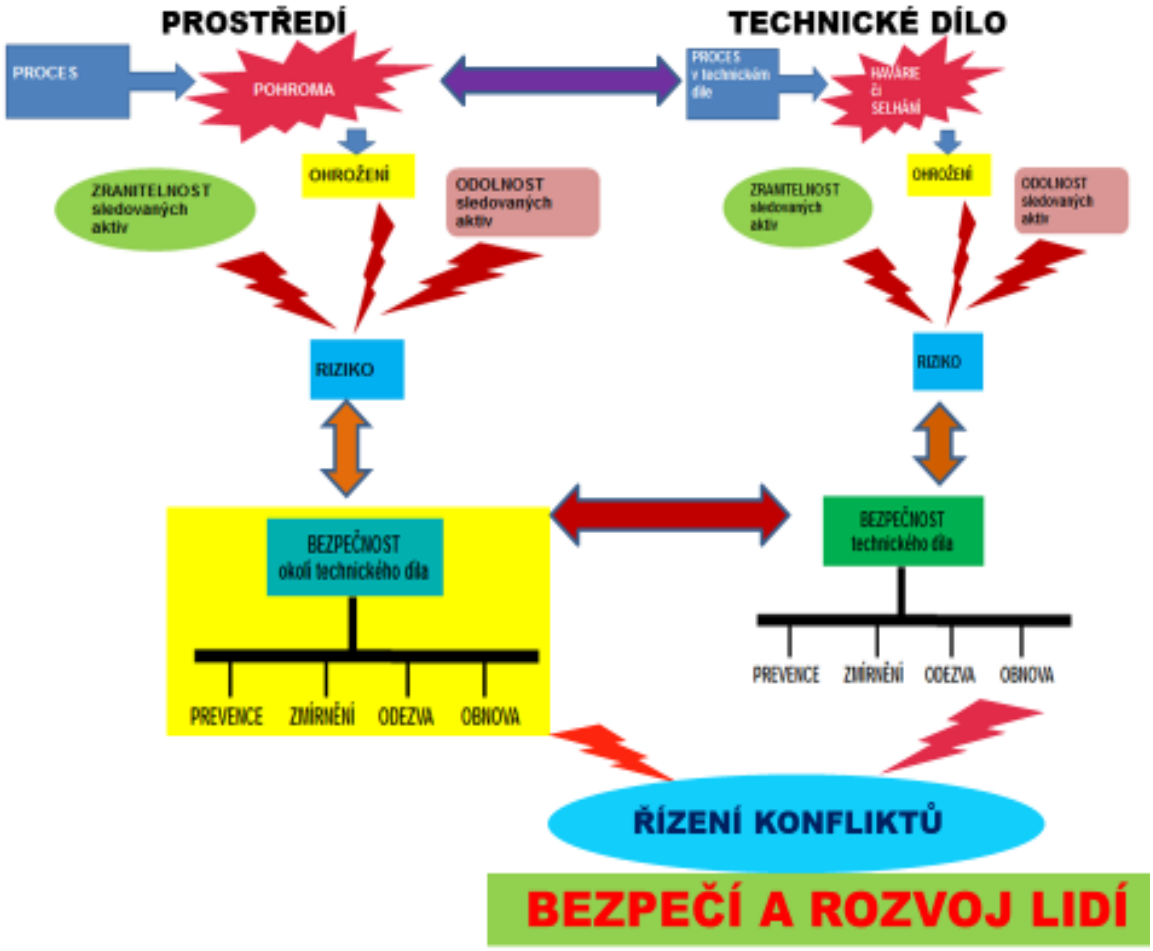
- každé technické dílo je systém systémů, který se v čase mění,
- v důsledku změn v technickém díle a okolí může dojít ke konfliktu, který nebyl očekáván (realizace neočekávaného rizika),
- technické dílo i okolí jsou postihovány pohromami s tím, že velké pohromy se vyskytují zřídka a nepravidelně, a proto jejich možné velikosti nejsou odhalitelné metodami založenými na teorii pravděpodobnosti (realizace neočekávaně velkého rizika),
- pohromami pro technické dílo se stávají i vazby a spřažení, a to jak ty, které jsou úmyslně vytvořené z důvodu cíle, který technické dílo plní, tak i ty, které vzniknou neplánovaně tím, že v důsledku pohromy dojde k neočekávaným propojením, která pak vyvolají selhání díla a nepřijatelné dopady na jeho okolí.

