VYPOŘÁDÁNÍ RIZIK V INŽENÝRSKÝCH OBORECH

Dana Procházková

PRAHA 2024

Recenzenti:
Doc. Ing. Branislav Lacko, CSc.
Doc. Ing. Petr Šrytr, CSc.

ISBN 978-80-01-07272-1

https://doi.org/10.14311/BK.9788001072721

OBSAH

ABSTRAKT

Sledování historie z pohledu vývoje nástrojů zajišťujících bezpečí a rozvoj lidských komunit ukazuje, že každé lidské společenství v době minulé pečovalo na své úrovni znalostí a zkušeností o svá sídla a jejich materiálním, technickém, ekonomickém a sociálním zázemí, tj. provádělo jistá opatření a činnosti pro své bezpečí, tj. cíleně pracovalo na bezpečnosti. To znamená, že lidstvo od svého počátku pracovalo na vypořádání rizik.

Riziko jako míra výskytu škodlivé události je ovlivněno dynamickým vývojem světa, a proto je ovlivněno nejistotou a neurčitostí. Proto k rozvoji poznání přispělo formulování principu neurčitosti v 30. letech minulého století německým teoretickým fyzikem, matematikem a filozofem Werner Karl Heisenbergem. Neurčitost se podobá nejistotě a označuje nedostatek znalostí a informací, protože se vztahuje k přirozené variabilitě procesů a dějů, nejednoznačnosti a neostrosti významů a vztahů.

Na základě výše uvedených poznatků se postupně vyvinuly inženýrské přístupy k řízení a vypořádání rizik – inženýrství rizika (risk engineering), které pracují jak s nejistotou, tak s neurčitostí. Inženýrství rizika je aplikace inženýrských dovedností a metodik pro řízení a vypořádání rizik. Předmětné přístupy umožňují proaktivně řídit a zmírňovat rizika. Tyto akce umožňují veřejné správě, organizacím, podnikům i občanům činit informovaná rozhodnutí a optimalizovat své investice na maximální hodnotu.

Monografie řeší řízení a vypořádání rizik, která se vyskytují v životním cyklu technických děl a technických zařízení:

- výběr typu technického díla či technického zařízení a lokality umístění,
- projektování, výstavba, testování a spuštění technického díla či zařízení do provozu,
- provoz technického díla či zařízení,
- údržba technického díla či zařízení,
- modernizace technického díla či zařízení,
- vyřazení z provozu technického díla či zařízení.

Ukazuje jak příčiny rizik, tak opatření a činnosti, a to technická i netechnická, pomocí kterých se rizika eliminují či alespoň zmírňují u technických zařízení a technických děl v uvedených životních cyklech. Řeší otázky metodické i praktické na úrovni současných znalostí a zkušeností. V závěru popisuje specifické inženýrské postupy, které jsou odborníky doporučované pro práci s riziky v praxi, a ukazuje, že při aplikaci opatření a činností je vhodné používat metodiku projektového řízení.

Klíčová slova: technické dílo, technické zařízení, riziko, bezpečnost, zdroje rizik, řízení rizik, vypořádání rizik.

SUMMARY

Monitoring the history from the point of view of the development of tools ensuring the security and development of human communities shows that each human community in the past cared for its settlements and their material, technical, economic and social background at its level of knowledge and experience, i.e. it carried out certain measures and activities for its security, i.e. it purposefully worked on safety. This means that humans have been working to cope with risks since their inception.

Risk as a measure of the occurrence of a harmful event is influenced by the dynamic development of the world, and therefore, it is affected by random uncertainty and epistemic uncertainty. Therefore, the formulation of the epistemic uncertainty principle in the 1930s by the German theoretical physicist, mathematician and philosopher Werner Karl Heisenberg contributed to the development of knowledge. Epistemic uncertainty resembles uncertainty, which refers to the lack of knowledge and information, since it refers to the natural variability of processes and actions, the ambiguity and fuzziness of meanings and relationships.

On the basis of the above-mentioned knowledge, engineering approaches to risk management and settlement have gradually developed – risk engineering, which work with both, the random uncertainty and the epistemic (knowledge) uncertainty. Risk engineering is the application of engineering skills and methodologies to manage and cope with risks. These approaches allow you to proactively manage and mitigate risks. These actions enable public administrations, organisations, businesses and citizens to make informed decisions and optimise their investments to maximum value.

The monograph deals with the management and settlement of risks that occur in the life cycle of technical facilities and technical equipment:

- selection of the type of technical facility or technical equipment and the location of sitting,
- design, construction, testing and commissioning of technical facility or equipment,
- operation of a technical facility or equipment,
- maintenance of technical facility or equipment,
- modernization of technical facility or equipment,
- decommissioning of a technical facility or equipment.

It shows both, the causes of risks and measures and activities, namely both, the technical and the non-technical ones, by means of which risks are eliminated or at least mitigated in the case of technical equipment and technical facility in the mentioned life cycles. It deals with methodological and practical issues at the level of current knowledge and experience. In conclusion, it describes specific engineering procedures that are recommended by experts for working with risks in practice, and shows that it is appropriate to use project management methodology when applying measures and activities.

Key words: Technical facility, technical equipment, risk, safety, sources of risk, risk management, risk settlement.

SEZNAM ZKRATEK

Zkratka	Název
AI	Umělá inteligence
ALARA	As Low as Reasonably Achievable
ALARP	As Low as Reasonable Possible
BOZP	Bezpečnost a ochrana zdraví při práci
CBA	Cost Benefit Analysis
CBM	Condition-Based Maintenance
ČR	Česká republika
ČSN	Česká technická norma
ČVUT	České vysoké učení technické
DSS	Decision Support System
EU	European Union
IAEA (MAAE)	International Atomic Energy Agency
I&C system	Information and Control System
ISO	International Organization for Standardization
IT	Informační technologie
OECD	Organisation for Econom ic Co-operation and Development
OSN / UN	Organizace spojených národů / United Nations
PC	Personal computer
PSA	Probabilistic Safety Assessment (pravděpodobnostní hodnocení bezpečnosti)
Sb.	Sbírka zákonů ČR
SoS	System of Systems (system systémů)
SIL	Safety Integrity Level (úroveň integrity bezpečnosti)

SMS	Safety Management System (systém řízení bezpečnosti)
TQM	Total Quality Management
USA	United States of America

PŘEDMLUVA

Od starověku v celé historii lidstva na různých místech světa jsou zřetelným příkladem rozvoje inženýrství (techniky) vojenské systémy, a to jak dobyvačné, tak ochranné. Jejich nedostatky a selhání ukazují mnohé historické události. Sledování historie z pohledu vývoje nástrojů zajišťujících bezpečí a rozvoj lidských komunit ukazuje, že každé lidské společenství v době minulé pečovalo na své úrovni znalostí a zkušeností o svá sídla a jejich materiální, technické, ekonomické a sociální zázemí, tj. provádělo jistá opatření a činnosti pro své bezpečí, tj. cíleně vypořádávalo rizika ve prospěch bezpečnosti.

Riziko jako míra výskytu škodlivé události určité velikosti je ovlivněno dynamickým vývojem světa, a proto je ovlivněno nejistotou (způsobenou náhodnými vlivy) a neurčitostí (způsobenou neznalostmi příštího dynamického vývoje světa). Postupně se vyvinuly inženýrské přístupy k řízení a vypořádání rizik – inženýrství rizika (risk engineering), které pracují jak s nejistotou, tak s neurčitostí. Inženýrství rizika je aplikace inženýrských dovedností a metodik pro řízení a vypořádání rizik. Předmětné přístupy umožňují proaktivně řídit a zmírňovat rizika. Tyto akce umožňují veřejné správě, organizacím, podnikům i občanům činit informovaná rozhodnutí a optimalizovat své investice pro maximální hodnotu

K zásadnímu rozdílu v pojetí bezpečnosti došlo v polovině 90. let minulého století. OSN ve zprávě pro rozvoj lidstva stanovila přechod od konceptu „bezpečný stát zajišťuje bezpečí pro lidi“ ke konceptu „bezpeční lidé zajišťují bezpečný stát“, tj. prioritou při volbě opatření a činností se stalo bezpečí lidí. V současné době se v souvislosti se zajištěním bezpečí a dalšího rozvoje pro lidskou společnost stále častěji diskutuje problematika kritických aktiv, kterými jsou kromě lidí a přírodních zdrojů i kritické objekty a kritické infrastruktury, které představují složité kyber-socio-technologické systémy.

Inženýrské disciplíny jsou hnací silou lidského vývoje, protože se zabývají i problémy, které je obtížné přesně řešit. K dosažení cíle používají kreativitu lidských jedinců a přístupy označované jako dobrá praxe. Pokrývají nejen technické a ekonomické obory, ale i sociální obory, protože člověk je tvůrcem i provozovatelem technických děl. Technická díla jsou výsledkem lidského intelektu a jejich aplikace v praxi umožňuje lidem rozvoj a přežití nástrah přírody. Představují inženýrská díla, která jsou ohrožena riziky, která jsou v místě jejich umístění i riziky vnitřními, a jsou také zdroji rizik pro své okolí. Proto vypořádání rizik je zásadní pro bezpečnost technických děl i bezpečnost jejich okolí.

Předložená práce propojuje poznatky získané z: odborné literatury; vlastního výzkumu; a ze zkušeností z praxe. Protože se opírá o současnou úroveň poznání, jde někdy i za hranice požadavků, které ukládá současná legislativa. Navazuje na předchozí publikace autorky jak pojmy, tak i konceptem a strategií.

Autorka děkuje recenzentům panu doc. Ing. Branislavu Lackovi, CSc. a panu doc. Ing. Petru Šrytrovi, CSc. za recenze a cenné poznámky a připomínky, které pomohly vylepšit text publikace. Velký dík patří panu Ing. Janu Jirouškovi a panu Ing. Karlu Vidlákovi za sponzorování publikace. Autorka zároveň velmi děkuje ČVUT za vydání publikace, která ukazuje způsoby vypořádat rizika, která je nutno zvažovat v inženýrských oborech.

1. ÚVOD

Cílem současné lidské společnosti je bezpečí a rozvoj lidské společnosti. Podle poznatků shrnutých v práci [1] to znamená, že lidé musí provádět opatření a činnosti, které zajišťují:

- existenci, tj. rovnováhu v lidském systému, který je modelem životního prostoru lidí,
- efektivnost, tj. schopnost lidského systému vyrovnat se s nedostatkem zdrojů,
- volnost, tj. schopnost lidského systému dobře zvládat výzvy z okolí,
- bezpečí, tj. schopnost lidského systému ochránit se před jevy uvnitř i vně,
- adaptaci, tj. schopnost lidského systému přizpůsobit se vnějším změnám,
- koexistenci, tj. schopnost lidského systému měnit své chování tak, aby chování reagovalo na chování a orientaci dalších systémů a aby je neohrožoval a ony neohrožovaly jeho.

Předložená práce je zaměřena na řízení a vypořádání rizik technických děl a technických zařízení. Zvažuje technická díla, která:

- zajišťují výrobky a služby, které zkvalitňují život lidí,
- přispívají k:
  - zaměstnanosti,
  - technické vzdělanosti,
  - energetické soběstačnosti
  - dopravě,
  - zásobování vodou
  - 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. Proto se bezpečností, chápanou jako úroveň souboru antropogenních opatření a činností k zajištění bezpečí a rozvoje lidské společnosti zabývají téměř všechny obory lidského zkoumání.

Publikace se zabývá zásadami inženýrství, které je zacíleno na bezpečnost v integrálním smyslu. Integrální bezpečnost má rozměry environmentální, ekonomické, technické, potravinové, zdravotní, osobnostní a komunitní i politické apod. ***Inženýrství zacílené na bezpečnost*** je inženýrská disciplína, tj. aplikovaná věda, která úzce souvisí s inženýrstvím systémů (v češtině systémovým inženýrstvím) a která zajišťuje, že inženýrské systémy mají přijatelnou úroveň bezpečnosti, tj. chovají se tak, jak je potřeba a přitom neohrožují sebe ani své okolí. Představuje soubor znalostí a dovedností, které řeší určitý problém, tj. uspokojují požadavky, kterými jsou užitečnost, disponibilita a bezpečnost.

Práce vychází ze současného poznání:

- technická díla chápe jako vzájemně propojené otevřené systémy různé povahy, které jsou umístěny v prostředí, které má též systémovou povahu a je dynamicky proměnné,
- riziko jako míra výskytu škodlivé události je ovlivněno dynamickým vývojem světa, a proto je ovlivněno nejistotou a neurčitostí. Neurčitost se podobá nejistotě (přesněji náhodné nejistotě) a označuje nedostatek znalostí a informací, protože se vztahuje k přirozené variabilitě procesů a dějů, nejednoznačnosti a neostrosti významů a vztahů.

Postupně se vyvinuly inženýrské přístupy k řízení a vypořádání rizik – inženýrství rizika (risk engineering), které pracují jak s nejistotou, tak s neurčitostí. Inženýrství rizika je aplikace inženýrských dovedností a metodik pro řízení a vypořádání rizik. Předmětné přístupy umožňují proaktivně řídit a zmírňovat rizika. Tyto akce umožňují veřejné správě i podnikům činit informovaná rozhodnutí a optimalizovat své investice pro maximální hodnotu.

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 (zdroje rizik), jejichž projevy nejsou synergické. Dopady těchto jevů 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 na základě svých znalostí a zkušeností předmětné jevy řídí s cílem zajistit své bezpečí a rozvoj. V rámci toho jde i o zajištění koexistence technických děl a okolí.

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 [2,3].

Dále sledujeme recentní pojetí bezpečnosti, které se opírá o teorii systémů a je ve vyspělých zemích prosazované od 90. let. Je kodifikované deklarací a smlouvou OSN v r. 1994 [4] a v Evropské unii je kodifikované Maastrichtskou smlouvou z roku 1992 [5]. Dle Maastrichtské smlouvy je bezpečnost nejvyšším znakem kvality sledovaného objektu. V uvedeném pojetí dle poznatků, které jsou shrnuty v pracích [1,2] platí:

- riziko je mírou očekávaných ztrát a škod na objektu, zařízení, území, procesu, technickém vybavení i technickém díle, které může způsobit škodlivý jev z pohledu lidské společnosti,
- bezpečnost je mírou kvality objektu, zařízení, systému, území, procesu, technického zařízení či technického díla, tj. vyjadřuje úroveň kvality souboru antropogenních opatření a činností, která vedou k zajištění bezpečí a rozvoje objektu, zařízení, území, procesu, technického zařízení i technického díla.

Dle současného poznání je riziko inherentní vlastností současného světa a je proměnné v čase i prostoru [1,2]. Proto bezpečnost každé entity lze zajistit jen permanentním řízením rizik, které aplikuje inženýrské dovednosti a metodiky (risk engineering) ke zmírnění dopadů rizik [1,2]. Vzhledem k dynamickému vývoji světa, je zajištění bezpečnosti kontinuální proces. Protože riziko lze zmírnit nejen technickými, ale i organizačními opatřeními, tak doplňkovou veličinou k bezpečnosti není riziko, ale kritičnost (tj. míra rychlé změny kvality sledované entity).

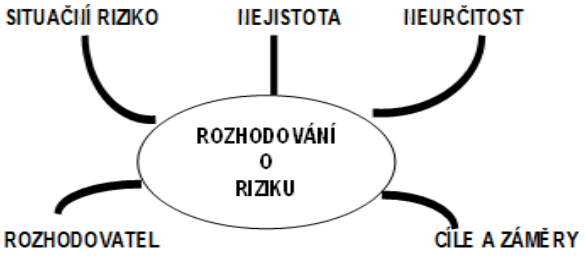
Jelikož lidské znalosti, schopnosti a možnosti jsou omezené, tak se při řízení rizik soustřeďujeme jen na podstatné položky, které označujeme jako položky kritické. Pojmy s vazbou na slovo „kritický“ se v oblasti bezpečnosti velmi rozšířily po roce 1998, ve kterém vydal prezident USA Bill Clinton Presidential Decision Directive 63, tzv. Bílou knihu [6], jejímž záměrem bylo přijetí nutných opatření pro snížení zranitelnosti důležitých sektorů kritické infrastruktury vůči fyzickým a kybernetickým útokům.

Pojem „kritický“ se v oblasti inženýrských disciplín používá u položek ve smyslu závažnosti/důležitosti pro funkčnost zařízení, objektu, území, organizace, území, státu [7], tj. je vždy spojen s pojmem bezpečnost. Označuje položku, která je zároveň potřebná a velmi zranitelná. Kritické jsou prvky, vazby mezi prvky či toky mezi prvky, procesy, funkce, komponenty, systémy či celé objekty. Pojem kritický není totožný s

pojmem vyhrazený, který je v české legislativě (např. zákon č. 22/1997 Sb.), ani s pojmem krizový (např. zákon č. 240/2000 Sb.), což politici a další často používají.

Seznam dále používaných pojmů a jejich definic je v práci [2]. Používané metody, postupy a software jsou charakterizovány v práci [3].

Při práci s riziky si je třeba uvědomit, 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 1.



Obr. 1. 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 (neurčitosti) 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 [3].

Z výše uvedené skutečnosti je zřejmé, že ke zvýšení „nebezpečnosti / kritičnosti“ rozhodnutí o rizicích technických děl obecně přispívají:
- *složitost a rozmanitost cílů* (často jsou konfliktní),
- *citlivost rozhodnutí na změny,*
- *neurčitost klíčových proměnných*
- *a rozdílné pohledy na situaci.*

Protože technická díla jsou pro lidstvo důležitá, tak si je třeba uvědomit, že při kritických situacích není řešení „technické dílo obětovat“, tj. provést opatření a činnosti, které ho zcela zničí, protože technické dílo jednak dodává výrobky nebo zajišťuje služby, a jednak zaměstnává lidi a je zdrojem ekonomického kapitálu pro dané území. Proto je třeba řídit závažná rizika se zacílením na bezpečnost technických děl při všech možných podmínkách.

Každé technické dílo má své limity a podmínky dané projektem a způsobem řízení rizik při jeho provozu [1]. Při dynamických změnách světa však vznikají i jevy, jejichž projevy přesáhnou limity, a proto inženýrské disciplíny systematicky předem vytváří ochranná opatření a činnosti, aby dopady na lidi, životní prostředí i technická díla byly co nejmenší.

2. SOUBOR POZNATKŮ O RIZICÍC77H V INŽENÝRSKÝCH OBORECH

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. Jejich cílem je 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.

2.1. Povaha a problémy technických zařízení a technických děl

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 shrnutých v pracích [1,8], každý inženýrský systém je charakterizován strukturou, hardwarem, procedurami, prostředím, toky informací, organizací a rozhraním mezi těmito komponentami. Základním prvkem ochrany technických děl a technických zařízení v oblasti technických řešení je aplikace spolehlivých technických prvků, jejich kvalifikované propojení a provozní režim dovolující bezpečný a spolehlivý provoz, včasná a řádná údržba, zálohování prioritních částí technických zařízení či děl, využití různých principů zálohování a promyšlené rozmístění záloh v území. Aspekty důležité pro péči o technická zařízení i celá technická díla jsou však velmi rozmanité, především jde o aspekty znalostní a technické, které předurčují kapacitní možnosti technických děl a technických zařízení, organizační a právní záležitosti, které umožňují provoz technických děl a technických zařízení na určité úrovni v území a v čase, a nelze opominout otázky finanční, personální a politické na národní a mezinárodní úrovni.

Na základě současného poznání [2] je každý objekt otevřený systém, který se skládá z řady položek, které jsou vzájemně propojené. Jednotlivé položky i celek, se dynamicky vyvíjí na základě procesů probíhajících uvnitř i vně systému. Propojení mezi položkami jsou fyzická, kybernetická, územní a logická a v řadě případů jsou zranitelnější než položky [1]. ***Bezpečnost objektu či procesu vyjadřuje úroveň kvality souboru antropogenních opatření a činností, která vedou k zajištění bezpečí a rozvoje objektu či procesu*** [1,2].

Vývoj objektu v čase je narušován jevy, které jsou světu vrozené / inherentní a mají od určité velikosti nežádoucí, a tudíž nepřijatelné dopady na objekty, které lidská společnost potřebuje pro život [2]. V inženýrských disciplínách při strategickém řízení zaměřeném na dlouhodobou bezpečnost a výkonnost technických děl a technických procesů je definováno riziko jako pravděpodobná velikost ztrát, škod a újmy na chráněných aktivech objektu a veřejných aktivech v okolí:

- způsobených škodlivým jevem s normativně určenou velikostí, kterou označujeme jako projektová / návrhová pohroma,
- a která je normovaná na zvolené jednotky času a území.

Riziko je závislé na velikosti konkrétního škodlivého jevu (pohromy) a na místní zranitelnosti aktiv [2]. Míra narušení bezpečnosti objektu se nazývá „***kritičnost***“ a závisí na velikosti škodlivého jevu a na zranitelnosti objektu, tj. zranitelnosti jeho aktiv a jejich propojení, tj. na velikosti rizika [2].

Cílem inženýrských disciplín je snížit riziko a zvýšit bezpečnost, přičemž zvýšení bezpečnosti lze dosáhnout nejen snížením rizika, ale i vzděláním a připraveností lidí a lidské společnosti [1,2]. Řízení a vypořádání rizik vyžaduje rozměr a měření rizik, které bere v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Proto je třeba aplikovat holistický přístup a respektovat skutečnost, že riziko je rozdělené na lokální, regionální i státní úroveň.