Ve spojitosti s technickými díly je třeba pro zajištění bezpečí a rozvoje lidí aplikovat práci s riziky zaměřenou na bezpečnost technických děl a jejich okolí. V důsledku náhodných i znalostních nejistot je pro každé lidské společenství z pohledu veřejného zájmu, konkurenceschopnosti technického díla a udržitelného rozvoje lidského systému důležité, zda:

- bezpečnost (tj. úroveň opatření a činností ve prospěch bezpečí lidí, tj. i technického díla) v čase roste či klesá,
- ve stanovených časových úsecích je dosahováno plánované úrovně bezpečnosti,
- aplikovaná opatření vedou skutečně ke zvýšení bezpečnosti.

Představa o řízení rizik procesů spojených s technickými díly a jejich okolím je zobrazena na obrázku 29. Technické dílo i okolí na sebe neustále působí, přičemž konfliktní situace nastávají zejména ve čtyřech fázích:
- výběr typu technického díla a jeho umístění do území,
- výstavba technického díla,
- provoz technického díla,
- vyřazení technického díla z provozu a umožnění dalšího využití území zabraného technickým dílem.

V kapitole 4 byly shrnuty hlavní zdroje rizik při výstavbě a provozu technických děl. Pro ostatní oblasti je třeba provést podrobný výzkum za účelem stanovení hlavních zdrojů rizik.



Obr. 29. Řízení rizik procesů spojených s technickými díly a jejich okolím.

Protože jak technické dílo, tak jeho okolí jsou složité systémy, které se vyvíjí a tento vývoj nemusí byt nutně synergický, tak aplikace přesných matematických metod za-

ložených na teoriích, které počítají jen s náhodnými změnami, není schopna určit parametry a jejich proměnnost, jež zajistí bezpečnost technického díla po celou dobu životnosti. Inženýrské disciplíny pracující s riziky proto zavádí do praxe nástroje založené na heuristickém přístupu pro práci s riziky, kterými lze zvládnout i podmínky, pro něž nebylo technické dílo konstruováno. Základní aspekty byly uvedeny v pracích [2-4,17] a jsou shrnuty v předchozích kapitolách.

Nashromážděná fakta ukazují, že pro zajištění bezpečnosti složitých technických děl je nutno z důvodu složitosti pracovat s riziky specifickým způsobem. Nestačí aplikace norem a standardů, které mají omezenou platnost. Je třeba poznat dopady stabilních i možných dočasných propojení mezi prvky, komponentami a systémy technického díla i při abnormálních a kritických podmínkách, a podle toho sestavit systém řízení bezpečnosti a způsob jeho fungování v čase. Jelikož během času vznikají rizika nová, je třeba mít pravidelný monitoring rizik, jehož součástí budou i připravená nápravná opatření pro případ výskytu nepřijatelných rizik.

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání technických děl, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie (často označované jako ***černé labutě, dračí králové*** atd.). Proto nyní připouštíme, že složité objekty, jakými jsou technická díla, jsou z různých důvodů čas od času v nestabilním stavu a vznikají extrémní havárie, kaskády selhání bez zjevné příčiny, neobvyklé jevy apod., tj. připouštíme nejistoty náhodné i znalostní v jejich chování. Z důvodu zajištění jejich bezpečnosti a ochrany lidí:

- zavádíme specifická technická opatření (např. po havárii jaderné elektrárny Fukushima čtvrtý nezávislý zdroj energie a čtvrtý nezávislý zdroj chladiva pro vytvoření schopnosti provést odezvu na příští extrémní pohromu),
- připravujeme řešení odezvy pro možné případy, kdy se realizují rizika z příčin, které nelze odhalit pravděpodobnostními přístupy, a budujeme pro ně náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik inženýrů a záchranářů.

V návaznosti na tento fakt, výsledky výzkumu v EU, uvedené v práci [3], ukazují velmi mnoho nedostatků spojených s prací s riziky. Příčiny uvedených nedostatků v oblasti vrcholového řízení států byly identifikovány takto:

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

Ve všech úvahách si je třeba uvědomit existující fakta, a to:

- riziko je inherentní vlastností lidského systému (světa) i každého technického díla, tj. není možné se mu zcela vyhnout,
- zdroje rizik jsou uvnitř i vně technického díla a v procesech, které v technickém díle probíhají a mění se v čase, a jsou také v člověku, tj. tvůrci technického díla,