V Evropské unii se od roku 1989 používá při řízení objektů, institucí i území řízení typu „Total Quality Management (TQM)“, který je pro oblast technologických celků charakterizován v práci [9]. Předmětný typ řízení je upraven soubory norem ISO 9000 a jejich formálními postupy certifikace v devadesátých letech 20. století. Dle tohoto konceptu jsou technická zařízení i technologické objekty (obecně entity) považovány za systémy systémů – SoS (otevřený soubor otevřených systémů) [1,2] a při jejich charakteristice se používají specifické pojmy jako jsou: koherentnost (soudržnost); kompatibilita; operabilita; interoperabilita; integrita bezpečnosti; provozní spolehlivost; odolnost; atd. [2].

Bezpečný objekt je systém, který je zajištěn vůči všem škodlivým jevům, a který ani při svých kritických podmínkách neohrožuje sebe a své okolí, tj. prostor, ve kterém žijí lidé. Při zajišťování bezpečnosti objektu [2] se odborně především posuzuje:

- očekávaná velikost ztrát, škod a újmy na chráněných aktivech,
- výčet nežádoucích jevů, které se mohou přihodit,
- přijatelnost dopadů rizik přímých i zprostředkovaných spletitou sítí vazeb a toků a jejich následků na aktiva, objekt jako celek a jeho okolí,
- míra schopnosti opatření zajistit ochranu
- a míra schopnosti systému řízení bezpečnosti zvládnout existující ohrožení, tj. zda zajistí, že riziko bude při realizaci akceptovatelné.

Způsob, jak rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet, je prakticky vždy spojen se zvyšováním nákladů. Řízení rizika je

proto vedeno snahou najít hranici, na kterou je únosné riziko snížit, aby vynaložené náklady byly společensky přijatelné. Míra určení přijatelného rizika je většinou předmětem vrcholového řízení a výsledkem politického rozhodování, a proto pro lidskou společnost je nutné, aby se přitom využily současné vědecké a technické poznatky a zohlednily ekonomické, sociální a další podmínky.

Základní principy pro práci a riziky dle [10] jsou:
- být proaktivní,
- domýšlet možné důsledky,
- správně určovat priority z pohledu veřejného zájmu,
- myslet na zvládnutí nepřijatelných dopadů,
- zvažovat synergie
- a být ostražitý.

Proto při stanovení rizika pro strategické rozhodování se musí používat hierarchický multikriteriální postup [2].

Je zřejmé, že nejsme-li schopni riziko identifikovat, analyzovat a ocenit, tak 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 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. Platí moudrost uvedená v práci [11] „Vědět znamená přežít, ignorovat znamená říkat si o zničení“, ze které vyplývá, že ignorování či podceňování řízení a vypořádání rizik je důvodem většiny problémů, nezdarů a katastrof.

Problémy složitých technických děl (jejich modelem jsou systémy systémů, tj. otevřené soubory vzájemně propojených otevřených systémů) [1] jsou:
- náhle vynořené rysy chování, které nelze získat ze znalostí o chování komponent, jde o tzv. emergenci,
- hierarchičnost,
- samo organizovanost,
- rozmanité řídící struktury, což vše dohromady připomíná chaos.

Jde o systémy, které mají otevřenou architekturu, tj. jsou vzájemně závislé. Jelikož při změnách se nechovají synergicky, tak dochází ke konfliktům. Řešení konfliktů znamená optimální vyřešení možných rizik.

Analýza provozu technických děl [1,12] ukázala položky, které ovlivňují výkon technického díla (obrázek 2) a charakteristiky, které je třeba sledovat při zajišťování jejich bezpečného provozu:
- interoperabilita, tj. míra schopnosti technického díla, která zajišťuje, že jeho dílčí části fungují společně efektivním způsobem podle konceptu projektu, který je zaměřen na určitý cíl,
- integrita bezpečnosti – SIL (safety integrity level), tj. schopnost technického díla dosáhnout požadovanou úroveň bezpečnostních funkcí,
- kritičnost, tj. míra, která označuje určitou prahovou hodnotu pro sledovaný SoS, tj. míra, s jakou může dojít k úrazu osob, zničení materiálu, škodě či jiným velkým ztrátám,
- provozní spolehlivost systému (dependability), tj. míra v jaké technické dílo *(*zařízení) plní stanovené požadavky *a* jeho provoz vyhovuje stanoveným podmínkám. Rozkládá se na zranitelnost a odolnost. Je důležitá proto, že spolehlivost ve smyslu

reliability není samotná schopná zajistit SIL. Proto je třeba použít specifické techniky, které zajistí, že systém se vyhne chybám a omylům, a proto se provádí řízení rizik zacílené na bezpečnost a dependability [1,8].

Obr. 2. Položky, které ovlivňují výkon technického díla.

2.2. Riziko a bezpečnost

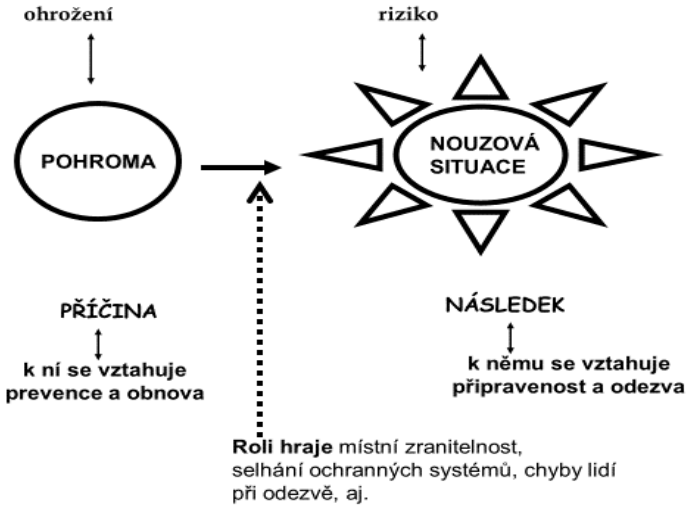
Jak bylo výše řečeno, riziko je mírou ztrát a škod na objektu, zařízení, území, procesu, technickém vybavení i technickém díle, které může způsobit škodlivý jev z pohledu lidské společnosti [2]. Je inherentní vlastností současného světa a je proměnné v čase i prostoru. Ve strategickém řízení [2] jsou definovány 2 veličiny:

- ohrožení (angl. hazard) jako pravděpodobná velikost pohromy, která se v daném místě vyskytne jedenkrát za definovaný časový interval (tzv. projektová nebo návrhová pohroma),
- riziko (angl. risk) jako pravděpodobná velikost ztrát, škod a újmy na sledovaných aktivech při projektové pohromě rozpočtená na jednotku času (nejčastěji 1 rok) a jednotku území.

Jejich vztah je zřejmý z obrázku 3.

Současné poznání shrnuté v práci [2] ukazuje, že:

- riziko je místně a časově specifické, protože závisí na množství a zranitelnosti aktiv v daném území a v daném čase,
- bezpečnost vyjadřuje úroveň kvality souboru antropogenních opatření a činností, která vedou k zajištění bezpečí a rozvoje objektu, zařízení, území, procesu, technického zařízení i technického díla,
- bezpečnost každé entity lze zajistit jen permanentním řízením rizik, které aplikuje inženýrské dovednosti a metodiky (risk engineering) ke zmírnění dopadů rizik



Obr. 3. Vztah mezi veličinami ohrožení a riziko.

2.3. Bezpečnost a spolehlivost

Bezpečný objekt je systém, který plní svou funkci a je zajištěn vůči všem škodlivým jevům, a který ani při svých kritických podmínkách neohrožuje sebe a své okolí, tj. prostor, ve kterém žijí lidé [2]. Podle poznatků shrnutých v práci [1], jsou parametry, které určují kvalitu systému, jsou uspořádány do pořadí:

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

U velmi složitých socio-kyber-technologických systémů majících formu systémů přistupuje k uvedeným parametrům další parametr kvality, kterým je interoperabilita, tj. schopnost propojených systémů plnit správně a včas v daném místě a čase požadované úkoly v požadované kvalitě.

Z výzkumu shrnutého v práci [1] vyplývá, že:

- bezpečný systém je spolehlivý, ale obráceně to neplatí,
- systém bezpečných systémů není vždy bezpečný systém (problémy jsou vazby a toky mezi systémy), a proto je vždy nutno řešit zvlášť otázky jak bezpečnosti jednotlivých systémů, tak jejich souboru,
- typy selhání objektů jsou příčinné, eskalující a kaskádovité,

- charakteristiky infrastruktur jsou prostorové (geografické), časové, provozní a organizační,
- vazby mezi položkami objektů a infrastruktur jsou volné, flexibilní nebo těsné s tím, že těsné vazby nedovolují přizpůsobení.

Je důležité si uvědomit, že bezpečnost i spolehlivost se zajišťují řízením rizik. V řízení rizik jsou nejen rozdíly v cílech řízení, daných definicemi obou položek, ale i v souborech sledovaných zdrojů rizik, které jsou zvažovány při práci s riziky. Obrázek 4 ukazuje, že při řízení rizik pro zajištění spolehlivosti se nesledují všechny zdroje rizik, jako u řízení bezpečnosti.

Obr. 4. Zdroje rizik sledované při řízení spolehlivosti a při řízení bezpečnosti.

Nicméně je třeba vzít v úvahu, že v současné době se používají 3 vyhraněné inženýrské koncepty, které pracují s riziky:

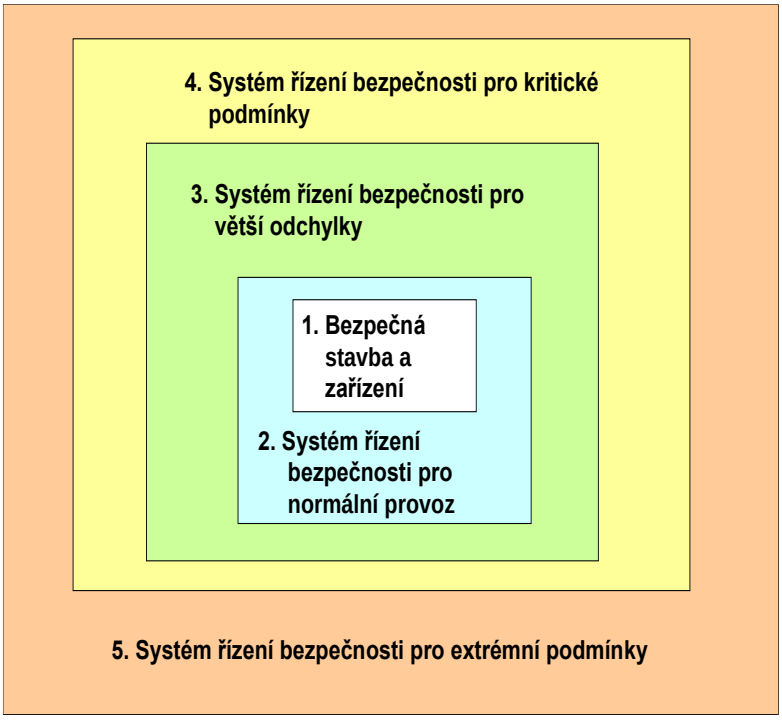
- inženýrství spolehlivosti objektu či zařízení,
- inženýrství zacílené na zabezpečení objektu či zařízení
- a inženýrství zacílené na bezpečnost objektu či zařízení.

Všechny tři uvedené koncepty jsou založené na řízení rizik a používají stejné postupy, metody, nástroje i techniky. Praxe ukazuje, že mezi nimi jsou občas konflikty [1].

U kritických objektů, kterými jsou elektrárny, přehrady, doly, překladiště, kritické infrastruktury, průmyslové a dopravní stavby, překladiště, nádraží, letiště, nemocnice atd. je nutné inženýrství zacílené na bezpečnost, protože předmětné objekty zajišťují služby, které jsou důležité pro základní funkce státu. Strategické řízení entit zaměřené na bezpečí a rozvoj lidské společnosti a dlouhodobou bezpečnost vyžaduje permanentně řešit konflikty mezi výsledky řízení rizik zacílených na bezpečnost, zabezpečení či spolehlivost. Práce [1] např. ukazuje nepřijatelné dopady neřešení konfliktů na lidi.

2.4. Principy pro řízení bezpečnosti

Dle poznatků shrnutých v práci [1], řízení bezpečnosti kritických objektů typu systém systémů používá princip ochrany do hloubky (Defence-in-Depth) – obrázek 5, který spočívá v kombinaci několika následných „nezávislých“ úrovní ochrany. Jeho základní premisa je, že když jedna úroveň ochrany nebo bariéry selže, tak následná úroveň ochrany zachovává funkci. Je-li princip dobře aplikován, tak by jednotlivé technické, lidské nebo organizační selhání nemělo vést k ničivým dopadům a kombinace několika selhání vedoucí k ničivým dopadům by měla mít extrémně malou pravděpodobnost výskytu. Základní principy pro aplikaci principu ochrany do hloubky jsou:



Obr. 5. Pětistupňový systém řízení bezpečnosti složitého objektu.

1. V návrhu, výstavbě a konstrukci inherentně používat principy bezpečného projektu, tj.:

- přístupy: All-Hazard-Aproach [13,14]; proaktivní; systémový aplikující integrální riziko, tj. i dílčí rizika spojená s vazbami a toky hmotnými, energetickými, finančními a informačními v dílčích systémech i napříč nich,
- správnou práci s riziky,
- monitoring provozu, ve kterém jsou zabudovány korekční opatření a činnosti,
- sestavení zadávacích podmínek, které odpovídají danému území a vyjadřují způsob ocenění místních zranitelností, které jsou spojeny s relevantními pohromami, které mohou postihnout dané místo (tj. aplikace All-Hazard-Approach) a respektují parametry technického díla.

Na základě recentního poznání, 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 objektu musí mít základní řídící funkce, alarmy a reakce operátora zpracované tak, aby objekt byl udržen v normálním (stabilním) stavu za normálních podmínek.
3. Objekt 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, což znamená, že má dobrou resilienci (houževnatost). 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 objektu, musí mít objekt 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 systému postihnou okolí objektu, musí mít objekt opatření i pro vnější odezvu, zmírňující opatření pro prevenci ztrát v objektu; a kapacitu pro překonání obtíží.

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.

Pro úspěšné zvládnutí rizik technických děl podle [12] je nutné:
- udržovat provoz ve středních provozních podmínkách - provozní personál musí být řádně vycvičený, ovládat potřebné dovednosti a chápat podstatu řízení základních provozních funkcí,
- zajistit bezpečný provoz za proměnných podmínek - řádně vycvičený provozní personál zná plány provozu za proměnných podmínek a respektuje požadavky kultury bezpečnosti,
- ovládnout kritický stav zařízení pomocí preventivních mechanismů (např. kritických systémů bezpečnosti) - to znamená aplikací pracovních postupů podle daných přijatých standardů a získaných výcvikem ve prospěch vypořádání odchylek od normálního provozu,

- při ztrátě ovládání je nutné znovu získat nadvládu nad systémem, k čemuž je nutné školit personál, aby byl schopen:
  - získat povědomí o situaci,
  - pochopit podstatu problému,
  - porozumět omezení základních stejně jako preventivních funkcí ovládání
  - a také improvizovat,
- při nemožnosti zvládnout zařízení, musí být personál schopen:
  - odstavit technologii tak, že zajistí, co nejmenší ztráty na technologii
  - a aktivovat vnější nouzový plán (tj. aplikovat ochranná opatření a činnosti, uvolnit rezervy, provést evakuaci).

Je zřejmé, že systémy řízení provozu objektu zaměřené jen na normální a abnormální podmínky, neřeší odezvu objektu (tj. technického díla) na specifické a kritické pohromy. Hloubka ochrany a počet jejich úrovní musí být takové, aby zvládly i odezvu. Ochrana do hloubky je proto součástí všech činnosti spojených s bezpečností technického díla: umísťování, navrhování, stavba, výroba, konstrukce, zkušební provoz, uvedení do trvalého provozu, provoz i odstavení z provozu.

Bezpečné technické dílo se zajišťuje pomocí souborů a systémů bariér a režimových opatření [1]. Cílem souboru bariér je:
- kompenzovat lidská a technologická selhání,
- odvrátit poškození zařízení i bariér samotných
- a ochránit lidi a životní prostředí.

Zároveň je nutné zajistit procesy nebo více stupňové bariéry pro případy selhání bariér a jiných prvků ochrany [1].

Cílem první úrovně ochrany (oblast 2 na obrázku 5) zabudované do systému řízení bezpečnosti (SMS – safety management systém) je prevence abnormálního provozu a selhání (základní prostředky jsou konzervativní návrh a vysoká kvalita konstrukce a provozu).

Cílem druhé úrovně ochrany (oblast 3 na obrázku 5) zabudované do SMS je řízení nebo ovládání abnormálního provozu a detekce selhání (ovládací, omezovací a ochranné systémy).

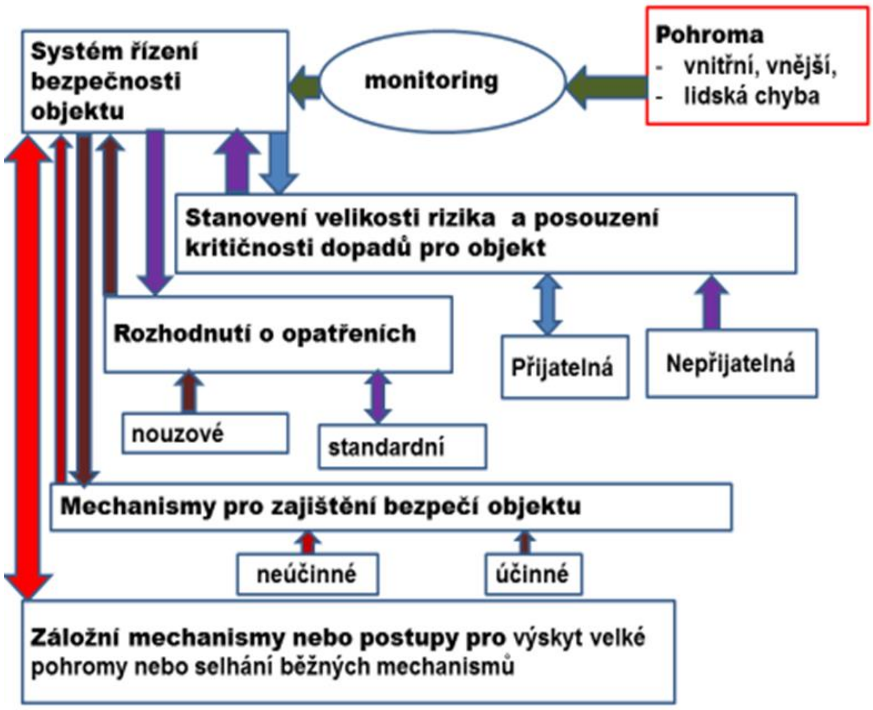
Cílem třetí úrovně ochrany (oblast 4 na obrázku 5) zabudované do SMS je řízení nebo ovládání havárií pomoci projektových opatření (typické znaky dohledu nad provozem jsou naprojektovány inherentní vlastnosti podporující bezpečnost).

Cílem čtvrté úrovně ochrany (oblast 5 na obrázku 5) zabudované do SMS je řízení nebo ovládání kritických podmínek včetně prevence dalšího rozvoje havárie a zmírnění dopadů havárie (alternativní opatření a řízení havárie) na objekt v takovém rozsahu, aby byla možná jeho obnova a iniciace zmírnění dopadů na okolí objektu (tj. iniciace vnějšího plánu odezvy).

Řešení bezpečnosti technického díla zabudované do SMS není možné uskutečnit izolovaně, tj. bez ohledu na okolí. Principy strategického řízení zabudované do SMS jsou ukázány na obrázku 6 [1].

Řízení každé entity dělíme dle rozsahu odpovědnosti, rozhodování a délky plánovacího horizontu. Každá entita plánuje a řídí své aktivity a procesy celkem na třech úrov-

ních: strategická (vrcholová, dlouhodobá), taktická (střednědobá) a provozní (operativní, krátkodobá), přičemž hranice mezi jednotlivými vrstvami nejsou pevné a ostré [1].



Obr. 6. Koncept řízení bezpečnosti objektu.

Řízení technických děl znamená propojit procesy řízení lidí a řízení technických procesů ve smyslu jejich ovládání. Řízení ve smyslu ovládání techniky lze provádět manuálně (ručně), poloautomaticky a automaticky. V současné době automatizace proniká do života všech technických děl. Na jednu stranu přináší obrovské výhody a úspory práce lidí a na straně druhé také další rizika. V souvislosti s automatizací je řízení definováno jako cílené působení řídicího systému na řízený objekt tak, aby bylo dosaženo určeného cíle. V daném kontextu je řízení členěno na automatické a ruční. V dnešní praxi se odlišují ovládání, regulace a vyšší formy řízení (optimální a adaptivní řízení, učení a umělá inteligence) [1].

Na základě poznatků shrnutých v práci [1] pravidla automatického řízení jsou pro daný technický systém vytvářena na základě modelování založeném na teorii spolehlivosti. Na základě dříve uvedených skutečností spolehlivost zařízení se buduje jen na základě dat o náhodných procesech. Proto není zaručena bezpečnost zařízení za všech podmínek, tj. kritických a extrémních podmínek vyvolaných znalostními nedostatky nebo extrémními vlivy. Na základě předmětné skutečnosti vzniká celá řada dalších zdrojů rizik pro technická díla, a to hlavně těch, která používají dálkové přenosy dat.

Systémy pro zajištění bezpečnosti technického díla jsou konstruované jako pasivní anebo aktivní. Nejefektivnějšími zařízeními jsou zařízení pasivní, která fungují na bázi fyzikálních principů (např. gravitace) a pro uvedení do činnosti nepotřebují žádný přidaný impuls. Musí být vždy vybaveny opatřeními pro minimalizování škod v případech, že opatření či systémy pro zajištění bezpečnosti a systémy selžou, anebo se vyskytne

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

U každého řízení technického procesu je důležité provést včas správné rozhodnutí. Lacko v práci [15] ukazuje, že k tomu je potřeba, aby osoba, která rozhoduje, měla dovednost, kterou označuje situační povědomí (situation awareness). V citované práci jsou uvedeny požadavky jak zajišťovat příslušné povědomí, tak příčiny ve vytváření nedostatečného povědomí v konkrétních případech.

3. ZDROJE RIZIK TECHNICKÝCH ZAŘÍZENÍ ZVAŽOVANÉ V INŽENÝRSKÝCH OBORECH

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 je třeba v inženýrských oborech zvažovat vnitřní zdroje rizik, které jsou 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.

3.1. Zdroje rizik při výběru typu technického díla a lokality pro jeho umístění

Na základě výzkumu založeného na analýze 254 případů [16], jehož výsledky jsou shrnuté v práci [17], příčiny selhání technických děl spojené s výběrem typu nebo jeho umístěním jsou uvedeny na obrázku 7. Z výzkumu vyplynulo, že hlavní zdroje rizik, které narušují koexistence technických děl s jejich okolím, jsou především spojeny se znalostmi a chováním subjektů, které řídí území, povolují a dozorují technická díla v území.

Obr. 7. Příčiny selhání koexistence technického díla a jeho okolí z důvodu chybného výběru typu technického díla nebo chybného umístění technického díla do území.

Důsledky chybného výběru typu technického díla nebo chyb při výběru místa se projevily tím, že technické dílo:

- nikdy nebylo dostavěno či dokončeno,
- bylo sice dostavěno, ale nebylo uvedeno do provozu,
- bylo dostavěno, dáno do provozu a provoz předčasně skončil, protože buď vznikly velké náklady na provoz (nákladná obsluha, častá přerušení vyžadující nákladné opravy apod.), anebo se objevily velké konflikty s okolím (kontaminace ovzduší plynnými nebezpečnými látkami, hluk, odpady apod.),
- bylo dostavěno, dáno do provozu a provoz ukončila velká havárie, která byla způsobená interakcemi mezi technickým dílem a okolím, které nebyly v projektu zváženy

Analýza některých konkrétních selhání chybného výběru specifikace či umístění technických děl ukázala, že při rozhodování nebyla zvážena existence podmínek transferu technologií [18]. De facto nebylo vzato v úvahu, že bezpečné (spolehlivé a funkční) technické dílo určují jak parametry technického díla, tak parametry prostředí, do něhož je technické dílo umístěno.

3.2. Zdroje rizik při projektování a výstavbě technickéh521 o díla

Na základě výzkumu založeného na analýze 521 případů [16], jehož výsledky jsou shrnuté v práci [19], příčiny selhání či havárií technických děl, které byly spojené s projektováním a výstavbou, jsou uvedeny na obrázku 8.

Obr. 8. Příčiny selhání koexistence technického díla a jeho okolí z důvodu nedostatků či chyb při projektování, zhotovení a spouštění technického díla do provozu

Z výzkumu vyplynulo, že hlavní zdroje rizik, které narušují koexistenci technického díla s okolím, byly především spojeny se znalostmi a chováním zhotovitelů a investorů a také orgánů veřejné správy, které řídí území, povolují a dozorují technická díla v území. Důsledky příčin selhání se projevily tím, že:

- došlo k selhání nebo havárii technického díla,
- technické dílo muselo být nákladně renovováno, aby splnilo požadavky na něho kladené či přestalo ohrožovat své okolí,
- bylo ztrátové a bylo brzy vyřazeno z provozu.

Analýza některých konkrétních selhání procesu projektování a zhotovení [19] ukazuje, že hlavní příčiny narušení koexistence způsobené chybným provedením procesu projektování, zhotovení a uvedení do provozu technického díla jsou především spojeny se znalostmi a chováním zhotovitelů a investorů, a také orgánů veřejné správy, které řídí území, povolují a dozorují technická díla v území

3.3. Zdroje rizik při provozu technického díla

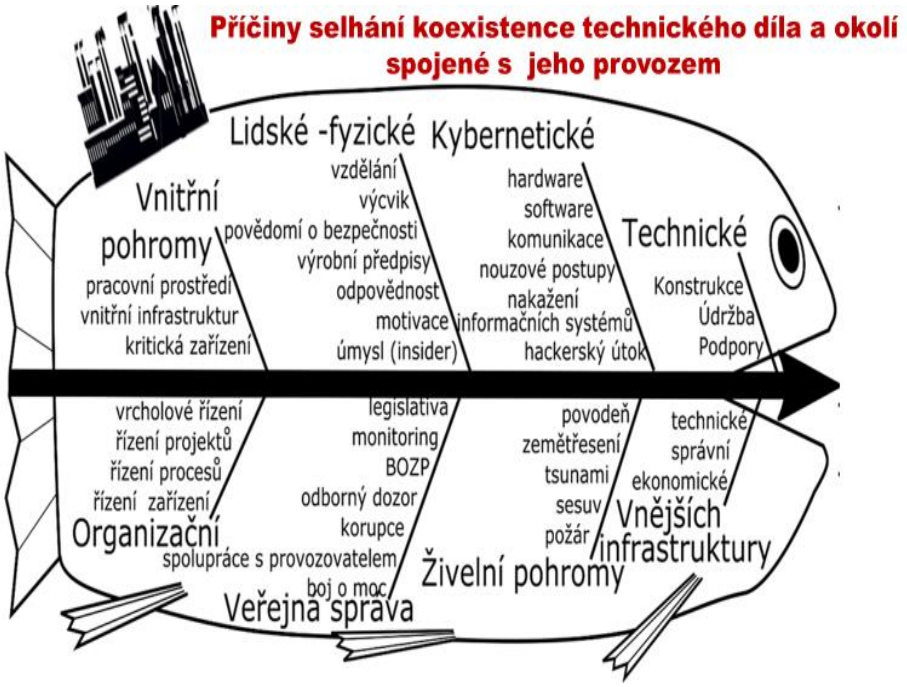
Dle práce [12] příklady oblastí vnitřních zdrojů rizik technických zařízení a technických děl, které vedly k selhání technických zařízení a technických děl, jsou uvedeny v tabulce 1.

Tabulka 1. Zdroje rizik technických zařízení a technických děl.

Kategorie pohrom (zdrojů rizik)	**Příklady vnitřních zdrojů rizik technických děl**
Technické	Specifické u zařízení – turbíny: mechanické, vibrace, stárnutí, zatížení atd.
Procesní	Vztahují se k výrobnímu procesu – úniky, výbušný nebo hořlavý materiál, prach, emise atd.
Pracovní činnost	Nebezpečné činnosti – práce ve výškách, řízení vozidel či bagrů, práce pod vodou, práce v osamocení atd.
Pracovní prostředí	Úprava podlahy – uklouznutí, zakopnutí a upadnutí; drsný povrch, horký / mrazivý povrch, stísněný prostor atd.
Vnější	Živelní pohromy, vnější havárie, pád letadla, teroristický útok.
Chování zaměstnanců	Nedodržování předpisů.
Organizační	Špatná organizace práce, velká pracovní zátěž, neadekvátní výcvik, špatné řízení změn.
Kontaminace v pracovním prostředí	Hluk, nebezpečné emise, kaluže, louže apod.
Finance	Výplaty, platby kontraktů, daně, dostupnost materiálu, řízení zásob apod.
Řízení projektů	Dostupnost lidských zdrojů, realizace projektu, řízení životnosti, řízení kontraktorů apod.

Na základě výzkumu založeného na analýze 7050 případů [16], jehož výsledky jsou shrnuté v pracích [1,12], příčiny selhání technických děl, které byly spojené s provozem, jsou uvedeny na obrázku 9. Z citovaného výzkumu vyplynulo, že hlavní zdroje rizik, které narušují koexistenci technického díla s okolím, byly především spojeny se způsobem a cílem řízení technického díla a jeho procesů, které probíhají v oblastech technických, organizačních, finančních, personálních a přes jejich rozhraní, a také se způsobem plnění odpovědností na straně veřejné správy. Důsledky příčin se projevily tím, že:

- došlo k selhání nebo havárii technického díla,
- technické dílo muselo být nákladně renovováno, aby splnilo požadavky na něho kladené či přestalo ohrožovat své okolí,
- bylo ztrátové a bylo brzy vyřazeno z provozu.



Obr. 9. Základní kategorie zdrojů rizik spojených s provozem technických děl, které vedou k selhání koexistence technického díla s okolím během jeho provozu.

Na základě analýzy dokumentací k haváriím a selháním technických děl použitých v práci [12] lze konstatovat, že velmi často dochází k havárii či selhání proto, že:

- dosud u složitých technických děl se používají zastaralé způsoby hodnocení rizik, např. stromové modely, které nezvažují souběhy jevů,
- provozovatel či vlastník je orientován hlavně na výkon (tj. zisk) a veřejná správa mu to dovoluje,
- personál, který je s příčinami a dopady rizik v kontaktu, nemá dostatečné kompetence pro zavedení proaktivních opatření a provozních předpisů přizpůsobených momentálním podmínkám (normálním, abnormálním, kritickým),
- technická rozhodnutí jsou poplatná různým partikulárním, politickým nebo ekonomickým tlakům a nepřihlížejí ke konkrétním rizikům, která se v průběhu provozu objevují.

Základními důvody, proč provozovatelé technických děl nejsou ochotni rizika řídit a řádně vypořádat, obvykle dle práce [15] jsou:
- nedostatečné povědomí o rizicích a jejich dopadech na technické dílo a jeho okolí,
- subjektivní pocity odpovědného subjektu, který nepovažuje riziko za aktuální,
- představa, že rizika se týkají vzdálené budoucnosti,
- kroky vedoucí k identifikaci rizika a jeho snížení jsou většinou v rozporu s okamžitými (většinou ekonomickými či politickými) zájmy provozovatele či vlastníka,
- konkrétní kompetentní pracovník většinou není tím, kdo o krocích vedoucích ke snížení rizika může přímo rozhodovat.

Nesprávné vypořádání rizik v technických dílech je způsobeno tím, že:
- rozhodovací procesy přímo v technických dílech bývají víceúrovňové. Na úrovni, kde lze reálně rozpoznat narůstající příznaky rizika a ocenit s tím související riziko, nelze rozhodnout o vynaložení vícenákladů na eliminaci tohoto rizika,
- je nedostatečné povědomí o rizicích, jejich řízení a vypořádání. Práce s riziky je chápána jako činnost, která spočívá v dodržení norem a předpisů, což není pravda, protože pravidla v nich zavedená pokrývají jen 68.4 % možných podmínek [20]; programy velké většiny vzdělávacích kurzů probíhajících v České republice tuto nedostatečnost ještě prohlubují,
- u inženýrů v provozu a jeho řízení je úzké chápání bezpečnosti; převládá orientace na technickou bezpečnost zařízení chápanou tak, že technické zařízení během životnosti nepředstavuje nebezpečí,
- je nedostatečná spolupráce profesí – stavařů, strojařů, ekonomů, chemiků, informatiků, personalistů atd. – každá profese pracuje odděleně, což neumožňuje řešit mezioborové a multioborové problémy,
- mnoho řídících pracovníků je přesvědčeno, že vše je věčné, tj. nezvažují změny technických zařízení v čase a se změnou podmínek, a tím podceňují údržbu, opravy, dovednost a dodržování režimů práce, které respektují fyzikální, chemické a biologické zákonitosti,

Poznatky získané studiem havárií a selhání technických děl [1,12] ukazují, že při prevenci havárií a selhání je třeba se vyvarovat:
- velkých chyb v prevenci rizik,
- a také výskytu drobných chyb, jejichž realizace v krátkém časovém intervalu je nebezpečná.

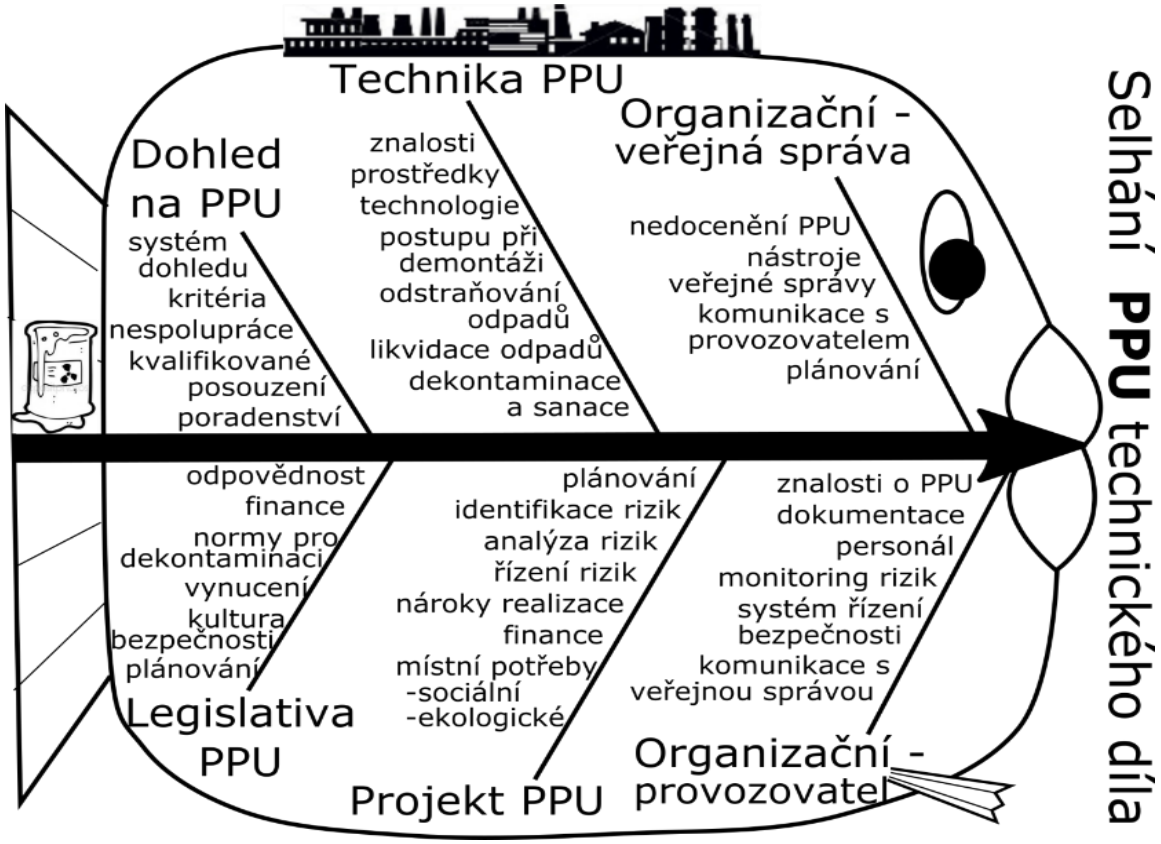
Druhá příčina je mnohem častější a je potvrzena řadou posledních havárií.

Seznam poznatků shromážděných v práci [12] i výzkum v citované práci popsaný ukazují, že nekvalitní údržba je jednou z příčin selhání a havárií (objevuje se u cca u 63%) a v řadě případů je příčinou klíčovou. Příčiny rizik technických zařízení a celých technických děl spojené s údržbou:
- neprováděná údržba,
- špatně prováděná údržba,
- nedostatečná údržba,
- špatný postup údržby,
- špatný rozvrh údržby,
- nedostatečně kvalifikovaný personál provádějící údržbu,
- nedostatečná preventivní údržba,
- chybí režim údržby a oprav, tj. neprovádí se kvalitní údržba a včasné opravy staveb, strojů a dalších zařízení s ohledem na stárnutí materiálů,

- velké opotřebení způsobené nároky na výkon či proměnné okolní podmínky bez odpovídající údržby
- apod.

3.4. Zdroje rizik při ukončení provozu technického díla a předávání zabraného území do dalšího užívání

Na základě výzkumu založeného na analýze 124 případů [16], jehož výsledky jsou shrnuté v práci [21], příčiny selhání technických děl, které byly spojené s ukončením provozu, demontáží, odvozem použitelných částí, odstraněním odpadů a procesem dekontaminace jsou uvedeny na obrázku 10.



Obr. 10. Příčiny selhání procesu PPU = procesu vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití.

Výsledky výzkumu ukázaly, že hlavní zdroje rizik, které narušují bezpečný proces likvidace technického díla po skončení jeho provozu a vyčištění území pro další využití byly především spojeny se znalostmi a chováním zhotovitelů a investorů a orgánů veřejné správy, které řídí území, povolují a dozorují technická díla v území. Důsledky příčin se projevily tím, že došlo k nežádoucí a nepřijatelné kontaminaci částí technického díla a území (a to někdy i dlouhodobému poškozování kvality životního prostředí).

Analýza některých konkrétních selhání procesu vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití ukázala, že:

- rozhodujícími faktory jsou znalosti a chování subjektů, které řídí, povolují a dozoruji technická díla v území po celou dobu jejich životního cyklu,
- při rozhodování nebyla zvážena existence podmínek transferu technologií [18]. De facto nebylo vzato v úvahu, že bezpečný proces vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití určují jak parametry technického díla vyřazeného z provozu, tak parametry prostředí, v němž činnosti probíhají.

3.5. Zdroje rizik technických děl používané v praxi

Na základě výsledků výzkumu popsaného v práci [2] se v praxi v souvislosti s technickými díly používají dále uvedené výběry zdrojů rizik ve spojení s určenou entitou (stroj, komponenta, výrobní linka apod.):

1. Zdroje rizik určené buď legislativou, anebo zkušenostmi pracovníka, který předmětný úkol řeší.
2. Jen technické zdroje rizik v dané entitě. 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 až 4 doplněné o zdroje rizik související s BOZP a s pracovním prostředím.
6. Zdroje rizik uvedené v bodech 2 až 5 doplněné o zdroje rizik v okolním životním prostředí.
7. Zdroje rizik uvedené v bodech 2 až 6 doplněné o zdroje rizik spojené s propojeními mezi dílčími zařízeními, komponentami a systémy. Jde o zdroje rizik, které jsou spojené s:
   - technickou integritou,
   - automatizací,
   - vzděláváním a dobrými dovednostmi,
   - ochranou majetku,

- ochranou dat a informací,
- ochranou specifických znalostí,
- ochranou know-how,
- ochranou good will,
- financemi,
- konkurenceschopností,
- kontinuitou provozu za podmínek kritických a extrémních apod.

Z uvedeného vyplývá, že v případech 1 až 6 jsou zanedbány mnohé zdroje rizik pro technická díla. Je to způsobeno skutečností, že v uvedených případech:

- při stanovení rizik nejsou zvažována všechna veřejná aktiva a všechna aktiva technického díla (tj. není respektován přístup All-Hazard-Approach [13,14], 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).

Z hlediska potřeb a ekonomického využití zdrojů je však pravdou, že v řadě praktických úloh postačuje zvažovat jen některé zdroje rizik, protože cílem je bezpečný stroj, a ne celý podnik a jeho okolí. Proto je třeba u každé úlohy spojené s prací s riziky důležité určení cíle řízení rizik.

Jelikož některá technická zařízení (pojišťovací ventily, odpouštěcí ventily apod.) či některé komponenty technického díla (tlaková zařízení, reaktory, řídicí systémy apod.) mají zásadní důležitost pro bezpečnost technického díla, tak u nich nestačí pracovat s riziky jen z hlediska samotné entity, ale musí se pracovat s riziky i z hlediska bezpečnosti celého technického díla). Jde o kritické prvky, kritická zařízení, kritické komponenty a kritické systémy technického díla, které vyžadují speciální práci s riziky.

4. METODICKÉ ASPEKTY PRÁCE S RIZIKY V INŽENÝRSKÝCH OBORECH

Z výše uvedeného plyne:
- důležitou roli pro zajištění bezpečného technického díla hraje řízení a vypořádání rizik [2],
- bezpečnost technických děl je dnes v odborných dokumentech a pracích chápaná jako vlastnost celého systému, ne jako vlastnost dílčích částí [2].

Práce s riziky technického díla zacílená na bezpečnost technického díla je ovlivněná řadou skutečností. Položky, které ovlivňují výsledek práce s riziky technického díla [2], jsou uvedeny na obrázku 11.

Obr. 11. Skutečnosti důležité pro bezpečné technické dílo.

V důsledku dynamického vývoje světa, tj. i technického díla, je třeba při práci s riziky technického díla ve prospěch bezpečnosti počítat nejen s náhodnými nejistotami, ale i s řadou znalostních nejistot. Proto nelze v řadě praktických úloh používat analytické metody, ale je třeba používat metody tvůrčího myšlení, jako jsou scénáře, metody rybí kosti, kontrolní seznamy aj. [3].