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

Na základě zkušeností autorky, která se v roli recenzenta odborných prací a projektů setkala s výsledky specialistů z oblasti informačních technologií, kteří na křídovém papíře prezentovali barevné obrázky modelů zpestřené blikajícími efekty, jež odporovaly fyzikálním zákonitostem (např. zákonu o zemské přitažlivosti, zákonu útlumu energie se vzdáleností apod.) uvádíme pravidla publikovaná Golombem v r. 1970 [106]:

1. Nevěřte důsledkům 33. řádu u modelů 1. řádu.
2. Neextrapolujte výsledky modelu za hranice jeho platnosti.
3. Nepoužívejte žádný model, dokud neporozumíte zjednodušujícím předpokladům, na kterých je založen.
4. Nevěřte tomu, že model je realita.
5. Nepokoušejte se realitu přizpůsobit modelu.
6. Neomezujte se pouze na jediný model sledovaného jevu nebo procesu. Použití více modelů pro sledovaný jev umožňuje lépe porozumět jeho různým aspektům.
7. Nepoužívejte modely, o kterých se ví, že nejsou správné.
8. Nebuďte zamilovaní do svého modelu.
9. Neaplikujte terminologii oblasti A na problémy oblasti B. Neprospěje to žádné z nich.
10. Nečekejte, že pokud jste problém pojmenovali, tak jste ho také vyřešili.

Zejména je třeba se vyvarovat přístupu, který je možno shrnout do následujících bodů:

1. Pokud máte kladivo, hledáte hřebík.

2. Pokud máte dobré kladivo, vše vypadá jako hřebík.

Dynamické vlastnosti systémů jsou dány dynamickými charakteristikami, které mohou být algebraické nebo experimentální. Algebraické dynamické charakteristiky používáme tehdy, když známe strukturu systému, chování jeho jednotlivých prvků, a to i s konkrétními číselnými hodnotami konstant a parametrů. Mezi dynamické charakteristiky lineárních soustav patří: diferenciální rovnice, obrazový přenos, frekvenční

přenos, frekvenční charakteristika v komplexní rovině, frekvenční charakteristika v semilogaritmických souřadnicích. Pro syntézu lineárních regulačních systémů má největší význam obrazový přenos definovaný na základě Laplaceovy transformace [107]. Jinak používáme experimentální dynamické charakteristiky, pomocí nichž sestavíme matematický model. Podle stability řízení řízeného systému dělíme řídicí systémy na stabilní, přechodové a nestabilní; cílem praktických úloh je pochopitelně tvorba a provoz stabilního řídicího systému.

Každý řídicí systém má v souladu s prací [108] pět vzájemně souvisejících struktur:
- rozhodovací,
- funkční,
- organizační,
- informační,
- technické zabezpečení.

Každá struktura řeší specifický okruh problémů, přičemž mnohé z nich jsou vzájemně provázané, tj. jde též o systém systémů. Cílem praktických úloh je pochopitelně najít optimální řešení pro všechny uvedené systémy, jak ukazuje [4].

Poznatky pro kvalitní práci s riziky, zacílenou na bezpečné technické dílo a jeho bezpečné okolí, uvedené v publikaci lze shrnout následovně:
- určit kritické procesy, kritická místa a kritická aktiva technického díla,
- zvážit všechny možné pohromy, které mohou ovlivnit technické dílo (All-Hazard-Approach) a vypořádat se s nimi pomocí aplikace přístupu Defence-In-Depth,
- monitorovat a posuzovat rizika v čase a posuzovat úroveň bezpečnosti technického díla a v případě, že není žádoucí reagovat kvalifikovaně na prioritní rizika; mít stanoven systém řízení bezpečnosti, jehož aspekty byly popsány v předchozích kapitolách.

Důležité je si uvědomit, že riziko je nejen proměnné v čase, ale i místně specifické, a tudíž není určitelné nástroji, které byly odvozené jinde pro konkrétní situace a mají softwarové podoby. Zde je nutné respektovat podmínky transferu technologií a nástroj přizpůsobit místním podmínkám. Přizpůsobení místním podmínkám vyžaduje:
- rekognoskaci technického díla a jeho okolí doprovázenou určením kritických procesů, kritických míst a kritických aktiv technického díla,
- stanovení variantních scénářů pro prioritní pohromy (příčiny prioritních rizik), jejichž zdroje jsou uvnitř i vně technického díla a také lidský faktor. Z důvodu výše zmíněného poznání, že použití jednoho software, které respektuje jen výrobní proces, vede k nezvážení dopadů pohromy na několik míst technického díla najednou (v technickém slangu mluvíme o příčinách selhání technického díla z jedné příčiny), je nutné vytvořit scénáře pro technické dílo jako celek s mnoha aktivy, i scénáře pro dobře definované části kolem kritických míst. Na základě všech scénářů stanovit dopady na aktiva technického díla metodou What, If,
- logicky vyhodnotit variantní scénáře a jejich dopady, a přitom vyznačit a posoudit možná propojení.

Pak už lze použít logické rutinní postupy, které jsou shodné u obecných metod, popsaných v kapitole 4, a které jsou obsaženy v modelu obsaženém v normě ISO 31 000, a mají softwarové podpory. Z uvedeného je zřejmé, že know how práce s riziky je právě v prvních bodech, které jsou určeny specifikami technického díla. Ze zkušeností z praxe vyplývá, že právě tato část je často podceněná zpracovateli, kteří věří v sílu software. Kvalitní provedení první specifické části práce s riziky vyžaduje spolupráci odborníka, který má zkušenosti s popsanými úkoly a odborníků

z technického díla, kteří mají místní znalosti a zkušenosti. Pro podporu praxe, jsou proto v publikaci uvedeny konkrétní příklady jak vzorů úspěšných aplikací nástrojů používaných inženýrskými disciplínami při práci riziky, tak obecné nástroje, které lze použít u každého technického díla, protože je v nich inherentně zabudována proměnnost sledovaných položek v prostoru i čase.

Předložená práce shrnula poznatky o rizicích technických děl a jejich okolí tak, aby ukázala nástroje, kterými lze řídit a vypořádat rizika ve prospěch bezpečnosti jak technického díla, tak jeho okolí, tj. aby byla zajištěna jejich koexistence. Tím vytvořila základ pro praktická inženýrská řešení.

LITERATURA

[1] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN: 978-80-01-04844-3. Praha: ČVUT 2011, 483p.

[2] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. ISBN: 978-80-01-04841-2. Praha: ČVUT 2011, 405p.

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

[4] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení.* ISBN: 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364p. http://hdl.handle.net/10467/72582

[5] UN. *Human Development Report*. New York… UN, 1994, www.un.org.

[6] HAIMES, Y. Y. 2009. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis* 29(2009), 12, pp. 1647–1654.

[7] ISO*. Risk Management – Principles and Guidelines*, ISO 31000:2009.

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

[9] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN: 978-80-01-04842-9. Praha: ČVUT 2011, 369p.

[10] PROCHÁZKOVÁ, D. *Krizové řízení pro technické obory*. ISBN 978-80-01-05292-1. ČVUT, Praha 2013, 303p.

[11] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury.* ČVUT, Praha 2012, ISBN: 978-80-01-05103-0, 318p.

[12] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Integrální bezpečnost zajišťuje optimální rozvoj životního prostředí*. ISBN 978-80-01-05480-2. ČVUT, Praha 2014, 224p.

[13] PROCHÁZKOVÁ, D. et al.: *Risk of Processes and Their Management*. ISBN: 978-80-01-06144-2; e- ISBN 978-80-01-06186-2. Praha: ČVUT 2017, 295p.

[14] PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. ISBN: 978-80-01-04843-6 Praha: ČVUT 2011, 301p.

[15] PROCHÁZKOVÁ, D., PROCHÁZKA, J, PATÁKOVÁ, H., PROCHÁZKA, Z., STRYMPLOVÁ, V. *Kritické vyhodnocení přepravy nebezpečných látek po pozemních komunikacích v ČR.* ISBN 978-80-01-05599-1. Praha: ČVUT 2014, 150p.

[16] PROCHÁZKOVÁ, D. *Study of Disasters and Disaster Management*. ISBN: 978-80-01-05246-4. Praha: ČVUT 2013, 202p.

[17] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223p.

[18] PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládání*. ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234p.

[19] PROCHÁZKOVÁ, D. The Human Factor and Its Handling. Chapter 7. In: Y. Chen and L. Li (edited book). *Advances in Intelligent Vehicles*, Academic Press 2013, ISBN-10:0123971993, pp. 199-224; ISBN-13:978-0-12-397199-9 Elsevier, Oxford 2014, ISBN 978-0-12-397199-9. https://www.elsevier.com/ books/advances-in-intelligent-vehicles/chen/978-0-12-397199-9; DOI: 10.1016/ B978-0-12-397199-9.00007-0.

[20] PROCHAZKOVA, D. *Challenges Connected with Critical Infrastructure Safety.* ISBN: 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218p.