4.1. Řízení rizik

Řízení rizik je proces určení opatření a činností vedoucích k ochraně před riziky; člověk ho prováděl od samého počátku uvědomělého konání. V některých pojetích zahrnuje i vypořádání rizik, které je chápané jako realizace konkrétních opatření a činností.

Řízení rizik 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 a náklady na konkrétní opatření.

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 [2].

Snižování rizika je prakticky vždy spojeno se zvyšováním nákladů. Proto z hlediska praxe je řízení rizika 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 správná a úplná data a umíme využít nástroje, které máme k dispozici [2].

Při řízení rizik ve prospěch bezpečnosti rozlišujeme 2 zásadní postupy, a to: řízení bezpečnosti procesů; a řízení bezpečnosti technologických celků.

4.2. Řízení bezpečnosti procesů

Bezpečnost procesů je soubor opatření a činností, který zajišťuje bezpečný provoz, tj. bezpečný průběh procesů, např. v případě chemických procesů se zaměřují na prevenci požárů, výbuchů a úniků nebezpečných látek do životního prostředí [22]. Specifická disciplína řízení bezpečnosti procesů (PSM – Process Safety Management) se vyvíjí od 40. let minulého století a jejím cílem je zajistit bezpečné procesy, které probíhají v technologiích. Jde o řízení principů a systémů pro identifikaci možných ohrožení, pochopení a zvládnutí procesů vedoucích k realizaci rizik. Jedná se o složitý postup, který vyžaduje vícerozměrný přístup, který kombinuje technologie a jejich řízení [3].

Řízení bezpečnosti procesů je široce používáno v továrnách a dalších automatizovaných prostředích k zajištění efektivity výroby. Technologie řízení bezpečnosti procesů je obecně navržena tak, aby monitorovala senzory a nastavovala důležité veličiny podle naměřených hodnot. Tato technologie umožňuje relativně malé skupině lidí řídit

složité operace a pomáhá zajistit, aby bylo trvale dosaženo požadovaného výsledku. Řízení bezpečnosti procesů je spojeno s kulturou bezpečnosti a *pro hodnocení bezpečnosti se často používají kontrolní seznamy* [23]. Příklady hodnocení řízení bezpečnosti procesů pomocí kontrolních seznamů jsou v příloze 1.

4.3. Řízení bezpečnosti technických celků

Každý technický celek je systém, který se skládá z několika propojených systémů, tj. tvoří více či méně složitý systém systémů. *Bezpečnost systému* je soubor opatření a činností, který zajišťuje bezpečné technické dílo a jeho bezpečné okolí. Předmětná disciplína vznikla na základě systémového přístupu ve strojírenských oborech. Integrální (celková, objektová) bezpečnost má své kořeny v inženýrství bezpečnosti průmyslu, které sahá až do 19. století a které po 2. světové válce aplikovalo disciplíny:
- systémové inženýrství
- a systémovou analýzu

k řešení nových a složitých inženýrských problémů.

V daném případě je bezpečnost chápaná jako vlastnost, která vystupuje na úrovni systému, když jsou komponenty provozovány společně. Události vedoucí k nehodě jsou pak složitou kombinací chyb zařízení, nesprávné údržby, problémů s informačním a řídicím systémem, lidského zásahu a konstrukčních chyb [24].

Bezpečnost systému ve sledovaném pojetí spočívá v aplikaci technických a manažerských dovedností při identifikaci, analýze, hodnocení a řízení škodlivých jevů a souvisejících rizik pomocí systémového přístupu [1,2,12]. Z praktických důvodů musí být přístupy používané ve sledované oblasti účinné a cenově dostupné. Orientace na bezpečnost musí být součástí systému řízení podniku a zároveň musí respektovat omezení, která vyplývají z vnějšího světa. Musí zvažovat dynamický vývoj světa, a proto práce s riziky vyžaduje schopnost předvídání jevů, které lze očekávat na základě zkušeností a dosavadních znalostí [25].

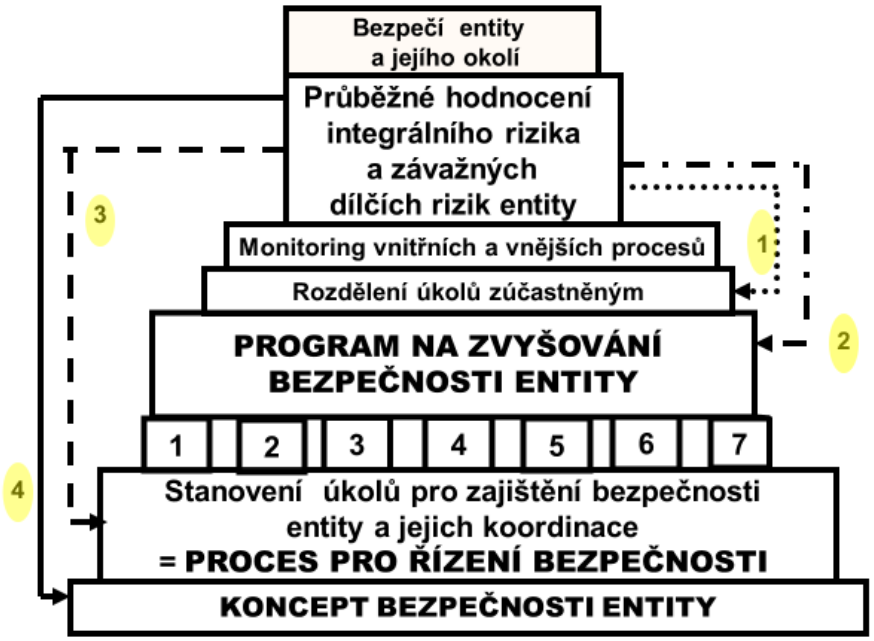
Bezpečnost systému aplikovaná na technická díla využívá teorii systémů a systémové inženýrství k prevenci předvídatelných nehod a k minimalizaci následků nepředvídatelných nehod. V moderním pojetí se obecně zajímá o všechny ztráty a škody, a to nejen o smrtelné nehody nebo zranění a škody na majetku, ale také o nesplnění poslání (mise, účelu) nebo poškození životního prostředí. Klíčovým bodem disciplíny je považovat ztráty za natolik závažné, aby se na jejich prevenci věnoval dostatek času, úsilí a zdrojů. Výše investic věnovaných na prevenci nehod a/nebo jejich dopadů do značné míry závisí na sociálních, politických a ekonomických faktorech. Proto u technologií, které mohou mít vážné důsledky, je požadavek předběžné opatrnosti uložen právními předpisy, aby byla zajištěna ochrana veřejných aktiv [12].

Řízení bezpečnosti technických celků je používáno při řízení technologických celků, celých továren, elektráren atd. [24]. Dnes jde o integrované řízení 7 procesů (obrázek 12) [26]:

1. Proces pro návrh a realizaci koncepce a řízení technického celku, který je dále rozdělen do dílčích procesů, které zajišťují:
   - celkovou koncepci bezpečnosti technického celku,

- plnění dílčích cílů bezpečnosti technického celku,
- řízení/správu bezpečnosti technického celku,
- systém řízení bezpečnosti technického celku,
- zaměstnance technického celku, což se dále dělí na procesy:
  - řízení lidských zdrojů technického celku,
  - školení a vzdělávání zaměstnanců technického celku,
  - interní komunikace/povědomí v technickém celku
  - a pracovní prostředí technického celku,
- přezkoumání a hodnocení plnění cílů bezpečnosti technického celku.

2. Proces provádění administrativních postupů v technickém celku, který se dále dělí na dílčí procesy, které zajišťují:
   - identifikace ohrožení technického celku od možných pohrom (škodlivých jevů všeho druhu) a hodnocení rizik s nimi spojených,
   - administrativní postupy (včetně systémů pracovního povolení) v technickém celku,
   - řízení změn v technickém celku,
   - bezpečnost technického celku při spolupráci s dodavateli,
   - dohled nad bezpečností výrobků či služeb technického celku.
   -



Obr. 12. Procesní model řízení bezpečnosti entity v čase. Procesy: 1- koncepce a řízení; 2 - administrativní po-stupy;3 - technické záležitosti (technická problematika entity a jejího okolí); 4 - vnější spolupráce; 5 - nouzová připravenost; 6 - dokumentace a šetření havárií; a 7 - zabezpečení entity – zpracováno dle [24].

3. Proces pro zajištění technických záležitostí v technickém celku, který je dále rozdělen do dílčích procesů, které zajišťují:
   - výzkum a vývoj technického celku,
   - projektování a montáže v technickém celku,
   - inherentně bezpečné procesy v technickém celku,
   - průmyslové normy a technické standardy v technickém celku,

- skladování nebezpečných látek v technickém celku,
- údržbu integrity a údržbu zařízení a objektů v technickém celku.

4. Proces pro zajištění externí spolupráce technického celku, který se dále dělí na dílčí procesy, které zajišťují:
   - spolupráci technického celku se správními orgány.
   - spolupráci technického celku s veřejností a dalšími zúčastněnými stranami (včetně akademických pracovišť),
   - spolupráci technického celku s jinými podniky.
5. Proces havarijní připravenosti a odezvy na havárie a nehody technického celku, který se dále dělí na dílčí procesy, které zajišťují:
   - plánování připravenosti technického celku na odezvu na havárie a nehody uvnitř technického díla,
   - usnadnění plánování připravenosti na odezvu vně technického díla (které spadá do odpovědnosti veřejné správy) při havárii či nehodě technického díla,
   - koordinaci činností resortních organizací při zajišťování havarijní připravenosti a odezvy.
6. Proces zpracování hlášení a vyšetřování havárií/skoronehod v technickém celku, který se dále dělí na procesy, které zajišťují:
   - zpracování zpráv o haváriích, nehodách, skoronehodách a dalších významných zkušenostech v technickém celku,
   - vyšetřování škod, ztrát a újmy a jejich příčin při nežádoucích jevech v technickém celku,
   - dokumentaci o odezvě na havárie a nehody a následných opatření (včetně uplatňování získaných zkušeností a sdílení informací) v technickém celku.
7. Proces pro zajištění fyzické a kybernetické bezpečnosti technického zařízení, který se dále dělí na dílčí procesy pro zajištění:
   - fyzické bezpečnosti,
   - kybernetické bezpečnosti proti hackerům.

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 12 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 12. 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 dle poznatků shrnutých v práci [2] běžně používají v integrovaném řízení procesů. V řadě případů jsou role a z nich vyplývající odpovědnosti 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,

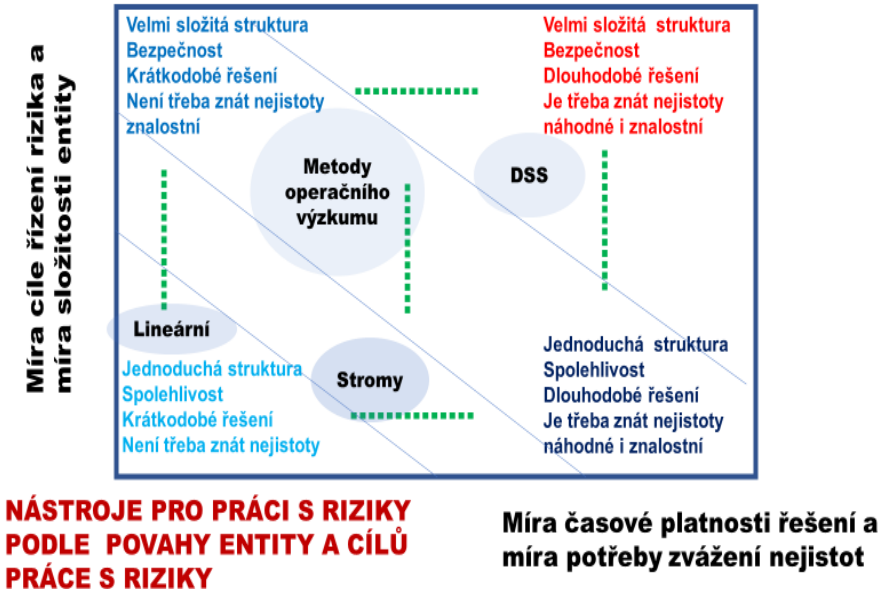
- zavést a cíleně prosazovat „kulturu bezpečnosti“, která je respektována a prosazována všemi zúčastněnými za všech okolností,
- ustanovit systémy řízení bezpečnosti, sledovat a popř. korigovat jejich činnost,
- používat principy inherentní bezpečnosti při navrhování, projektování, výstavbě a provozování 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.

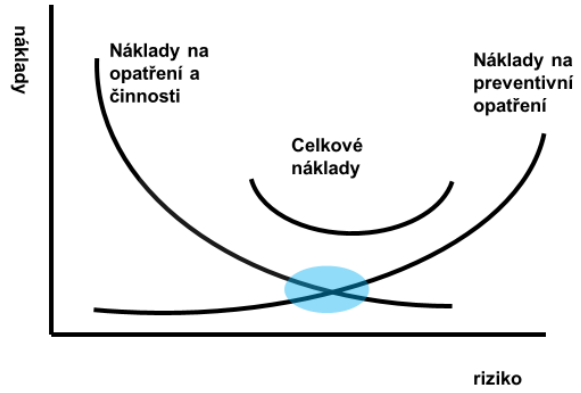
Inženýrství orientované na bezpečnost celku cíleně provádí úkoly řízení bezpečnosti, tj. úkoly řízení rizik ve prospěch bezpečnosti a vývoje lidského systému. V technickém slangu hovoříme o vytváření inherentní bezpečnosti technického díla proti projektovým pohromám pomocí řízení bezpečnosti. Při uplatňování zásady předběžné opatrnosti zajišťujeme zvýšení odolnosti vůči nepřijatelným dopadům nadprojektových pohrom, jejichž výskyt je tak nepravděpodobný, že je nepředvídatelný. Do praxe se v technologiích na základě zmíněných cílů zavádí principy jako „selži bezpečně“, „prováděj jen určené funkce, tj. když nemůžeš splnit cíl, tak nic nedělej“ apod. [12].

Při práci s riziky ve prospěch bezpečnosti u technologických celků se používají složitější metody [2]; obrázek 13 [27].



Obr. 13. Rozložení nástrojů řízení rizik ve prospěch bezpečnosti v závislosti na cílech a složitosti entity.

Vzhledem k tomu, že zdroje každé entity jsou omezené, je třeba porovnávat náklady na snížení rizika a náklady na nutná opatření, tj. jde o aplikaci metody CBA [28] s vyhověním požadavkům na bezpečnost; obrázek 14.



Obr. 14. Interval celkových nákladů, ve kterém je zajištěna bezpečnost; oblast optimálních nákladů je vyznačena modře; zpracováno dle [27].

U důležitých technických děl jde v praxi nejen o bezpečnost, ale i o výkonnost [30], protože je tak může být technologický celek konkurenceschopný. To znamená, že technologický celek musí mít velkou resilienci (houževnatost), tj. schopnost udržet si i v náročných situacích vnitřní kontinuitu, která zajišťuje požadovanou výkonnost, což vyžaduje rychle se zotavit z nouzových situací, které entitu postihnou. Proto v dynamicky proměnném světě používáme kontinuální řízení rizik ve prospěch bezpečnosti a výkonnosti [29,30]. V inženýrských disciplínách sleduje několik druhů resilience (houževnatosti):

- v inženýrství a stavebnictví jde o vytvoření schopnosti budov a infrastruktury absorbovat dopady pohrom a útoky, aniž by došlo k úplnému selhání,
- v energetice jde o vytvoření schopnosti energetických zdrojů a energetických sítí absorbovat dopady pohrom a útoky, aniž by došlo k úplnému selhání,
- v nauce o materiálech jde o vytvoření schopnosti materiálu absorbovat energii při deformaci a uvolnit tuto energii při odstranění zatížení,
- u počítačové sítě jde o vytvoření schopnosti počítačové sítě udržovat službu tváří v tvář poruchám,
- v lidských sídlech jde o vytvoření schopnosti zajistit základní funkce pro obyvatele v minimálním rozsahu, který zajistí přežití lidí,
- v oblasti informační bezpečnosti jde o vytvoření schopnosti kybernetické sítě zajistit základní propojení, která jsou nutná pro základní funkce v lidské společnosti.
- v oblasti řídicích systémů jde o jde o vytvoření schopnosti řídicích systémů vytvářet kognitivní, kyberneticko-fyzickou houževnatost vůči hrozbám.

5. METODIKY ŘÍZENÍ A VYPOŘÁDÁNÍ RIZIK TECHNICKÝCH CELKŮ VE PROSPĚCH BEZPEČNOSTI

Dle poznatků shrnutých v práci [2], klíčové koncepty řízení rizik zacíleného 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.

Položky, které ovlivňují výsledek práce s riziky technického díla, jsou zobrazeny na obrázku 11.

V ideálním případě inženýři zabývající se bezpečností zvažují první návrh systému zařízení nebo technického díla, analyzují jej, aby zjistili, jaké poruchy se mohou vyskytnout, a poté navrhnou požadavky na bezpečnost, které musí být specifikovány v konstrukčních specifikacích a změny v návrhu s cílem zvýšit bezpečnost. To znamená, že *řízení rizik ve prospěch bezpečnosti se v technice provádí od umísťování přes projektování až po ukončení provozu sledovaného objektu*, a to u procesů i objektů [26]. Postupy se běžně označují jako:

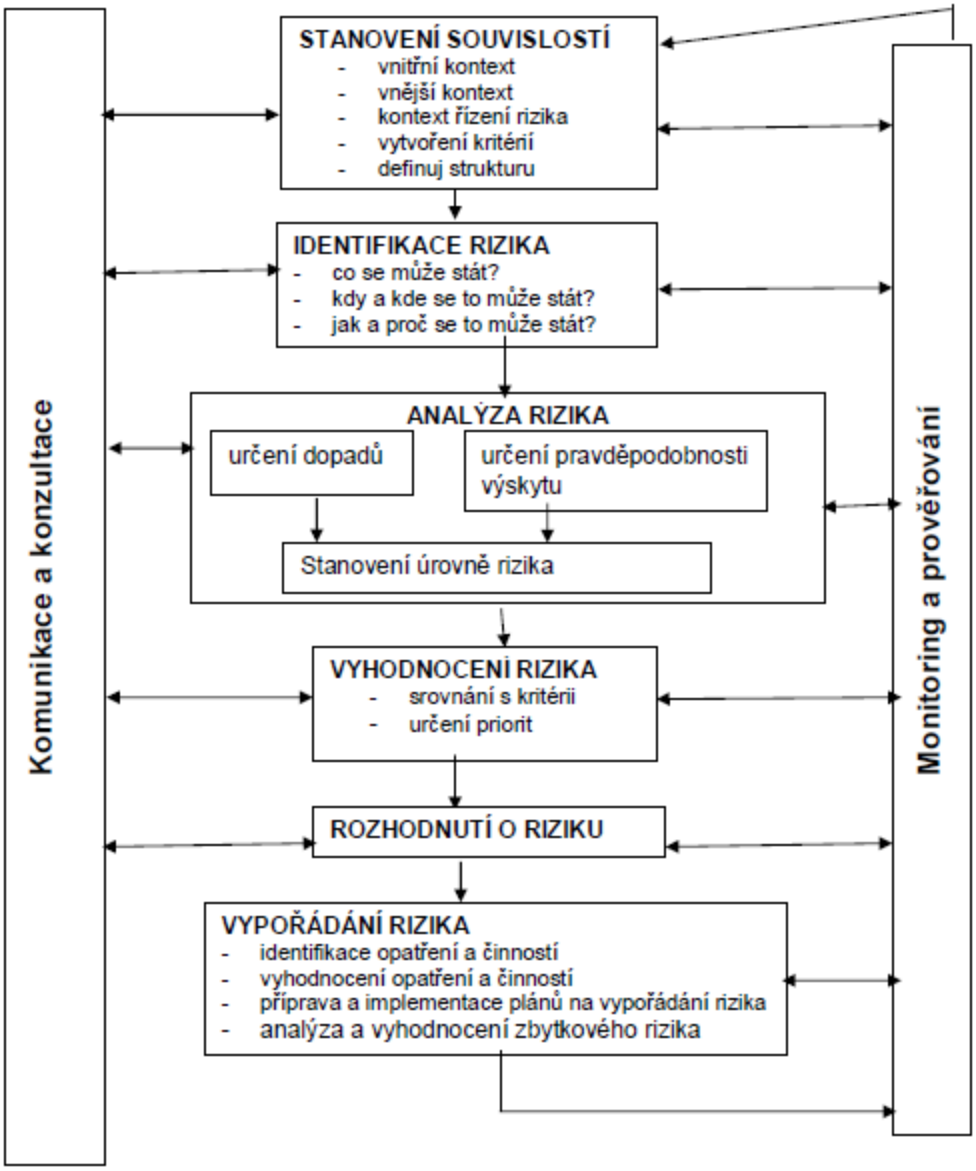
- risk based design,
- risk based operation,
- risk based maintenance
- apod.

Při řízení rizik ve prospěch bezpečnosti se používá řetěz bezpečnosti, obrázek 15.

Obr. 15 Činnosti pro zajištění bezpečnosti sledovaného systému.

5.1. Postup řízení rizik dle norem

Logika postupu řízení rizik dle normy ISO 31000 je zobrazena na obrázku 16.



Obr. 16. Postup řízení rizik dle ISO 31 000.