[21] PROCHAZKOVA, D. *Challenges to Future Disasters Management*. ISBN: 978-3-659-53926-8. Saarbruecken. Lambert Academic Publishing 2014, 170p.

[22] PROCHÁZKOVÁ, D. *Boj proti terorismu. Projekt EU: Improving Security by Democratic Participation – ISDEP*. ISBN: 978-80-01-05568-7. Praha: ČVUT 2014, 200p.

[23] PROCHÁZKOVÁ, D., PROCHÁZKA, J., PATÁKOVÁ, H., PROCHÁZKA, Z., STRYMPLOVÁ, V. Výsledky systematického studia rizik spojených s přepravou nebezpečných látek. In: *Ochrana obyvatelstva 2014.* ISBN: 978-80-7385-142-2, ISSN: 1803-7372, Ostrava: SPBI 2014, pp. 191-194.

[24] PROCHAZKOVA, D. *Safety of Complex Technological Facilities.* ISBN: 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244p.

[25] BRIŠ, R., GUEDES SOARES, C. & MARTORELL, S. (eds). *Reliability, Risk and Safety. Theory and Applications.* ISBN 978-0-415-55509-8. London: CRC Press 2009, 2362p.

[26] ALE, B., PAPAZOGLOU, I., ZIO, E. (eds). *Reliability, Risk and Safety.* ISBN 978-0-415-60427-7. London: Taylor & Francis Group 2010, 2448p.

[27] BÉRENGUER, C., GRALL, A., GUEDES SOARES, C. (eds). *Advances in Safety, Reliability and Risk Management*. ISBN 978-0-415-68379-1. London: Taylor & Francis Group 2011, 3035p.

[28] IAPSAM (eds). *Probabilistic Safety Assessment and Management Conference. International. 11th 2012. (and Annual European Safety and Reliability Conference).* ISBN: 978-1-62276-436-5. Helsinki: IPSAM & ESRA 2012, 6889p.

[29] STEENBERGEN, R., VAN GELDER, P., MIRAGLIA, S., TON VROUWENVELDER, A. (eds). *Safety Reliability and Risk Analysis: Beyond the Horizon*. ISBN 978-1-138-00123-7. London: Taylor & Francis Group 2013, 3387p.

[30] NOWAKOWSKI, T., MLYŇCZAK, M., JODEJKO-PIETRUCZUK, A., WERBIŃSKA-WOJCIECHOWSKA, S. (eds) *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453p.

[31] PODOFILLINI, L., SUDRET, B., STOJADINOVIC, B., ZIO, E., KRÖGER, W. (eds). *Safety and Reliability of Complex Engineered Systems: ESREL 2015.* ISBN 978-1-138-02879-1. London: CRC Press, 4560p.

[32] WALLS, L., REVIE, M., BEDFORD, T. (eds). *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. ISBN 978-1-315-37498-7. London: CRC Press, 2942p.

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

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

[35] PROCHÁZKOVÁ, D. (ed.). *Selected Risks of Business Processes.* ISBN:978-80-01-05831-2 Praha: ČVUT 2015, 190 p.

[36] PROCHÁZKOVÁ, D. (ed.). *Rizika podnikových procesů 2015.* ISBN: 978-80-7414-967-2. Ústí nad Labem: Universita Jana Evangelisty Purkyně 2015, 212 p.

[37] PROCHÁZKOVÁ, D. (ed.). *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT, 2016, 507p.

[38] PROCHÁZKOVÁ, D. (ed.). *Risk and Business and Territorial Processes.* ISBN: 978-80-7561-021-8. Ústí nad Labem: UJEP 2016, 204p.

[39] PROCHÁZKOVÁ, D. (ed.). *Řízení rizik procesů spojených s technickými díly.* ISBN: 978-80-01-06351-4. Praha: ČVUT 2017, 297p. http://hdl.handle.net/ 10467/73522

[40] EU. *The Safe Community Concept*. PASR project.Brussels: EU 2004.

[41] GEYSEN, W. The Acceptance of Systemic Thinking in various Fields of Technology and Consequences on Respective Safety Phylosophies. In: *Safety of Modern Systems.*

Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 19-27.

[42] PROCHÁZKOVÁ, D. Identification and Management of Risks of System of Systems. *PSAM11 and ESREL 2012 Proceedings*. ISBN 978-162-276-4365. Helsinki: IPSAM & ESRA 2012, pp 6542-6551.