Norma ČSN ISO 31000 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. 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 dle poznatků shrnutých v práci [2] 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.
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. Stanovení odpovědnosti za opatření a činnosti spojené s řízením rizik.
4. Zdroje nutné pro řízení rizik včetně znalostí, dovedností, zkušeností a kompetencí.
5. Stanovení mechanismů pro interní komunikaci a podávání zpráv o rizicích a jejich zvládání.
6. Stanovení mechanismů pro externí komunikaci a podávání zpráv o rizicích a jejich zvládání.

Pro implementaci opatření a činností, které vyplynou z procesu 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 rizik znamená kritické studium kauzálního vztahu příčiny – dopady. Hodnocení rizik znamená porovnání úrovní rizik získaných analýzou rizik s kritérii pro posuzování rizik. Hodnocení rizik technického díla z pohledu prevence, připravenosti, odezvy a obnovy musí obsahovat:
- identifikaci ohrožení technického díla,
- specifikaci jevů (nebo scénářů), které ohrožují technické dílo,
- četnosti výskytu jevů (nebo scénářů), které ohrožují technické dílo,
- odhad dopadů jevů, které ohrožují technické dílo a ve kterých je zahrnuto i působení místních zranitelností,
- odhad míry/velikosti rizika z kombinace důsledků jevů (nebo scénářů), které technické dílo ohrožují a četností jejich výskytu,
- posouzení rizika technického díla pro potřeby rozhodnutí,
- standardy a normy pro regulaci projektování a provozování technického díla,
- postupy a systémy řízení bezpečnosti
- a popř. další.

Pro zajištění bezpečnosti technického díla je důležité:
- jakým způsobem jsou cíle řízení rizika nastaveny, zda: cíle týkající se úrovně rizika jsou kvalitativní nebo kvantitativní,
- jak cíle řízení rizika splňují technické standardy,
- zda standardy řízení rizik technického díla jsou systémové.

Zvládání / vypořádání rizik znamená v případě, že riziko technického díla 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.

Je logické, že 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) [2]. 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.

Podle poznatků a zkušeností shrnutých v práci [2], při řízení rizik hrají roli:

- cíle řízení rizik, tj. požadovaná úroveň bezpečnosti,
- metody a postupy k dosažení stanoveného cíle,
- kompetence institucí a osob, které rozhodují o opatřeních a financích potřebných na opatření pro zmírnění rizik,
- požadavky norem a standardů, které stanoví legislativa,
- a limity (znalostní, finanční, materiálové a popř. i jiné), které je nutné zvažovat v praxi.

Protože, jak již bylo výše uvedeno, nikdy není dostatek zdrojů, sil a prostředků, tak se v inženýrské praxi orientujeme jen na kritické atributy, tj. jen na kritické položky a nepřijatelná a podmíněně přijatelná rizika, která označujeme ALARA / ALARP. Používáme ISO normy založené na projektovém řízení typu TQM (Total Quality Management) [9], tj. normy řady ISO 9 000, 14 000, 18 000, 31 000, 31010 aj. Příklad dalších je v tabulce 2.

Tabulka 2. Příklady norem podporujících zajištění bezpečnosti technických zařízení.

Značka	**Oblast**
EN/ISO 12100	Bezpečnost strojních zařízení
EN/ISO 13849	Bezpečnost strojních zařízení - bezpečnostní části ovládacích systémů
EN/ISO 13855	Bezpečnost strojních zařízení - umístění ochranných zařízení ..
EN/ISO 13850	Bezpečnost strojních zařízení – funkce nouzového zastavení
EN/ISO 14120	Bezpečnost strojních zařízení – ochranné kryty
EN/ISO 10218	Roboty a robotická zařízení - Požadavky na bezpečnost
ISO/IEC 27000	Informační technologie - bezpečnostní techniky - systémy řízení bezpečnosti informací
ISO/IEC 15408	Informační technologie - bezpečnostní techniky - kritéria pro hodnocení bezpečnosti IT
IEC 62443	Průmyslová kybernetická bezpečnost
EN 61508	Funkční bezpečnost řídicích systémů. Harmonizovaná je pouze její sektorová norma EN 62061.
ISO 26262	Funkční bezpečnost elektrických a elektronických systémů ve vozidlech
IEC 62 443	Zabezpečení automatizovaných průmyslových a řídicích systémů
IEC 61511	Funkční bezpečnost v průmyslu
IEC 61513	Bezpečnost v jaderné energetice
ISO/DIS 26262	Funkční bezpečnost v automotive
IEC 60601	Bezpečnost v medicíně
IEC 80001	Bezpečnost v medicíně
CENELEC EN 50126	Bezpečnost železnice
CENELEC EN 50128	Bezpečnost železnice
CENELEC EN 50129	Bezpečnost železnice

CENELEC EN 50159	Bezpečnost železnice
MIL-STD-882E	Bezpečnost systémů / produktů / zařízení / infrastruktur (hardware i software) po celou dobu existence – od návrhu, vývoje, testování, výroby, používání a likvidace.

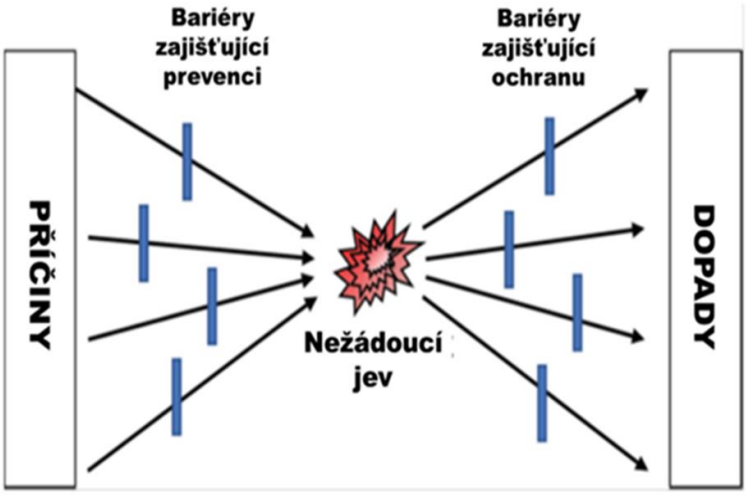
5.2. Instrukce pro provedení řízení a vypořádání rizik technického díla

Instrukce pro provedení řízení a vypořádání rizik technického díla dle poznatků a zkušeností shrnutých v práci [2] zahrnují:

1. Identifikaci rizik dle principu All-Hazard-Approach [13,14]. Dle [1,2,12,19] je třeba u technických celků sledovat zdroje rizik:
   - chyby v řízení a ovládání entity (procesu /objektu/zařízení/systému/komponenty),
   - vnitřní zdroje rizik entity spojené s jejím projektem, konstrukcí, jejími propojeními a provozem, nově do této kategorie patří i vložení padělaných kritických součástí do technického díla [30],
   - chyby personálu obsluhy entity při provozu,
   - vnější zdroje rizik entity spojené s živelními pohromami,
   - vnější zdroje rizik entit spojené se selháním okolních entit a procesů (vazby a toky) – např. selhání dodávek elektřiny, vody, chladiva, dodávek materiálu, dopravy atd.,
   - vnější zdroje rizik entity spojené s chováním veřejné správy (daně, poplatky, pobídky apod.), konkurencí, trhem apod.,
   - útoky na entitu,
   - kybernetické zdroje rizik spojené s automatizací a komunikacemi uvnitř i vně entity,
   - válka,
   - chybný dozor veřejné správy.
2. Určení rizik a jejich klasifikace dle [2,9,12,19] na:
   - seznam vyhodnocených rizik,
   - seznam rizik vyžadujících nejvyšší pozornost
   - a seznam neaktuálních/vyřešených rizik.
3. Rozdělení rizik vyžadujících pozornost při provozu [1,12,19] dle postupu na obrázku 17 takto:
   - rizika, která se eliminují preventivními opatřeními v projektu,
   - rizika, která se zmírňují odezvou při provozu a pro která musí být vložena v projektu technická opatření, která umožňují kvalitní odezvu.

   Um projektanta spočívá ve správném rozdělení rizik.
4. Vytvoření projektu:
   - zohlednění rozdělení rizik v bodě 3,
   - aplikace principů inherentní bezpečnosti,
   - aplikace principu ochrany do hloubky (obrázek 5),
   - návrh požadavků pro provoz a údržbu při provozu.

5. Provoz:
   - dle požadavků bezpečnostní zprávy a provozních předpisů, které respektují požadavky projektu,
   - monitoring provozu a řízení rizik výrobních a dalších procesů včetně údržby v čase [24,26] - obrázek 12. Při údržbě spojené s výměnou kritických položek je třeba zohlednit požadavky ochrany před padělky [31],
   - zpracování plánu řízení rizik při provozu (ISO 31000) pro případ selhání zařízení nebo procesu v entitě.



Obr. 17. Rozdělení rizik na ta, která se zvládnou preventivními opatřeními vloženými do projektu a na ta, pro která do projektu musí být vložena technická opatření, která umožní kvalifikovanou odezvu [19].

Plán řízení rizik je nástroj proaktivního řízení rizik. V inženýrské praxi se zaměřuje pouze na kritické atributy, tj. pouze na nepřijatelná a podmíněně přijatelná rizika (ALARA/ALARP) [1,12]. Přijatelnost souvisí s veřejným zájmem, kterým je bezpečná kritická infrastruktura, která zajišťuje základní funkce státu, tj. její bezpečné objekty a jejich bezpečná propojení. Plán řízení rizik je vypracován ve formě tabulky, která obsahuje: příčiny rizika; popis dopadů rizik na veřejný majetek a služby poskytované danou entitou; četnost výskytu poruch a velikost dopadů selhání dané entity stanovené na základě místní databáze příčin selhání sledované entity; a zajištění odezvy na realizaci rizika:

- řízení rizik nebo alespoň jasně stanovená zmírňující opatření. Jde o opatření:
  - technická,
  - organizační,
  - personální,
  - metodická,
  - vzdělávací
  - a finanční,
- pro každou akci, je určena osoba fyzická nebo právnická (nebo její odpovědný zástupce), která zajistí odezvu,
- u každé akce je uvedena osoba odpovědná za správné a včasné provedení odezvy.

Plán řízení rizik je osvědčeným strategickým nástrojem, který se ve vyspělých zemích používá k udržení a zvýšení bezpečnosti zařízení, objektů, organizací a celých technických děl. Používá se k řízení prioritních rizik způsobených přírodními pohromami, technologickými haváriemi a poruchami, jakož i lidského faktoru tak, aby se:

- zvýšilo bezpečí lidí a technického díla či technického zařízení samotného (příklady jsou v příloze 2; generické modely pro jednotlivé cykly životnosti technického díla jsou v pracích [12,17,19,21]),
- zlepšily služby technického díla pro region, které jsou důležité pro životní podmínky lidí,
- podporoval rozvoj a konkurenceschopnost regionů
- a zlepšila ochrana životního prostředí.

5.3. Postupy řízení rizik u složitých systémů

Při řízení objektů, které jsou složitými systémy, se používají organizační struktury, postupy a pravidla, které ovlivňují výkon a kvalitu práce lidí (výrobky či služby, údržbu, renovace i změny). Významnými faktory dle [1] jsou:

- odpovědnost a rozumná autonomie,
- adaptabilita a celistvost
- a smysluplnost úkolů.

Řízení rizik ve prospěch bezpečnosti technických objektů řeší otázky, týkající se:

- materiálu,
- technologií,
- konstrukce,
- výstavby,
- provozu,
- personálu,
- organizace plnění úkolů,
- BOZP,
- vzdělávání,
- financí
- a práva tak.

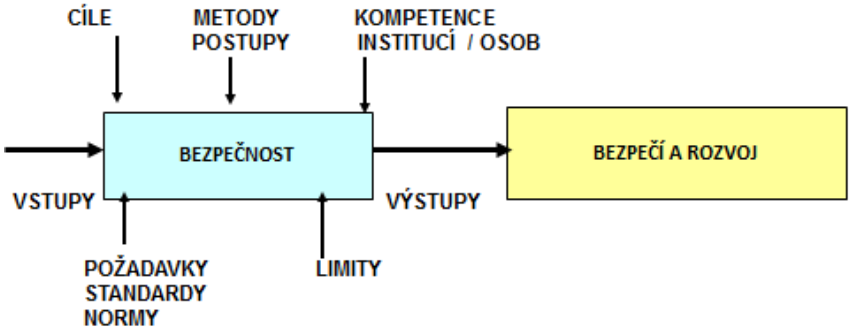
Cílem řešení problémů je zajistit žádoucí procesy, které:

- provozovateli technického díla přináší zisk,
- zajišťují soulad se státem,
- konkurenceschopnost
- a zároveň potlačují procesy, které přináší provozovateli technického díla i občanům škody a ztráty.

Model vytváření bezpečnosti je na obrázku 18.

Strategie řízení bezpečnosti [1] představuje ucelenou sadu standardních, prakticky ověřených kroků a nástrojů k řízení změn a zároveň i samotný proces řízení předmětných změn. Vychází z poznání, že zvládnutí jakéhokoliv netriviálního procesu v systému není dílem okamžiku, ale je výsledkem zaměřeného působení souboru opatření a činností aplikovaných v prostoru a čase. Zahrnuje přesné určení žádoucího směru

změn, stanovení přesného postupu jejich zavedení a průběžné sledování a vyhodnocování jejich průběhu a výsledků.



Obr. 18. Procesní model vytváření aktuální bezpečnosti technického díla a důležité faktory, které ovlivňují proces.

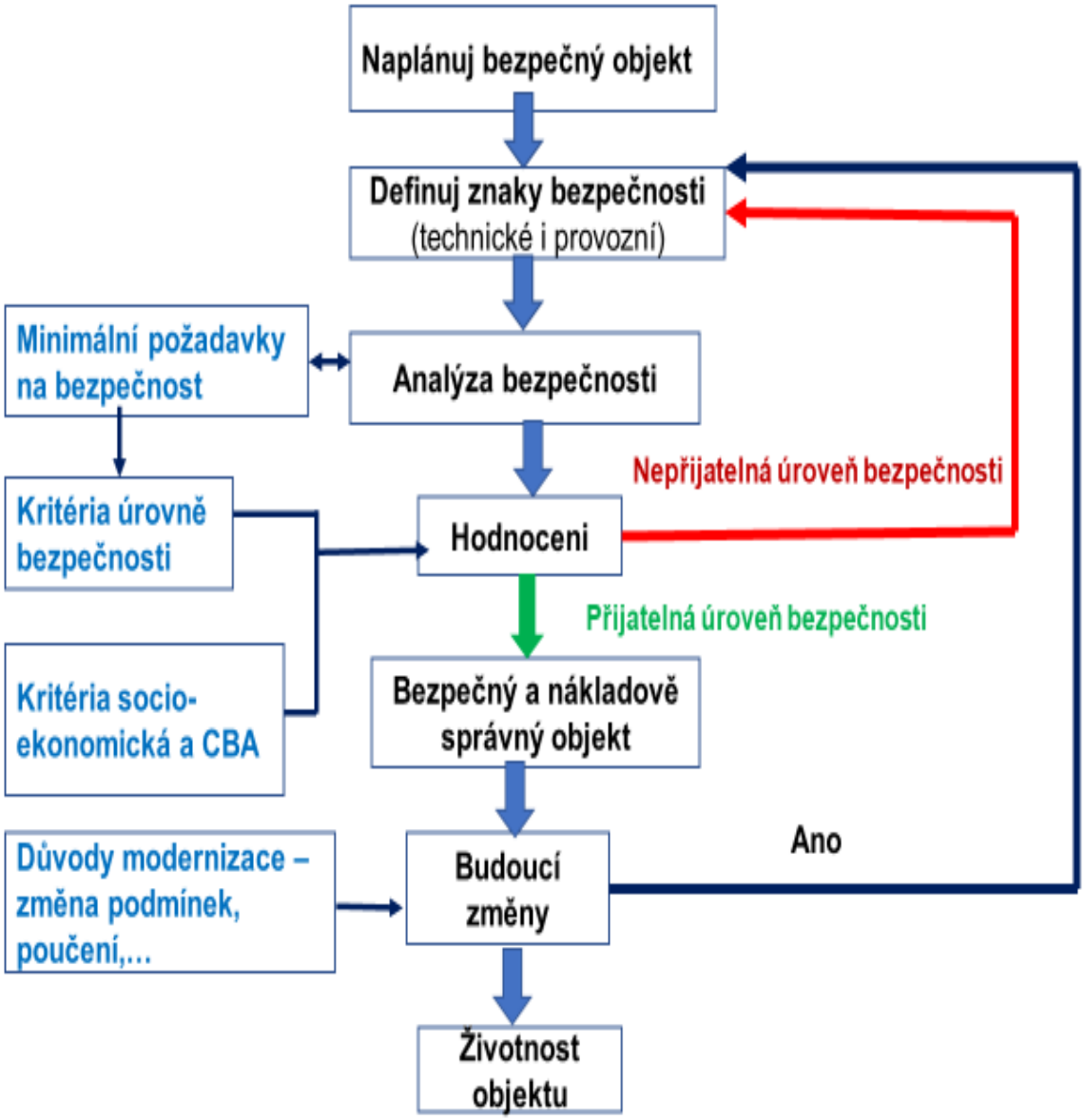
Strategické plánování je její nástroj, který se zaměřuje na to, aby řídící subjekt mobilizoval a co nejefektivněji využíval všechny vlastní zdroje, síly a prostředky, a včas a správně reagoval na změny v okolním prostředí. Dle něho řízení bezpečnosti musí:

- být založeno na znalostech o chování složitých systémů v dynamicky proměnném světě,
- být vždy zaměřeno na podstatné aspekty, tj. zajišťovat udržitelný a prozíravý rozvoj životně důležitých infrastruktur, což znamená zajištění rovnováhy mezi ekonomikou, životním prostředím a sociální oblastí, a také se soustředit na snižování zranitelnosti a zvyšování odolnosti,
- ***věnovat pozornost tomu, co je nejzranitelnější***. Systém odezvy na selhání životně důležitých infrastruktur se musí zaměřit na potřeby a priority. Základní prioritou je ochrana lidí a ochrana kritických zdrojů a systémů, na nichž závisí existence komunity,
- podporovat kulturu prevence,
- zabránit organizačním haváriím způsobeným špatnou kulturou bezpečnosti, především na úrovni vrcholového managementu (podle ESRIA „odborná komise EU pro řešení problémů kritické infrastruktury“ jde i o nesprávná rozhodnutí managementu, která vedou k nedostatečné údržbě, nedostatečné kvalitě oprav apod.),
- ***mít programy pro prevenci a zajištění připravenosti na zvládnutí selhání životně důležitých objektů infrastruktur, které musí být součástí programu rozvoje území,***
- respektovat právo občanů na spravedlivou pomoc (asistenční službu) při selhání životně důležitých infrastruktur. Pomoc se musí poskytovat spravedlivě a konzistentně bez ohledu na ekonomické a sociální okolnosti a územní lokalizaci,
- zajistit, že občané budou znát ***nouzové plány a plány odezvy na selhání životně důležitých objektů infrastruktur, a budou vědět, co obsahují, jaká je jejich role a odpovědnost, jak mohou napomoci v prevenci selhání životně důležitých***

infrastruktur, jak by měli reagovat, a proč, při vzniku selhání životně důležité infrastruktury apod.

- zajistit odezvu na selhání životně důležitých objektů infrastruktur, která je transparentní i pro občany a je přizpůsobena místním podmínkám,
- zajistit legitimitu, udržitelnost, přijatelnost a systémovost odezvy.

Postup strategického plánování bezpečného objektu po celou dobu životnosti, sestavený na základě současného poznání [1,19] je zobrazen na obrázku 19. Analogicky se strategicky plánuje bezpečný proces.



Obr. 19. Postup strategického plánování bezpečného objektu.

Na základě současného poznání shrnutého v práci [1] je třeba řídit rizika optimálním způsobem, to znamená, že je třeba u sledovaného objektu:

- 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,
- rozdělit odpovědnosti a příslušné kompetence ke všem důležitým úkonům a procesům.

Rozdělení kompetencí a odpovědností při řízení rizik i řízení bezpečnosti je zásadní a důležité v každé složitější činnosti lidské společnosti i u každého složitějšího technického díla. Za bezpečnost technického díla odpovídají vlastníci a provozovatelé, ale i veřejná správa, která musí provádět dohled nad bezpečností technického díla ve veřejném zájmu.

Při stanovení úrovně bezpečnosti položky se obvykle používá verbální stupnice obsahující stupně „velmi dobrý“ až do stupně „špatný“, a „kritický (tj. velmi špatný) [20]. Vhodné je použít pětistupňovou stupnici:

1. Velmi dobrý stav:
   - položka je v bezvadném fyzickém stavu a plní zamyšlené funkce,
   - náklady na údržbu jsou v souladu se standardy a normami,
   - nároky na provoz odpovídají projektu,
   - provozní problémy nejsou.

   Míra bezpečnosti velmi vysoká.
2. Dobrý stav:
   - položka je fyzicky v dobrém stavu a plní zamyšlené funkce,
   - náklady na údržbu jsou v souladu se standardy a normami, ale rostou,
   - položka je asi v polovině své životnosti,
   - nároky na provoz odpovídají projektu, provozní problémy jsou jen občas.

   Míra bezpečnosti je vysoká,
3. Přijatelný stav:
   - položka vykazuje známky opotřebení a nižší výkonnosti než je zamyšlená,
   - některé části jsou nedostatečné,
   - náklady na údržbu překračují částky stanovené standardy a normami a rostou,
   - položka byla dlouho používána a je v poslední fázi své životnosti,
   - nároky na provoz odpovídají projektu, provozní problémy jsou časté.

   Míra bezpečnosti je střední.
4. Špatný stav:
   - položka vykazuje významné známky opotřebení a plní zamyšlené funkce na nízké úrovni,
   - mnoho částí je nedostatečných,
   - náklady na údržbu významně přesahují částky ze standardů a norem,
   - položka se blíží ke konci své životnosti,
   - nároky na provoz přesahují údaje v projektu, provozní problémy jsou zřejmé.

   Míra bezpečnosti je malá.
5. Kritický stav:

- položka je ve špatném stavu a nepracuje tak, jak by měla,

- je vysoká pravděpodobnost jejího selhání,
- náklady na údržbu jsou vysoce nepřijatelné ve srovnání se standardy a normami,
- rekonstrukce není nákladově efektivní,
- je nutná výměna položky,
- nároky na provoz jsou výrazně vyšší než projektové,
- provozní problémy jsou vážné a trvalé.

Míra bezpečnosti je zanedbatelná.

Práce s riziky v rámci řízení bezpečnosti objektů pokrývá několik okruhů [1,12,19] :
- bezpečnost procesů,
- ochrana zdraví a bezpečnost zaměstnanců (bezpečnost práce)
- a omezování vlivů na životní prostředí.

Proto se do praxe zavedlo, že analýza dopadů řízení na bezpečnost podniku se provádí dle Reasonova modelu organizační havárie [32]. Příčiny organizační havárie se hledají ve třech základních aspektech:
- organizační procesy,
- podmínky, které působí vznik chyb nebo porušení předpisů,
- neřešené problémy, které dovolují chyby a/nebo porušení předpisů.

Strategie pro zajištění bezpečí a udržitelného rozvoje technického objektu či technického zařízení dle [1] spočívá v:
- aplikaci systémového a pro-aktivního řízení, které se opírá o znalosti a zkušenosti získané pro objekt z kvalifikovaných dat,
- kvalifikovaném vyjednávání s riziky ve prospěch bezpečí a udržitelného rozvoje objektu,
- vypořádání rizik pomocí prevence, zmírnění, pojištění, rezervy, připravenosti na odezvu a obnovu a sestavení plánu na zvládnutí nepředvídaných situací (contingency plan),
- aplikaci správného řízení, ve kterém jsou provázané řízení bezpečnosti, nouzové řízení a krizové řízení,
- sestavení programu na zvyšování bezpečnosti,
- stanovení měr na posuzování úrovně bezpečnosti ve smyslu účinnosti bezpečnostního systému (indikátory),
- naplnění programu na zvyšování bezpečnosti provázanými projekty + naplnění projektů provázanými procesy,
- adresném přidělení úkolů a odpovědností všem zúčastněným,
- realizaci příslušných činností a opatření, která je spojená s kvalifikovaným a důsledným monitoringem.

Základním nástrojem pro zvýšení nebo alespoň udržení požadované úrovně bezpečnosti je:
- kvalifikované propojení řízení oblastí technické, organizační, finanční, personální, sociální, znalostní,
- a jasné role a odpovědnosti všech zúčastněných. Nástroje správy objektu [1], 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,
- systém spolupráce s veřejnou správou, s organizacemi v území a s organizacemi používajícími podobné technologie,
- výkonné složky ke zvládnutí nouzových situací,
- systémy ke zvládnutí kritických situací (řízení kontinuity, krizové řízení),
- bezpečnostní, nouzové a krizové plánování.

Jak již bylo výše řečeno, při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika. Systém řízení bezpečnosti SMS (Safety Management System) objektu dle poznatků a zkušeností shromážděných v práci [26], obrázek 20, proto musí obsahovat provázané položky:

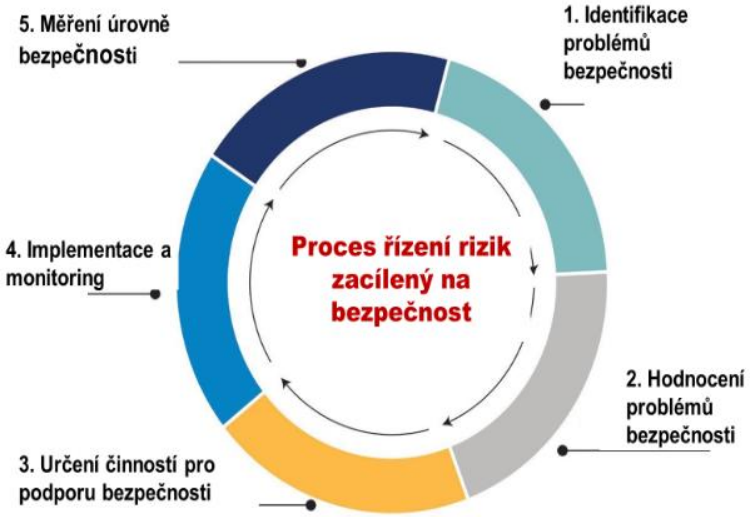
- strategický postup pro zajištění bezpečnosti,
- organizace řízení bezpečnosti,
- plán pro řízení bezpečnosti,
- opatření pro vypořádání rizik,
- měření úrovně bezpečnosti,
- rozhodování o opatřeních pro udržení či zvýšení úrovně bezpečnosti.

Obr. 20. Položky sledované v systému řízení bezpečnosti (SMS) objektu.

Podle současných znalostí je nutné při sestavování konceptu bezpečnosti objektu začít od jeho umístění, přes projektování, zhotovení a až k provozu. *Je třeba propojit normy a výsledky řízení rizik ve prospěch bezpečnosti* [1,33]*, tj. používat nástroje risk-based design, risk-based operation; risk-based inspections, risk-based maintenance* atd.[26], které propojují normy a výsledky řízení rizik. Vlastní metodický proces řízení rizik ve prospěch bezpečnosti (obrázek 21) zahrnuje:

- identifikaci problémů spojených s bezpečností,
- vyhodnocení těchto problémů z hlediska požadované úrovně bezpečnosti
- určení opatření a činnosti pro udržení či zvýšení úrovně bezpečnosti,

- implementaci opatření a zahájení monitoringu jejich účinnosti,
- posouzení úrovně bezpečnosti a v případě, že není dostatečná, identifikace problémů
- a opakování řetězce.



Obr. 21. Proces řízení rizik zacílený na bezpečnost objektu.

Bezpečnost i zabezpečení objektů, hlavně kritických je zásadní pro ochranu a rozvoj lidí i státu, proto každý stát musí mít strategii na udržování a popř. i zvyšování bezpečnosti. Protože svět se dynamicky vyvíjí, tak mohou nastat podmínky, na které nejsou limity objektu připraveny, a proto systémy řízení bezpečnosti (i systémy řízení zabezpečení) musí být vždy vybaveny opatřeními pro minimalizování škod v případech, že bezpečnostní opatření a bezpečnostní systémy selžou, anebo se vyskytne neidentifikované nebezpečí [1,12].

Minimalizování škod může mít podobu varovné a výstražné signalizace, výcviku, pokynů a procedur pro chování v nebezpečných situacích, nebo izolace nebezpečných zařízení od osídlených center. Opatření před nehodami včetně nouzového plánování musí být vypracováno ještě před tím, než je zařízení spuštěno do provozu. Při vzniku havárie by už na to nemuselo být dosti času [12].

Podle projektu všechny prvky či zařízení, komponenty a propojení kritických objektů (které jsou složité socio-kyber-fyzické systémy s vysokým počtem mnoha různých propojení) mají své limity, které jsou nastaveny na určité podmínky tak, aby společně plnily zadaný cíl (interoperabilita) [1,20,34]. Jelikož v důsledku dynamického vývoje světa se podmínky mění, tak se mění i podmínky pro interoperabilitu. Proto bezpečnost objektů se mění v závislosti na podmínkách.

Závěrem lze shrnout výhody konceptu řízení objektu zacíleného na bezpečnost:
- řeší konflikty proaktivně,
- v systému řízení bezpečnosti (SMS) kloubí aspekty technické, organizační, právní, finanční, manažerské, sociální, znalostní, vzdělávací, mezinárodní apod.
- a v hlavních procesech respektuje zásady řízení bezpečnosti procesů; obrázek 12.

Rizika technických objektů se ovládají [1,12] na základě:

- aplikace technických opatření, která se realizují pomocí:
  - výběru vhodných materiálů pro stavby a zařízení,
  - způsobů konstrukce staveb a zařízení,
  - vložení pasivních bariér, které zabrání jevům jako rozlet úlomků nebo rozptylu nebezpečné látky při ztrátě soudržnosti zařízení nebo stavby (např. obálky různých typů),
  - vložení záložních zařízení a systémů, tj. několika zařízení majících stejnou roli a popř. používajících různé fyzikální principy k dosažení plnění úkolu
  - či vložení ochran důležitých prvků,
- výběru vhodných řídicích systémů různých typů, které podle výsledků kontinuálního monitoringu upravují provoz,
- organizačních opatření, jejichž cíle jsou:
  - ochránit zaměstnance, pracovní a popř. i okolní prostředí od škodlivých dopadů
  - a také stavby a zařízení objektu od velké destrukce, protože technologické celky nejsou levné a pro zachování schopnosti rozvoje území jsou jejich výrobky žádoucí.

Podle výsledků v praxi nejvyšší účinnost (až 80%) mají opatření technická [1,8]. Přijatelné riziko závisí na sociálních, ekonomických a politických faktorech a že platí, že přijatelná úroveň rizika neznamená nulové škody, ztráty a újmy na chráněných aktivech, tj. že pravděpodobnost vzniku ztrát, škod a újmy na chráněných zájmech je malá až zanedbatelná.

Systém řízení bezpečnosti objektu (safety management systém – SMS) je mechanismus, který řídí (reguluje/ kontroluje) sledovaný objekt. Určuje dynamické chování objektu tím, že popisuje mechanismy, které ho určují. Mechanismy jsou vytvářeny systémy zpětných vazeb. Zpětné vazby jsou pozitivní, když mají synergickou zesilující funkci, a negativní, když mají regulační funkci. Lze na ně pohlížet jako na systémové mechanismy, které zajišťují dynamickou rovnováhu systému (každý systém se vyvíjí a může existovat jen tehdy, když je v dynamické‘ rovnováze). To znamená, že v případě menšího narušení provádí předmětné mechanismy kompenzaci narušení menšími vnitřními změnami, v případě větších narušení změnami většími, které mohou narušit stabilitu systému, a tím i jeho bezpečnost. Realita je složitější, máme poznatky o různých působeních kumulace menších narušení, a to ve smyslu positivním i negativním, které osvětlují až recentní teorie, a to teorie chaosu, teorie možností či teorie komplexity.

Je pochopitelné, že schopnost dynamických mechanismů systému není neomezená a při velkých zásazích nemusí být zmíněné mechanismy schopny kompenzovat narušení v dostatečné míře tak, aby odvrátily selhání objektu. Při regulaci (tj. při tvorbě regulačních mechanismů u technologických systémů) se vychází z kybernetického pojetí, že každý systém má určité podmínky existence a že existují bariéry v prostoru a čase, které v zájmu jeho existence nesmí být narušeny. Úkolem lidí odpovědných za řídicí systém je předmětné bariéry rozpoznat a regulovat dostupnými prostředky (pasivními i aktivními) a antropogenními činnostmi chování předmětných systémů tak, aby nedošlo k překročení bariér.

Řízení bezpečnosti vychází z řízení procesů, které je založeno na důsledném využití znalostí o problému v systému a jeho okolí, a proto se mu také říká „knowledge management“. Předmětný postup je velmi důležitý v analýze kořenových příčin problémů [35] a je kritickým faktorem pro udržitelný proces [36]. Řízení procesů založené na

řízení znalostí se nezaměřuje na výsledky, ale na příčiny. Je založené na rozpracování koncepce a metodologie:

- strategická úroveň tohoto řízení určuje základní směry vývoje, ze kterých vyplývá, které procesy je nezbytné upravit nebo vytvořit, jaké organizační změny bude nezbytné provést, kde získat know-how, finanční zdroje atd.,
- taktická úroveň řízení procesů pomáhá utřídit činnosti nutné pro realizaci dlouhodobých záměrů. Hledají se odpovědi na otázky jak procesy nastavit, v jakém stavu je udržovat a jak musejí tyto procesy navzájem spolupracovat,
- operativní úroveň řízení rozhoduje o konkrétním rozmístění zdrojů v procesu (lidských, technologických, finančních) a také o výkonu jednotlivých činností v rámci nastavených procesů (jak provést konkrétní operaci). Snahou je zajistit transfer znalostí a dovedností mezi pracovníky,
- na technické úrovni řízení se řeší konkrétní problémy. Je si třeba uvědomit, že nejnáročnější je vyjednávání s riziky, které se odehrává právě na této posledně jmenované úrovni řízení; zde se zvyšuje odolnost prvků, zařízení, komponent i celých systémů a dle údajů z praxe úspěšnost technických opatření se pohybuje mezi 40 a 80% [8].

Systém řízení bezpečnosti (tzv. SMS – Safety Management System) složitého objektu 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. Používá k tomu tzv. zlatá pravidla, kulturu bezpečnosti a plán řízení prioritních rizik [1,2]. Způsob řízení bezpečnosti (SMS) objektu se opírá o koncepci prevence pohrom či alespoň jejich závažných dopadů [1], která zahrnuje povinnost zavést a udržovat systém řízení, ve kterém jsou zohledněny dále uvedené problémy:

1. Role a odpovědnosti osob podílejících se na řízení závažných nebezpečí, která jsou spojená s možnými škodlivými jevy na všech organizačních úrovních kritického objektu a opatření na zajištění výcviku, která jsou sladěna s identifikovanými potřebami výcviku.
2. Systematické sledování rozhraní člověk – technika; člověk – IT; a technika – IT.
3. Plány pro systematické identifikování závažných nebezpečí spojených s možnými škodlivými jevy a z nich plynoucích rizik, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti).
4. Plány a postupy pro zajištění bezpečnosti všech komponent, systémů a funkcí v kritickém objektu a v jeho okolí, a to včetně údržby objektu i jeho zařízení.
5. Plány na implementaci změn v kritickém objektu a v objektech i zařízeních, které jsou v okolí.

6. Plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na možné nouzové situace.
7. Plány pro průběžné hodnocení souladu s cíli vyjasněnými v koncepci bezpečnosti a zabudovanými v SMS, a účinné mechanismy pro vyšetřování a provádění korekčních činností v případě selhání s cílem dosáhnout stanovené cíle.
8. Plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků kritického objektu.

Pro zajištění bezpečnosti zahrnující funkčnost, provozní spolehlivost a stabilitu objektu jsou důležité limity a podmínky nastavené v projektu [1]. Úkolem SMS je udržovat určené fyzikální veličiny (parametry dílčích systémů) na předem určených hodnotách a při použití automatizace upozornit na významné odchylky vyvolané chováním senzorů. V procesu regulace mění řídicí systém působením na akční veličiny stavy jednotlivých řízených systémů tak, aby bylo dosaženo žádaného stavu celého systému. U řídicího systému se sledují v prioritním pořadí vlastnosti jako:
- úroveň dodržování stanovených podmínek provozu a nevytváření škodlivých (nepřijatelných) dopadů na samotný systém a na jeho okolí,
- funkčnost (úroveň plnění požadovaných úkonů),
- provozuschopnost, tj. úroveň plnění požadovaných úkonů v závislosti na podmínkách normálních, abnormálních a kritických,
- provozní stálost, tj. úroveň dodržování stanovených podmínek provozu v čase,
- inherentně zabudovaná odolnost vůči možným pohromám.

Z výše uvedeného vyplývá, že řídicí systémy určují bezpečnost (kvalitu) a výkon (výkonnost) systémů. Mají rozhodující vliv na bezpečnost, a proto se u řídicích systémů sledují faktory:
- odpovědná autonomie,
- adaptabilita,
- celistvost
- a smysluplnost úkolů.

Celistvost vyjadřuje vnitřní jednotu, tj. autonomnost, nezávislost a odlišnost od okolí. Protože lidské chování není deterministické, jsou hlavními charakteristikami předmětných systémů:
- vynořující se vlastnosti,
- nedeterministické chování
- a složité vztahy mezi organizačními cíli.

O každém sledovaném systému vždy rozhoduje člověk a údržba, renovace, změny. Z inženýrského pohledu se sledované systémy charakterizují strukturou, hardwarem, procedurami, prostředím, toky informací, organizací (problém organizačních havárií) a rozhraním mezi uvedenými položkami [1].

Účinná kultura bezpečnosti je základním prvkem bezpečnosti [1,12]. Odráží koncepci bezpečnosti a vychází z hodnot, stanovisek a jednání vrcholových řídících pracovníků a z jejich komunikace se všemi zúčastněnými. Ukládá managementu objektu, aby praktikoval takový systém řízení bezpečnosti objektu, který udrží procesy v objektu v určitých mezích. 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 / objektu. 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 oblastech, kde jsou nadřazené systémy propojeny toky či vazbami s podřízenými či vedlejšími systémy [1,12] jde především o zabránění:
- přenosu chybných a matoucích informací, tj. chyby na vstupu nebo na výstupu systémů,
- přerušení informačních a materiálových toků,
- vykonávání navzájem se ovlivňujících funkcí
- a poruchám okolních systémů a realizaci relevantních pohrom.

V oblastech propojení mezi jednotlivými vrstvami systému řízení bezpečnosti [1,12] jde především o zabránění:
- aplikaci chybných metodik pro identifikace ohrožení a analýzy rizik z vyšších úrovní systému řízení bezpečnosti (SMS),
- neporozumění požadavkům a informacím z jiné vrstvy SMS,
- přenosu poruchových stavů v případě jejich výskytů z jedné vrstvy do druhé
- a nedodání vstupní informace.

Na rozhraní technických děl s okolním prostředím [1,12] jde o:
- zabránění nepředvídatelným událostem a útokům,
- změny podmínek pro provoz technického díla ze strany státu,
- zabránění úmyslným poškození technického díla,
- zabránění cíleným útokům na technické dílo.

Složitost objektů a infrastruktur roste. Na jedné straně tím roste efektivita předmětných systémů, ale na druhé straně se vytváří nové zdroje rizik, které jsou hůře odhalitelné. Některé způsoby zajištění jejich bezpečnosti (např. redundance, znásobení součástkových komponent pro ochranu před selháním obvodů měřící nebo regulační funkce - zálohování) poskytuje ochranu před haváriemi zapříčiněnými selháním individuálních částí, není však stejně efektivní vůči škodlivým jevům, které vygenerují interakce mezi komponentami ve stále komplexnějších a vzájemně interagujících inženýrských systémech dneška. Redundance mohou ve skutečnosti zvýšit složitost až do takové míry, při které už ony samotné jsou přispívajícími faktory k haváriím [1,12].

Proto mnohé z nových nebezpečí jsou záludnější, hůře odhalitelná a eliminovatelná, než v minulosti. Navíc neexistuje žádná předchozí zkušenost, které by mohlo být využito při překonávání nových nebezpečí. Mnoho zkušeností a poučení z předcházejících havárií je uloženo v zákonech, normách a v postupech dobré praxe. Ale odpovídající zákony a normy pro mnohé z nových inženýrských odvětví a technologií (kybernetika, AI) ještě nejsou vypracované. Mnohokrát se poučení získané za celá staletí ztratí, když se starší technologie nahradí novějšími; například, když se mechanické zařízení nahradí digitálními počítači.

Dalšími novými nebezpečími jsou již jen heslovitě např.:
- vzrůstající expozice nebezpečí,
- zvyšování kumulace energií a dosahů nebezpečí,
- zvyšování automatizace,
- narůstající centralizace a výrobní kapacita,
- nárůst tempa technologických změn.

Proto je třeba kontinuálně monitorovat účinnost opatření a činností zacílených na bezpečnost a při zjištění odchylek aplikovat korekční opatření, anebo změnit koncept práce s riziky, jak ukazuje obrázek 12.

V rámci strategie pro zajištění bezpečnosti a udržitelného rozvoje se musí v kritických objektech nastavit:

- program pro neustálé zvýšení bezpečnosti kritických objektů,
- míry pro posuzování úrovně bezpečnosti z hlediska účinnosti bezpečnostního systému (ukazatele),
- program, který zajišťuje bezpečnost, který je sestaven z provázaných projektů
- a projekty, které jsou naplněné provázanými procesy.

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.
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.

Normativ určující úroveň práce s riziky má sedm položek (obrázek 11), 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 [9] a Coaseho teorému [27].
6. Techniku řízení a vypořádání rizik technického díla.
7. Způsob řízení rizik v čase.

6. OPATŘENÍ A ČINNOSTI PRO VYPOŘÁDÁNÍ RIZIK

Opatření a činnosti pro vypořádání rizik technických zařízení a technických děl jsou:
- technická,
- organizační,
- metodická,
- vzdělávací
- a právní.

V každém životním cyklu jsou více či méně specifická. Důležitá je také metodika provedení vypořádání rizik.

6.1. Opatření a činnosti pro řízení a vypořádání rizik technického díla ve prospěch bezpečnosti z oblasti řízení

Základní premisou je, že systém řízení bezpečnosti musí být založen na dobré kultuře bezpečnosti, tj. na dobré úrovni systematicky prováděných lidských opatření a na jasně určených odpovědnostech. Časté nedostatky a příčiny organizačních havárií jsou shrnuty v práci [2]. Pro zvládnutí řady těchto nedostatků jsou dle ISO 31000 zpracovávány plány řízení rizik.