[43] IAEA. *Safety Guides and Technical Documents*. Vienna: IAEA 1954 – 2017. www.ns.iaea.org/standards

[44] COMAH. *Safety Report Assessment Manual: COMAH*. London: UK- HID CD2 London 2002, 570 p.

[45] PROCHÁZKOVÁ, D. Optimum Concept of Management and Trade-off with Risks. In: *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. CD ROM. London: Taylor & Francis Group 2015, pp 1463-1471.

[46] BORGES, HICKEY, C. Balancing Safety and Performance through QRA and RAM Analyses. In: Safety and Reliability: Methodology and Applications. ISBN: 978-1-138-02681-0. London: Taylor & Francis Group 2015, pp 445-452.

[47] 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.

[47] IAEA. *Assessment of Defence in Depth for Nuclear Power Plants*. ISBN:92–0–114004–5. Safety report series No. 46. IAEA, 2005 Vienna, 119p.

[49] INSAG. *Defence in Depth in Nuclear Safety. INSAG-10.* ISBN 92-0-103295-1 IAEA, 1996.

[50] IAEA. *Safety of Critical Power Plants: Design, Safety Standards Series No. NS-R-1.* Vienna: IAEA 2000.

[51] SEVCIK, A., GUDMESTADO, T. Solutions and Safety Barriers: The Holistic Approach to Risk-Reducing Measures. In: *Safety and Reliability: Methodology and Application*. ISBN:978-1-138-02681-0. London: Taylor & Francis Group 2014.

[52] VATN, J. Structuring Contributors to Successful Operation. In: *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group, 2014.

[53] IAEA. *Format and Content of the Safety Analysis Report for Nuclear Power Plants. Safety Guide. No. GS-G-4.1*. Vienna: IAEA 2010.

[54] OECD. *Guiding Principles on Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2003, 192 p.

[55] SCHOPPE, G., ZEHETNER, J., FINGER, J., BAUMANN, D., SIEBOLD,U., HÄRING, I. Risk Assessment Methods for Improving Urban Security. In: *Safety and Reliability: Methodology and Application*. ISBN: 978-1-138-02681-0. London: Taylor & Francis Group 2015.

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

[57] THON, R. *Cybersecurity – the human factor.* www.nsm.strat.no

[58] PROCHÁZKOVÁ, D. *Metodika pro odhad nákladů na obnovu majetku v územích postižených živelní nebo jinou pohromou*. Ostrava: SPBI SPEKTRUM XI 2007, ISBN 978-80-86634-98-2, 251p.

[59] PERROW, CH. *Normal Accidents: Living with High-Risk Technologies.* Princeton: Princeton University Press 1999.

[60] REASON, J. *Human Error*. Cambridge: Cambridge University Press, 1990.

[61] SHAFER, G. A. *Mathematical Theory of Evidence*. Princeton: University Press 1976, 292p.

[62] DEMPSTER, A. P. Upper and Lower Probabilities Induced by a Multivalued Mapping. In: *The Annals of Mathematical Statistics*, 38 (1967), No 5, pp. 325-339.

[63] PROCHÁZKOVÁ, D. *Archiv řešených úloh z oblasti řízení bezpečnosti a krizového řízení.* Praha: ČVUT, fakulta dopravní, ústav bezpečnostních technologií a inženýrství

[64] PROCHÁZKOVÁ, D. Šetření podstaty stížností a konfliktů týkajících se technických řešení. *Kontrola MSK ČR 1992*. MSK ČR Praha, 95p.

[65] KEENEY, R. L, RAIFFA, H. *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1976, 1993, 569p.

[66] PROCHÁZKOVÁ, D., ŠESTÁK, B. *Kontrolní seznamy. Nástroj rizikového inženýrství*. ISBN 80-7251-225-0. Praha: PA ČR 2006, 319p.

[67] SPERSTAD, I. B., KIEL, E. S. SINTEF Energy Research, Trondheim, Norway. In: *Risk, Reliability and Safety: Innovating Theory and Practices*. ISBN: 978-1-138-02997-2. London: CRC Pres / Balkema 2016, pp.1599-1608.

[68] CONTINI, P. M., CONTINI, S., COPELLI, S., ROTA, R., DEMICHELA, M. From HazOp Study to Automatic Construction of Cause Consequence Diagrams for Frequency Calculation of Hazardous Plant States. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1 (Hbk+CD-ROM), ISBN:978-1-315-64841-5 (eBook pdf), London: Taylor &Francis Group 2015. www.crcpress.com – www.tayloeandfrancis. com, pp. 347-355.