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 technického díla a vysoká kvalita konstrukce a provozu,
- zabudování ovládacích, omezovacích a ochranných systémů a další typické znaky dohledu nad provozem,
- zavedení inherentních vlastností podporujících bezpečnost do projektu technického díla,
- vytvoření alternativních opatření pro řízení havárií a selhání – 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 technická díla bylo možno zprovoznit v jisté dohledné době po velké havárii. Na základě zkušeností z odezev na havárie a selhání technických děl se odezva s tímto cílem musí řádně naplánovat, připravit a procvičit.

6.2. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti při výběru typu technického díla a lokality jeho umístění

Podle poznatků shrnutých v práci [17] je třeba při navrhování a umísťování technického díla do území zvážit veškeré známé údaje a zkušenosti. Na základě [2,17,37] pozornost při volbě opatření a činností pro řízení a vypořádání rizik ve prospěch bezpečnosti technických děl při umísťování je třeba sledovat zdroje rizik spojené 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.

Aby technické dílo splnilo očekávané úkoly nebo služby potřebné pro rozvoj lidské společnosti, tak je důležité si nejprve vyjasnit:

- úkoly, které má technické dílo zajistit,
- nároky na zdroje, síly a prostředky potřebné na realizaci technického díla a jeho provoz,
- rizika spojená s technickým dílem v různých fázích jeho existence, tj. od výstavby, přes provoz až po vyřazení z provozu,
- nároky na vybudování schopnosti dané lidské komunity (stát, vlastník, občané) zajistit realizaci a bezpečný provoz technického díla po celou dobu životnosti.

Při výběru typu technického díla a jeho umístění do území je třeba posuzovat zdroje rizik, které mohou významně ovlivnit bezpečí lidí a životního prostředí, anebo narušit bezpečnost samotného technického díla [17]. V druhém případě jde proto o posouzení:

- bezpečnosti technologie, tj. její spolehlivosti a funkčnosti, po celou dobu životnosti; je třeba zvažovat její udržovatelnost, opravitelnost a nároky na obsluhu,
- dostupnosti a konkurenceschopnosti technologie,
- splnitelnosti nároků dané technologie na znalosti, materiál, finance, instalaci a provoz technologie, a to i při změnách legislativy nebo trhu,
- schopnosti zabezpečit bezpečný provoz technického díla po celou dobu životnosti.

Konkrétní příčiny selhání (nedokončená realizace, velké problémy při provozu, a proto předčasné ukončení provozu), které lze shrnout takto:

- nesprávně zvolená specifikace technického díla,
- nesprávně zvolené umístění technického díla
- velká materiálová náročnost i energetická náročnost technického díla,
- velké nároky provozu technického díla na kvalifikovaný personál,
- velké nároky technického díla na dopravu a informační zajištění, tj. komunikační sítě,
- velké nároky technického díla na finance při výstavbě a provozu,
- velké nároky technického díla na odpovědnost za bezpečnost,

- velké nároky na řízení technického díla a na dohled státních orgánů nad bezpečností technického díla.

Vzhledem k dynamickému vývoji světa, všechna rizika nelze eliminovat, a proto pro zmírnění rizik je třeba používat systém pro podporu rozhodování a plán řízení rizik, jejichž modely jsou v práci [17]. Aplikace DSS umožňuje odhalit zdroje rizik jednotlivých variant technického díla, jejichž realizace může narušit koexistenci technického díla a jeho okolí, a to dnes i v budoucnu. Při výběru optimální varianty hraje roli:
- dosažená úroveň bezpečí a udržitelného rozvoje při aplikaci varianty,
- technická proveditelnost opatření s tím, že se bere vhodnost opatření pro daný systém,
- materiálová náročnost i energetická náročnost,
- rychlost realizace,
- nároky na kvalifikovaný personál,
- nároky na informační zajištění,
- nároky na finance,
- nároky na odpovědnost,
- nároky na řízení / organizaci v území apod.

Rozhodování o výběru varianty usnadní odpovědi na dále uvedených sedm otázek:

1. Co je prioritním rizikem, a co není prioritním rizikem.
2. Kdy se prioritní riziko realizuje, a kdy se prioritní riziko nerealizuje.
3. Jak se prioritní riziko realizuje, a jak se prioritní riziko nerealizuje.
4. Proč se prioritní riziko realizuje, a proč se prioritní riziko nerealizuje.
5. Kde se riziko realizuje, a kde se riziko nerealizuje.
6. Kdo nebo co přispívá k realizaci prioritního rizika, a kdo nebo co přispívá k odvrácení realizace prioritního rizika.
7. Jak zjistíme, že se prioritní riziko realizovalo, a jak zjistíme, že se prioritní riziko nerealizovalo.

Z ekonomického pohledu je vhodné provést rozhodování o vhodné variantě pro dané místo na základě skórování rizik a přínosů technického díla pro provozovatele a veřejnou správu předmětného území po dobu očekávané životnosti technického díla. Rozhodnutím o variantě jsou také určeny zdroje rizik, která bude nutno vypořádávat v budoucnu.

Vzhledem k dynamickému vývoji světa je pro zajištění bezpečného procesu výběru typu technického díla a jeho umístění do území v práci [17] uveden model plánu řízení rizik při realizaci předmětného procesu.

6.3. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti při projektování a zhotovení technického díla

Podle poznatků shrnutých v práci [19] je třeba při navrhování a umísťování technického díla do území zvážit veškeré známé údaje a zkušenosti. Na základě [2,19,37]

pozornost při volbě opatření a činností pro řízení a vypořádání rizik ve prospěch bezpečnosti technických děl při umísťování je třeba sledovat zdroje rizik spojené s projektováním, stavbou a technologiemi. Jde o zdroje rizik spojené s:

- lokalitou,
- projektováním a zhotovením, které obsahují zdroje rizik spojené 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 při výstavbě technického díla a jejího okolí během realizace technického díla, které způsobí dodavatel,
  - vlivem technického díla na životní prostředí během jeho životnosti, které způsobí veřejná správa špatným rozhodnutím při povolení provozu technického díla a špatným dohledem nad provozem technického díla,
  - vlivem technického díla na životní prostředí během jeho životnosti, které způsobí dodavatel a provozovatel,
- použitím chybných technologií, které obsahují zdroje rizik spojené s:
  - vadami vzniklými v průběhu realizace technického díla,
  - použitím chybné technologie v technickém díle,
  - technologickou nedostatečností technického díla,
- ostatními zdroji vnějších rizik, která jsou spojená s:
  - národní či mezinárodní situací,
  - terorismem,
  - změnami v legislativě a v systému daní,
  - požadavky nadnárodních institucí – EU, NATO.

Sledovaná etapa životnosti technického díla [19] zahrnuje širokou oblast problémů, např.:

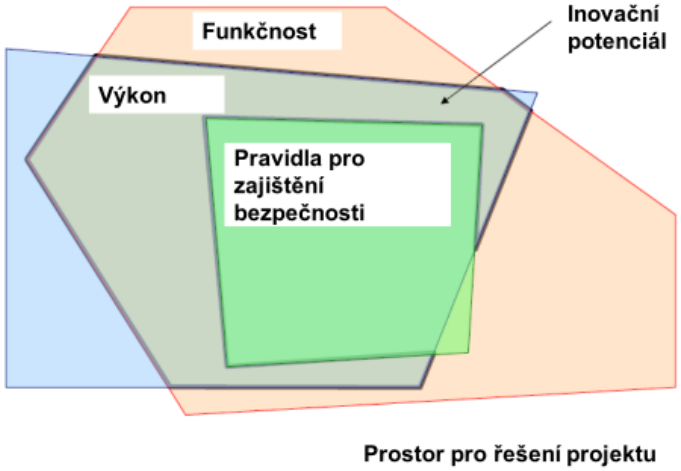
- teoretické analýzy kritických procesů, zařízení a míst a návrh praktického provedení technicky a finančně dostupných protiopatření,
- výběr: materiálů; technických principů; postupů výstavby; postupů konstrukce; stanovení kritických procesů výstavby a konstrukce; apod.,
- experimentální ověřování instalovaných zařízení a jejich provozuschopnosti za podmínek normálních, abnormálních a kritických,
- zajištění: trvanlivosti; ovladatelnosti zařízení a procesů; požadované životnosti; kvalitní a dostatečné lidské zdroje; náklady v požadované výši; technické služby; servis; apod.
- realizace staveb, konstrukcí a vybavení v daných podmínkách atd.

Na základě poznatků a zkušeností shromážděných v práci [19] je třeba při řešení projektu technického díla zvažovat skutečnosti uvedené na obrázcích 22 a 23.

Dle poznatků shromážděných v práci [19] při návrhu a realizaci optimální varianty technického díla v daném konkrétním případě pak hraje roli:

- dosažená úroveň bezpečí technického díla a jeho okolí,
- technická proveditelnost opatření pro zajištění bezpečného technického díla s tím, že se bere do úvahy vhodnost opatření pro daný systém, tj. technické dílo a jeho okolí,
- materiálová náročnost i energetická náročnost technického díla,

- rychlost realizace technického díla,
- nároky provozu technického díla na kvalifikovaný personál,
- nároky technického díla na dopravu a informační zajištění, tj. komunikační sítě,
- nároky technického díla na finance při výstavbě a provozu,
- nároky technického díla na odpovědnost za bezpečnost,
- nároky na řízení / organizaci v území spojené s technickým dílem.



Obr. 22. Položky, které je třeba zvažovat při zpracování projektu technického díla.

Obr. 23. Aspekty, které musí řešit projekt technického díla.

V rámci řízení rizik technického díla zacíleného na integrální bezpečnost je třeba kvalitně provést pět klíčových aktivit [2], a to:

1. Vymezení cíle a centra zájmu řízení bezpečnosti technického díla, což znamená:
   - identifikovat kontext,
   - určit prioritní cíle,
   - a určit zásadní úkoly v jednotlivých oblastech.

Výběry opatření jsou založeny na hodnocení aktiv a cílů řízení rizik. V rámci této činnosti stanovíme, která rizika jsou v daném případě prioritní, jak požaduje současně preferovaný typ řízení TQM (Total Quality Management).

2. Popis chování technického díla a okolí za různých podmínek, který směřuje k objektivnímu pochopení:
   - pravděpodobnosti výskytu a velikosti dopadů (v kvalitativním nebo lépe kvantitativním vyjádření) možných pohrom
   - a selhání technického díla.

   Jedná se o vysoce odbornou činnost vyžadující hluboké znalosti a kvalitní data.
3. Rozhodnutí, které je založeno na vyhodnocení kvality předpovědi vývoje technického díla a jeho okolí, pokud možno jako optimum při zvážení přínosů a ztrát při provozu technického díla v dynamicky proměnném okolí. Jde o specifikaci, jak zmírnit a řídit rizika a jak implementovat opatření preventivní, zmírňující, reaktivní i obnovovací. Reprezentuje klíčový krok v rámci řízení rizik technického díla.
4. Komunikace, která vede k projednání souboru opatření a činností s klíčovými aktéry provozu technického díla a s ostatními zúčastněnými. Legislativa vyžaduje v důležitých otázkách také:
   - komunikaci s veřejností,
   - konzultace s odborníky,
   - odstranění konfliktů
   - a stanovení partnerství při řešení budoucích problémů.
5. Monitoring a poučení, které zajistí sledování určených veličin a jejich hodnot, které charakterizují důsledky rozhodnutí a činností na technické dílo, a v případě zjištění významných odchylek, které mohou narušit dosažení cíle, aplikovat korekce.

Proces projektování a zhotovení technického díla se skládá z několika následných procesů [19]. Jde o proces:
- sestavení zadávacích podmínek technického díla,
- zpracování projektu technického díla,
- výstavba a konstrukce technického díla,
- testování provozuschopnosti a bezpečnosti technického díla
- a zprovoznění technického díla.

Předmětný proces je významně ovlivněn:
- znalostmi a zkušenostmi navrhovatelů a zhotovitelů,
- vlastnostmi prostředí, do kterého se technické dílo umísťuje,
- finančními možnostmi objednatele technického díla,
- znalostmi a zkušenostmi zhotovitele technického díla,
- úrovní dohledu veřejné správy nad bezpečností technického díla ve veřejném zájmu.

Proto musí odpovídat požadavkům legislativy a být dozorován veřejnou správou.

Proces projektování a zhotovení technického díla je komplexní oblast, s neustále se měnícími procesy a činnostmi [19]. Účastní se ho mnoho aktérů, kteří jsou na sobě vzájemně závislí, a proto by spolu měli spolupracovat. Je také ovlivňováno řadou vnějších faktorů, jako je:
- stav na trhu,
- projekty okolních technických děl,
- velikost technického díla,

- dostupnost zdrojů,
- místně specifický charakter kritických infrastruktur; způsobilost
- a zkušenost manažerů a zaměstnanců.

Poznatky shrnuté v práci [19] ukazují, že pro zajištění bezpečnosti technických děl ve sledované fázi životnosti je důležitá znalost:
- předpisů,
- rizik v lokalitě, do které je technické dílo umísťováno,
- technického systému, který představuje technické dílo,
- modelů a teorií spojených s nehodami,
- metod analýzy, řízení a vypořádání rizik,
- způsobu řízení, který použije provozovatel po uvedení do provozu (finance, lidské zdroje, organizace, technologie, inovace atd.).

Dále je nutno, aby všichni zúčastnění respektovali veřejný zájem, podíleli se na budování kultury bezpečnosti a aby vedoucí pracovníci motivovali zaměstnance ke kvalitní práci, a to i vlastním příkladem, jak ukazují tzv. zlatá pravidla [1,19].

Na základě poznatků shrnutých v práci [19] je třeba z pohledu veřejného zájmu použít varianty procesu projektování a zhotovení technického díla, které mají riziko nižší než stanovená míra přijatelného rizika s tím, že výše rizik bude pravidelně monitorována s ohledem na dynamický vývoj světa. Ostatní varianty projektu je třeba při rozhodování o vydání či nevydání povolení ke zhotovení technického díla buď vyloučit, anebo upravit jejich parametry a v případě nezbytnosti technického díla zajistit opatření na zmírnění nejhorších dopadů na veřejná chráněná aktiva v případě realizace rizika.

Podle údajů shrnutých v práci [19], při realizaci procesu projektování a zhotovení konkrétního technického díla je třeba zvažovat zdroje všech rizik dle přístupu All-Hazard-Approach [13,14]. Do uvedeného souboru patří i škodlivé jevy, které jsou důsledkem všech vzájemných reakcí daného technického díla s jeho okolím za podmínek normálních, abnormálních i kritických. Určení vnitřních zdrojů rizik technického díla spojených jednak s jednotlivými technickými zařízeními, jejich uspořádáním do komponent a systémů, a jednak s výrobními procesy a jejich řízením, je místně specifická činnost, která vyžaduje identifikaci rizik na několika úrovních, a to:
- technická zařízení,
- komponenty,
- systémy,
- technická, organizační a kybernetická vzájemná propojení za normálních podmínek provozu,
- technická, organizační a kybernetická vzájemná propojení za abnormálních podmínek provozu,
- technická, organizační a kybernetická vzájemná propojení za kritických podmínek provozu,
- u vysoce důležitých technických děl, jako jsou jaderné elektrárny, přehrady apod., i technická, organizační a kybernetická provozu vzájemná propojení za extrémních podmínek provozu.

Při identifikaci zdrojů rizik pro technické dílo je dle poznatků shromážděných v pracích [12,19] velmi důležité zvážit uvnitř technického díla a v jeho blízkém okolí všechny stabilní i mobilní zdroje:
- požárů (mžikový, proudový, kaluže, zášlehový, tryskavý, BLEVE - ohnivá koule),

- explozí (mechanických, elektrických, chemických, exploze mraku plynů, prachu a popř. i jaderných),
- úniku nebezpečných látek,

protože škody způsobí jak jejich dopady, tak i možné domino efekty.

Pro potřebu projektu je třeba určit správně hodnoty projektových pohrom a na jejich základě dle místních podmínek určit velikost rizik, která budou zvažována v projektu a výstavbě – postupy jsou v práci [19]. Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika. Vypořádání rizik (někdy se též používá 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, že se provedou, jak již bylo dříve řečeno:

- preventivní opatření, která sníží nebo odvrátí realizace rizika,
- účelová zmírňující opatření odezvy a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení), kterými se zmírní dopady, tj. sníží nebo odvrátí se nepřijatelné dopady při realizaci rizika, - akce na zajištění pojištění na krytí možných ztrát a škod,
- akce pro přípravu rezerv na odezvu a obnovu a záloh pro zajištění přežití lidí a kontinuitu provozu území, objektu či organizace,
- akce pro přípravu plánu pro odezvu na nepředvídané situace (Contingency Plan) pro případ realizace rizik neřiditelných nebo příliš nákladných, anebo málo častých.

V souvislosti s každým rizikem si je třeba vždy uvědomit:

- co se může stát,
- kde se to může stát,
- co může spustit velké ztráty a škody,
- jaká aktiva budou zasažena,
- co je třeba si připravit pro ochranu veřejných aktiv a koexistence technického díla s okolím.

Na základě současného poznání shromážděného v pracích [2,3,19] platí, že pokud nejsou havárie nevyhnutelně zapříčiněné událostmi, které se dají vyjádřit pravděpodobnostmi, nelze pro ně všeobecně používat míry pravděpodobnosti rizika. Odhady pravděpodobnosti měří pravděpodobnost náhodných chyb, a ne míru rizik a nehod anebo havárií (které souvisí s neurčitostmi). Když se při analýzách systému řízení bezpečnosti najde chyba v projektu, je daleko účinnější, tuto chybu odstranit než někoho přesvědčovat pomocí vypočítaných pravděpodobností, že tato chyba nikdy nezpůsobí havárii. Nízké hodnoty pravděpodobnosti výskytu havárie nezaručují bezpečnost a bezpečnost nevyžaduje mnohdy ultra vysokou spolehlivost zařízení.

Hlavním nedostatkem pravděpodobnostních modelů nejčastěji není to, co zahrnují, ale to, co nezahrnují. Nízké hodnoty pravděpodobnosti jednoduše nehovoří o tom, že systém neselže uvažovaným způsobem, ale naopak, že selže s daleko vyšší pravděpodobností způsobem, o kterém uvažováno nebylo.

Již od návrhu technického díla je třeba dbát na jeho snadnou ovladatelnost obsluhou. Proto je třeba v návrhu zvažovat schopnost obsluhy při jeho řízení, tj. zda je možné vytvořit dobrou kulturu bezpečnosti na všech úrovních řízení technického díla [1,8]. Všechny výše uvedené skutečnosti ukazují, že návrh technického díla vyžaduje řadu pohledů a u složitých technických děl spolupráci mnoha odborníků.

V práci [1] je ukázáno, že řízení rizik složitých technických děl je důležité ve dvou oblastech:

1. Oblast propojující veřejnou správu a management složitého technického díla.
2. Oblast věcná zabývající se daty, metodami, materiálovými a technickými záležitostmi, organizačními, právními, finančními a personálními záležitostmi přímo v technickém díle.

Na závěr se identifikují oblasti, ve kterých se rizika technického díla a jeho okolí řídí nedostatečně nebo vůbec neřídí. V těchto oblastech se pak ***v návrhu technického díla zavádí kromě již zmíněných faktorů, tj. inherentní bezpečnosti a položek pro zvyšování pružné odolnosti*** na základě poznání shrnutého v pracích [1,8] zavádí další opatření, a to:

1. Bezpečnost technického díla se zajišťuje použitím:
   - zabudováním principu selži bezpečně,
   - vložením ochran před nepředvídatelnými jevy,
   - vložením ochran před jednoduchými selháními,
   - vhodného opatření inherentní bezpečnosti,
   - principu Defence-In-Depth,
   - opatření pro řízení odpadu z provozu.

   Musí být snaha vytvořit návrh technického díla tak, aby technické dílo nezpůsobilo ztráty na životech lidí, životním prostředí a zničení díla a spolehlivě plnilo funkce po dobu životnosti. Proto se používá princip předběžné opatrnosti, studují se dopady možné velké havárie a již v návrhu technického díla se dělají opatření na jejich zmírnění. Někdy je třeba snížit spolehlivost na podporu bezpečnosti – např.: falešné alarmy poškozují spolehlivost zařízení, ale pro bezpečnost je lépe mít nějaké falešné alarmy než nevarování.
2. Spolehlivost technického díla se zajišťuje použitím:
   - záloh (obvyklé jsou 3 typy – zařízení běžící paralelně, které se používá tam, kde není možné přerušení; zařízení startující v krátké době po žádosti, které se používá tam, kde je možné krátké přerušení; zařízení, které je třeba nainstalovat),
   - rozmanitostí záloh,
   - vložením záloh proti selhání,
   - systémů, které tolerují chyby,
   - faktorů pro posílení provozní bezpečnosti.

   Musí být snaha vytvořit návrh technického díla tak, aby technické dílo:
   - plnilo správně funkce po dobu životnosti,
   - bylo ziskové
   - a mělo jistou provozní bezpečnost,

   a to proto, že jsou systémy, které jsou hodně spolehlivé, ale jsou nebezpečné – např. vlak za špatných podmínek z důvodu bezpečnosti zpomalí nebo zastaví, a tím se zpozdí, což znamená, že nesplní požadavek spolehlivosti.
3. Pro řízení a zvládnutí rizik, hlavně prioritních u technického díla, se používají:
   - principy prevence,
   - princip předběžné opatrnosti,
   - princip ochrany,
   - způsoby omezení rizik,
   - způsoby zvládnutí projektových pohrom,
   - vytváření schopnosti přežít nadprojektové pohromy.