[69] US EPA. PHA Techniques in Chemical Emergency Prevention & Planning. *Newsletter* 2008, No. 8, pp. 3-6.

[70] GUANGHAO ZHU, YUFENG SUN & GUANGYAN ZHAO. A Dynamic Fault Tree Method for Availability Assessment of the Repairable Gas Transmission System. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1 (Hbk+CD-ROM), ISBN:978-1-315-64841-5 (eBook pdf) London: Taylor &Francis Group 2015. www.crcpress.com – www.tayloeandfrancis.com pp. 1897-1903

[71] SHORTRIDGE, J. E., AVEN, A., GUIKEMA, S. D. Risk Assessment under Deep Uncertainty: A Methodological Comparison. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1 (Hbk+CD-ROM), ISBN:978-1-315-64841-5 (eBook pdf) www.crcpress.com – www.tayloeandfrancis.com, London: Taylor &Francis Group 2015. pp. 847-855

[72] http://www.uneptie.org/apell

[73] DROGUETT, E. L, MOSLEH, A. Bayesian Methodology for Model Uncertainty Using Model Performance Data. *Risk Analysis*, 28 (2008), pp. 1457-1476.

[74] BJERGA, T., AVEN, T., ZIO, E. An Illustration of The Use of an Approach for Treating Model Uncertainties In Risk Assessment. *Reliability Engineering & System Safety*, 125 (2014), pp. 46-53.

[75] KAZEMI, R., MOSLEH, A. Improving Default Risk Prediction Using Bayesian Model Uncertainty Techniques. *Risk Analysis*, 12 (2012), 11.

[76] STRAUB D., PAPAIOANNOU I., BETZ W. Bayesian Analysis of Rare Events. *Journal of Computational Physics*, 314 (2016), pp. 538–556.

[77] PROCHÁZKOVÁ, D. Critical Infrastructure Safety Management. In: *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-415-55509-8, ISBN 978-0-203-85975-9. Leiden: CRC Press / Balkema 2009, pp. 1875-1882.

[78] KLIR, G. J. Where Do We Stand on Measures of Uncertainty, Ambiguity, Fuzziness, and the Like. *Int. J. Fuzzy Sets and Systems* (1987), 24, pp. 141–160.

[79] FERSON, S., GINZBERG, L., AKÇAKAYA, R. Whereof one CANNOT SPEAK: When Input Distributions are Uknown. *Applied Biomathematics Report 2001.* http://www.ramas.com/whereof.pdf. Retrieved on 03/04/16.

[80] SAATY, R. The Analytic Hierarchy Process—What It Is and How It Is Used. *Mathematical Modelling* 9 (1987), 3–5, pp. 161–176.

[81] DEVUYST, D. Sustainaability Assessment: the Application of a Methodological Framework. In: *Proceedings of the 19th Annual Meeting of the International Association for Impact Assessment*. Glasgow, 15-20 June 1999, 37p.

[82] VISSER, J. K.. Comparison of Probability Distributions for Use in Reliability and Maintainability Simulation. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1 (Hbk+CD-ROM), ISBN:978-1-315-64841-5 (eBook pdf). London: Taylor&Francis Group 2015. www.crcpress.com, www.tayloeandfrancis. com

[83] RINNE, *H. The Weibull Distribution: a Handbook*. London: CRC Press (Taylor and Francis Group) 2008.

[84] NIKLOVÁ, D. *Kvantitativní charakteristiky zemětřesné činnosti*. Diplomová práce. Praha: MFF UK 1968.

[85] ZHANG, H. et al. *Numerical Methods for Simulation and Optimization of Piecewise Deterministic Markov Processes*. JohnWiley & Sons 2015.

[86] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Problems Connected with Determination of Size of Maximum Expected Disaster in Selected Site. In: *Risk, Reliability and Safety: Innovating Theory and Practices*. ISBN: 978-1-138-02997-2. London: CRC Pres / Balkema 2016, pp. 1443-1450.

[87] PROCHÁZKOVÁ, D. Seismické inženýrství na prahu třetího tisíciletí. ISBN 978-80-7385-022-7. Ostrava: SPBI SPEKTRUM XII 2007, 468p.

[88] PROCHAZKOVA, D., DEMJANCUKOVA, K. *Earthquakes, Hazards and Principles for Trade-off with Risks.* ISBN: 978-80-261-0170-3. Plzen: University of West Bohemia, 2012,212p.

[89] KÁRNÍK, V., PROCHÁZKOVÁ, D., SCHENK, V., SCHENKOVÁ, Z., BROUČEK, I. Seismic Zoning Map - Version 1987. *Studia geoph. et geod.,* 32 (1988), 144-150.

[90] 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. ISBN:978-1-138-02879-1 (Hbk+CD-ROM), ISBN:978-1-315-64841-5 (eBook pdf) www.crcpress.com – www.tayloeandfrancis.com, pp.365-371.

[91] ERCAN, P. MERT, B. Occupational Health and Safety in Food Seasoning Sector. *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1 (Hbk+CD-ROM), ISBN:978-1-315-64841-5 (eBook pdf). London: Taylor &Francis Group 2015. www.crcpress.com – www.tayloeandfrancis.com 3245-3251

[92] WSH. *Code of Practice on Workplace Safety and Health Risk Management.* London: Workplace Safety 2011. www.wshc.sg.

[93] NHS. General Workplace Health and Safety Risk Assessments. *Trust Standard Procedure 2014. Version 01*. http://www.torbaycaretrust.nhs.uk.

[94] KUZUCUOĞLU, A. H. Risk Management in Libraries, Archives and Museums. IIB *International Refereed Academic Social Sciences Journal*. 5 (2014), 15, pp. 277–294.

[95] COASE, R. H. The Problem of Social Cost. *Journal of Law and Economics,* 3 (1960), pp. 1-44.

[96] PROCHÁZKOVÁ, D., PROCHAZKA, J. Checklist for Judgemet of Technical Facility Safety and Results Obtained by Its Application in Practice. judgement of technical facility safety level and results obtained by its application in practice. Proceedings of International European Safety and Reliability Conference, ESREL2018. ISBN: 978-0-8153-8682-7 (Handbook). London: Taylor & Francis Group 2018; ISBN: 978-1-351-17466-4 (eBook); https://www.ntnu.edu/esrel 2018; pp. 1175-1184.

[97] ALE, B. J. M. Tolerable or Acceptable: A Comparison of Risk Regulation in the United Kingdom and the Netherlands. *Risk Analysis* 25(2005), 2, pp. 231–241.

[98] MELCHERS, R. E. On the ALARP Approach to Risk Management. *Reliability Engineering and System Safety* 71 (2000), pp. 201–208.

[99] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.

[100] ČR. ČSN EN 61508-X, 61511-X

[101] KERTIS, T., PROCHÁZKOVÁ, D. Informační výkon a kybernetické příčiny dopravních nehod. In: *Řízení rizik procesů spojených s technickými díly.* ISBN: 978-80-01-06351-4. Praha: ČVUT 2017, http://hdl.handle.net/10467/73522, pp. 44-59,

[102] HUDSON, P., HUDSON, T. *Possibility space: Understanding risk.* https://www.ntnu.edu/ esrel2018

[103] FAWCETT, H. H. *Hazardous and Toxic Materials. Safe Handling and Disposal.* New York: Willey 1984.

[104] PROCHÁZKOVÁ, D., PROCHAZKA, J. Causes of Accidents in Civilian Aircraft Operation and Tools for Management of Selected Risks. In: *Safety and Reliability – Theory and Applications.* ISBN: 978-1-138-62937-0. London: Taylor & Francis Group 2017, pp. 3057-3066.

[105] MOSLEH, A. *Ask An Expert.* https://www.ntnu.edu/esrel2018

[106] GOLOMB, S. W. Mathematical Models - Uses and Limitations of Simulation. *Mathematical Journal*, 14 (1970), No. 4, pp 197 - 198.

[107] BURÝ, A. Teorie systémů a řízení. Ostrava: VŠB-TU 2007, 62p.

[108] NACHÁZEL, K. *Stochastické metody ve vodním hospodářství*. Praha: ČVUT 2000, 63p.

REJSTŘÍK KLÍČOVÝCH SLOV

V seznamu nejsou uvedena základní klíčová slova, na které je práce zaměřena, tj. bezpečí, bezpečnost a riziko, protože se vyskytují příliš často.

Titul:	Analýza, řízení a vypořádání rizik spojených s technickými díly
Autor:	Doc. RNDr. Dana Procházková, DrSc.
Recenzenti:	Prof., Ing. Josef Říha, DrSc. Doc. Ing. Jiří Lukavský, CSc. Doc. Ing. Václav Beran, DrSc. Doc. RNDr. Miroslav Rusko, PhD.
Vydavatel:	DSPACE ČVUT v Praze
Počet kopií:	Open Access
Počet stránek:	222
Rok vydání:	2018

ISBN 978-80-01-06480-1