4. Pro potřeby řízení se do projektu technických děl vkládají zařízení a systémy, které umožňují sledovat specifické veličiny, jako jsou interoperabilita a kritičnost.

Při navrhování složitých technických děl existují limity, které je nutno respektovat. Jde o limity:
- fyzikální, které jsou dané fyzikálními zákony pro možné podmínky provozu,
- určené legislativou nadnárodních institucí (IAEA, EU…),
- určené národní legislativou,
- určené v bezpečnostní zprávě technického díla a v jeho technických specifikacích,
- určené v provozních předpisech technického díla.

V inženýrské praxi je základem znalost norem a inženýrských postupů dobré praxe. 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 [2].

Základem projektové dokumentace jsou zadávací podmínky technického díla, které specifikují velikosti rizik, které musí respektovat projekt. Tj. projekt musí předmětná rizika vypořádat prevencí, anebo pomocí technických opatření přímo vložených do projektu. Při jejich tvorbě je třeba mít znalosti a kompetence, které jsou shrnuté v práci [19]. Projektování technických děl je velmi komplexní činnost. Konkrétní projekt technického díla závisí na složitosti navrhovaného technického díla a na požadavcích stanovených veřejným zájmem. V projektu každého technického díla z pohledu bezpečnosti je třeba sledovat požadavky na:
- trvanlivost,
- ovladatelnost zařízení a procesů,
- životnost,
- lidské zdroje,
- náklady,
- technické služby,
- servis,
- bezpečí zaměstnanců,
- bezpečí lidí v okolí
- a bezpečí životního prostředí.

Zvážení a dobré zajištění předmětných požadavků totiž určuje budoucí náklady na zajištění bezpečnosti a koexistence technického díla s okolím.

Podle poznatků a zkušeností shromážděných v práci [19] při projektování je třeba zvážit:
- velikosti rizik stanovené zadávacích podmínkách,
- pochopit kritické úkoly technického díla z pohledu integrální bezpečnosti,
- pochopit úkoly technického díla a příčiny jejich kritičnosti,
- identifikoval možná lidská selhání; a navrhnout opatření k zajištění bezpečnosti s ohledem na proměnné podmínky.

Kritické úkoly technického díla z pohledu integrální bezpečnosti dle [19] jsou fyzické činnosti, jejichž způsobem provedení člověk přispěje k:
- spuštění nežádaného a nepřijatelného jevu,
- detekci a prevenci předmětného jevu,
- řízení a zmírnění předmětného jevu,
- odezvě na nouzovou situaci.

Proto cílem projektu technického díla je vytvořit výrobní proces, který je ziskový, ekonomický, bezpečný a neohrožuje veřejná aktiva, a to především lidi a životní prostředí. Toho lze dosáhnout optimalizací bezpečnostních, ekonomických a funkčních kritérií. Z tohoto důvodu projekt technického díla zahrnuje širokou oblast problémů, např. výběr:

- materiálů,
- technických principů,
- postupů výstavby,
- postupů konstrukce,
- stanovení kritických procesů výstavby a konstrukce
- způsobu ochrany fyzické, kybernetické aj.,
- apod.

Aby se splnily výše uvedené požadavky, je nutná účast mnoha odborností, tj. řady specialistů z různých odborů. Je si třeba uvědomit, že právě zde se projevuje lidský faktor. Je třeba zvážit a konsensuálně vyřešit problémy spojené s:

- daným procesem
- návrhem procesu,
- řízením procesu,
- provozním personálem a signalizací jeho stavu,
- systémem pro zajištění bezpečnosti,
- dalšími technickými systémy podporujícími bezpečnost,
- vnějšími aktivními a pasivními systémy pro zmírnění rizika spojeného se selháním procesu,
- nouzovou odezvou technického díla,
- nouzovou odezvou lokality, v níž je technické dílo umístěno.

Strategie řízení rizik výrobních procesů, které technické dílo bude realizovat při projektování dle poznatků shrnutých v práci [19], spočívá v aplikaci:

- principů inherentní bezpečnosti,
- systémů pasivní bezpečnosti,
- systémů aktivní bezpečnosti,
- principů ochrany do hloubky,
- bariér,
- dostatečné resilience kritických prvků a komponent a jejich propojení,
- procedurálních postupů, které jsou osvědčené, anebo důkladně prověřené tak, aby neobsahovaly latentní zdroje nebezpečí za možných podmínek.

Dle současného poznání [19] zhotovené technické zařízení a technické dílo je třeba před uvedením do provozu otestovat; složité technické dílo navíc musí projít zkušebním provozem a atestací o provozuschopnosti. Při testování zařízení se ověřuje správnost dokumentace a výsledky nedestruktivních testů [19].

Nedestruktivní testy pomáhají odhalit, zda sledovaná část technického díla nemá defekt ve smyslu odchylky od norem a standardů, a v případě jeho zjištění určit jeho povahu a polohu, a to bez jeho porušení. Nedestruktivní testy využívají:

- různá fyzikální pole,
- záření všeho druhu,
- chemické interakce
- a různé způsoby monitorování.

Jejich cílem je posoudit stav zkoumané položky a při provozu pak i odhad zbytkové životnosti nebo rizika spojeného s dalším využíváním testované části technického díla. Tím se zajistí, že rizika zařízení a technického díla jsou přijatelná, tj. dílo je bezpečné pro sebe i okolí. Metod a variant jejich provedení je velké množství, a podobně jako u výpočetních modelů platí, že z důvodu věrohodnosti závěrů je vhodné v praxi použít několik metod [19].

Cílem nedestruktivních metod [19] je:
- zjistit celistvost technického zařízení, což garantuje jeho spolehlivost,
- předejít selhání technického zařízení vlivem poruch, čímž se předchází úrazům, zajišťuje se ochrana investic a jejich návratnost,
- spokojenost uživatelů zařízení i služeb, které tato zařízení poskytují,
- podpoření goodwill provozovatele,
- zlepšení designu technického zařízení,
- zlepšení řízení výrobních procesů,
- snížení výrobních nákladů.

Rozlišuje se šest hlavních kategorií nedestruktivních metod: vizuální; radiační; magneticko-elektrické; mechanické vibrace; termální; a chemické / elektrochemické. Cílem každé metody je zjistit údaje o jednom parametru materiálu nebo o několika parametrech materiálu:

1. Existence diskontinuit v materiálu a jejich rozdělení (trhliny, dutiny, městky, štěpení, dělení na vrstvy apod.).
2. Charakter struktury materiálu (krystalická, amorfní, velikost zrn, mezilamelární defekty, segregace, poruchy apod.).
3. Velikost a charakteristika poruch materiálu (povrchové, pronikající dovnitř, šířka, tloušťka, průměr, spáry, popraskání apod.).
4. Fyzikální a mechanické vlastnosti diskontinuit (odrazivost, vodivost, modul pružnosti, rychlost zvuku apod.).
5. Složení a chemická analýza materiálu (identifikace slitin, nečistoty, příměsi, rozložení nečistot apod.).
6. Pnuti a dynamická odezva materiálu (zbytkové pnutí, narůstání trhlin, opotřebení, vibrace apod.).
7. Výskyt termálních, magnetických, elektrických a jiných anomálií v materiálu.

Ze sledovaných zdrojů i zkušeností autorky vyplývá, že žádná metoda neodhalí všechny defekty v materiálu. Pro posouzení rizika spojeného s matriálem technických zařízení v provozu někdy postačí jedna správně vybraná metoda a jindy je třeba použít metod několik.

Metodami nedestruktivních testů sledujeme zpravidla jedno aktivum, a to technické zařízení, a velikost rizika měříme jeho dopadem na vybrané parametry materiálu (kumulace a množství trhlin, intenzity magnetické intenzity).

Pro zajištění kvalitního provedení technického díla je třeba zajistit, aby procesy výstavby, konstrukce, vložení potřebného vybavení, testování a uvedení do provozu byly bezpečné. Na základě výše uvedených skutečností je vhodné pro řízení bezpečnosti jednotlivých postupů používat kontrolní seznamy.

Vzhledem k dynamickému vývoji světa, všechna rizika nelze eliminovat, a proto pro zmírnění rizik ve sledované fázi životnosti technického díla je třeba používat systém pro podporu rozhodování a plán řízení rizik, jejichž modely jsou v práci [19]. Aplikace DSS umožňuje odhalit zdroje rizik jednotlivých variant provozu technického díla, jejichž realizace může narušit koexistenci technického díla a jeho okolí, a to dnes i v budoucnu. Při výběru optimální varianty hraje roli:

- dosažená úroveň bezpečí a udržitelného rozvoje při aplikaci varianty,
- technická proveditelnost opatření s tím, že se bere vhodnost opatření pro daný systém,
- materiálová náročnost i energetická náročnost,
- rychlost realizace,
- nároky na kvalifikovaný personál,
- nároky na informační zajištění,
- nároky na finance,
- nároky na odpovědnost,
- nároky na řízení / organizaci v území apod.

Rozhodování o výběru varianty projektu technického díla či technického zařízení usnadní odpovědi na sedm otázek, které jsou uvedeny v odstavci 6.2. Z ekonomického pohledu je vhodné provést rozhodování o vhodné variantě pro dané místo na základě skórování rizik a přínosů technického díla pro provozovatele a veřejnou správu předmětného území po dobu očekávané životnosti technického díla. Rozhodnutím o variantě jsou také určeny zdroje rizik, které se musí při provozu průběžně sledovat a řídit.

Vzhledem k dynamickému vývoji světa je pro zajištění bezpečného procesu projektování a zhotovení technického díla v práci [19] uveden generický model plánu řízení rizik při realizaci procesu projektování a zhotovení technického díla. Pro zajištění bezpečného provozu je vhodné použít kontrolní seznam v tabulce 3.

Tabulka 3. Kontrolní seznam pro zajištění bezpečného procesu projektování, výstavby a spuštění technického díla

Otázka	**Hodnocení**	**Pozn.**
Míra, v jaké jsou uplatněny při projektování výsledky analýzy a hodnocení rizik přizpůsobené technickému dílu a jeho okolí.		
Míra, v jaké jsou při projektování uplatněny zásady pro zajištění integrální bezpečnosti.		
Míra, v jaké jsou při projektování uplatněny zásady strategického plánování.		
Míra, v jaké je při projektování uplatněna hierarchizace problémů.		
Míra, v jaké je navrhovaná varianta projektu správná.		
Míra v jaké jsou zpracovány zadávací podmínky projektu.		
Míra, v jaké má projektant znalosti a kompetence.		
Míra, v jaké jsou v projektu aplikovány zásady inherentní bezpečnosti.		
Míra, v jaké je naplněna odpovědnost za kvalitu projektu.		
Míra, v jaké jsou v projektu uplatněny zásady řízení na zvládání nouzových a kritických situací.		

Míra, v jaké je při sestavování zadávacích podmínek pro projekt uplatněn přístup All-Hazard Approach.		
CELKEM		

6.4. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla při provozu

Podle poznatků shrnutých v práci [12] je třeba při navrhování a umísťování technického díla do území zvážit veškeré známé údaje a zkušenosti. Na základě [2,12,37] pozornost při volbě opatření a činností pro řízení a vypořádání rizik ve prospěch bezpečnosti technických děl při umísťování je třeba sledovat zdroje rizik spojené s:

- lokalitou,
- nedostatky v projektu 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,
- 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 provozu technického díla ze strany veřejné správy,
- technickými zařízením a vybavením technického díla, kde jde o zdroje rizik spojené s:
  - vlastním technickým zařízením a vybavením,
  - vstupy, tj. kvalitou a vlastnostmi používaných materiálů,
  - údržbou, opravami, modifikacemi a adaptacemi,
  - nízkou zůstatkovou hodnotou.
- způsobem řízení technického díla, kde jde o zdroje rizik spojené s:
  - chováním managementu technického díla,
  - způsobem rozhodování managementu technického díla,
  - zavedenou kulturou bezpečnosti,
  - chováním managementu technického díla k zaměstnancům,
- prováděním rozhodování a řízení, kde jde o zdroje rizik spojené s:
  - kvalitou koncepce a strategickým rozhodováním ve prospěch bezpečnosti,
  - prevencí ztrát a péčí o kritická aktiva,
  - reputací,
  - odpovědností třetí straně,
  - změnami smluv,
  - poručováním obecně závazných předpisů,
  - korupci,

- chováním a jednáním zaměstnanců, kde jde o zdroje rizik spojené s:
  - neodpovídajícími pracovními silami,
  - nezastupitelností kvalifikovaných pracovníků u kritických činností,
  - nedostatkem lidských zdrojů,
  - pracovně právními spory,
  - selháním lidského faktoru.
  - lidskou spolehlivostí, tj. s náchylností člověka dělat chyby (v technických dílech jde o projektanty, konstruktéry, technology, provozáře, údržbáře, techniky a ostatní personál),
  - podvodným jednáním zaměstnanců,
  - nelegálním jednáním zaměstnanců,
  - poškozováním zařízení, krádeží apod.,
- bezpečností technologických a kybernetických zařízení a systémů.

V současné době jsou provozovaná a budovaná technická díla jako socio – kyber - technické (fyzické) systémy. Automatizace proniká do života všech technických děl. Na jednu stranu přináší obrovské výhody a úspory práce lidí a na straně druhé také další rizika. Proto je důležitý výběr správného software [38] a kvalitní testování programových produktů [39].

V souvislosti s automatizací je řízení technického díla definováno jako cílené působení řídicího systému na řízený objekt tak, aby bylo dosaženo určeného cíle. V daném kontextu je řízení technického díla členěno na automatické pomocí informačních technologií, poloautomatické (pomocí zásahu technických mechanismů) a ruční (prováděné člověkem). V praxi se odlišují ovládání, regulace a vyšší formy řízení (optimální a adaptivní řízení, učení a umělá inteligence).

Podle údajů v současné odborné literatuře, shrnutých v práci [1], jsou pro technická díla používané různé typy řízení, které se podle cílů řízení technických děl máme v praxi:

1. Řízení spolehlivosti (reliability management).
2. Řízení zabezpečení (security management).
3. Řízení bezpečnosti (safety management).
4. Řízení kontinuity (continuity management).
5. Řízení pružné odolnosti (resiliency management).
6. Řízení aktiv (asset management).

Každý z těchto typů má jistá specifika [12]:
- první typ řízení upravují technické normy a standardy,
- druhý typ řízení se kromě řízení spolehlivosti soustřeďuje na ochranu technických děl před vnitřními i vnějšími škodlivými jevy (pohromami), a to včetně chování lidí, kteří je vytváří a provozují [2]. Zabezpečení (anglicky security) ve spojení s jistým objektem znamená obecně soubor opatření a činností, kterými se zajistí, že objekt neutrpí ztráty, škody a újmy při výskytu vnitřních i vnějších škodlivých jevů. K jeho realizaci se také používá fyzická a kybernetická ochrana objektu [40], a to nejen proti útokům zvnějšku, ale i z vnitřku. Pravidla pro řízení zabezpečení technických děl jsou rozpracovaná v práci [41], ve které jsou uvedeny i rozdíly proti pravidlům řízení bezpečnosti technických děl [42]; odlišení je též v dokumentech IAEA [43].

Přestože logicky je bezpečný objekt též objekt zabezpečený [1,8], tak existují stále dohady, co je důležitější. Shoda je v tom, že ***zabezpečené technické dílo*** stejně jako bezpečné technické dílo bezchybně plní stanovené úkoly po stanovenou dobu za určitých podmínek, a přitom je ochráněno proti všem vnitřním a vnějším pohromám, včetně lidského faktoru. Rozdíl je v tom, že zabezpečené technické dílo nemá zabudovánu ochranu okolí,
- charakteristika dalších typů je v práci [12].

Součástmi všech typů řízení jsou pak specifické typy, kterými jsou nouzové řízení a krizové řízení [12].

Protože zdrojů, sil a prostředků na bezpečnost, tj. na řízení rizik, není nikdy dostatek, je třeba z důvodů hospodárnosti [12] 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).

Bezpečný provoz technického díla je určen jak architekturou a provedením technického díla, tak způsobem provozu zařízení, komponent a jejich systémů. Protože žádný projekt technického díla a jeho provedení nejsou ideální a nadčasové, musí být bezpečnost technických děl kvalitně řízena s pomocí kvalifikované údržby, a to i s ohledem na zastarávání technických postupů a zařízení [12]. Aspekty důležité pro provoz technických zařízení i celých technických děl jsou však velmi rozmanité, především jde o aspekty:
- znalostní a technické, které předurčují kapacitní možnosti technických děl a technických zařízení,
- organizační a právní záležitosti, které umožňují provoz technických děl a technických zařízení na určité úrovni bezpečnosti v území a v čase,
- finanční, personální, sociální a politické na národní a mezinárodní úrovni.

Pro bezpečnost technických zařízení a technických děl musí provozovatel technických zařízení a technických děl zajišťovat opatřeními a činnostmi tři cíle z hlediska veřejného zájmu:
- prvním cílem je zajistit provozní spolehlivost (dependability) technického zařízení i technického díla, protože tím sledovaná položka zabezpečuje služby a výrobky, ke kterým je vybudována,
- druhým cílem je zajistit integrální (systémovou) bezpečnost sledované položky, tj. ochrana předmětné položky před pohromami všeho druhu (vnitřními i vnějšími, a to včetně lidského faktoru),
- třetím cílem je zajistit, aby technické zařízení či technické dílo ani při svých kritických podmínkách neohrožovalo sebe a své okolí, tj. ostatní veřejná aktiva, tj. je nutno zvážit systémovou podstatu měnící se v čase různým způsobem.

Bezpečnost technických zařízení i celých technických děl je značně ovlivněna úrovní provádění provozních opatření a činností obsluhou [12]. Proto obsluha (především kritický personál) musí mít znalosti, schopnost a dovednost provádět jak standardní úkony, tak opatření a činnosti při výskytu neočekávaných jevů. Tabulka 4, zpracovaná dle práce [44], ukazuje:

- nároky na obsluhu, která má schopnost nakládat s neočekávanými jevy,
- cíle, způsoby nástroje pro zajištění schopnosti nakládat s neočekávanými jevy.

Tabulka 4. Jak získat schopnost nakládat s neočekávanými jevy; zpracováno dle [38].

Požadavky	**Cíl, způsob a nástroj zajištění**
Mentální připravenost, že přijde něco nečekaného	Cíl: řídící pracovníci mají povědomí, že neočekávaná událost může nastat a ochotu (pohotovost) se na ni připravit. Jak: výcvik v mnoha scénářích možných havárií a neustálé vzdělávání ve zvládání jevů. Nástroj: výcvik, samostudium případů, studium poučení a diskuse.
Mít povědomí o stavu procesů v technickém díle	Cíl: získání technicko-provozní kompetence. Jak: mít znalosti o klíčových komponentách technického díla, klíčových parametrech technického díla, termodynamice; schopnost předvídat činnost systémů technického díla; mít povědomí o reakcích systému při normálních podmínkách a při poruchách. Nástroj: praxe, výcvik, samostudium, diskuse, studium poučení z minulých událostí a skoro nehod.
Výběr správné osoby	Cíl: znalost role, odpovědnost, kompetence, informace potřebné pro rozhodování. Jak: znalost organizace práce a organizace nouzové odezvy. Nástroj: praxe, výcvik.
Rozhodování při neobvyklé dynamické situaci	Cíl: schopnost rozložit problémy, analyzovat a rozčlenit informace a povědomí o možných léčkách při rozhodování. Jak: pochopení kreativních přístupů při rozhodování a schopnost přemýšlení a spojité vyhodnocování a přehodnocování situací a aktiv v případě, že je nutno přizpůsobovat cíle, anebo strategie. Nástroj: výcvik, studium poučení z minulých událostí a diskuse se zkušenými odborníky.
Spojité přizpůsobování	Cíl: kompetence týmové spolupráce v neočekávané situaci je mnohem potřebnější než za normálních podmínek. Jak: udržování zdravého toku informací, aby všichni zúčastnění rozuměli cílům a strategii pro jejich dosažení a zajištění vzájemné podpory a informování. Nástroj: výcvik, diskuse postupů pro řešení problémů.
Využití co největšího počtu dostupných technologií	Cíl: technologické kompetence. Jak: umět provozovat umístěné technologie a nástroje (dýchací zařízení) a přizpůsobit užití dostupných technologií podmínkám a mít povědomí o tom, jak získat informace pro řešení, jak zapojit náhradní instrumenty apod. Nástroj: praxe, výcvik

Zacílení na výkon a strategie	Cíl: Povědomí a schopnost ovládat vlastní poznávací procesy, mít povědomí o prioritách a schopnost měnit pořadí priorit. Jak: ochranou proti samolibosti, tunelovému vidění, víře v náhlou spásu apod. Nástroj: výcvik, simulátor.
Udržovat spolupráci v týmu	Cíl: umět se soustředit na problém. Jak: soustavně vytvářet zdravé sebevědomí týmu. Nástroj: výcvik, simulátor.

Podle poznatků shrnutých v práci [12] je třeba při řízení provozu technického díla do území zvážit veškeré známé údaje a zkušenosti. Je třeba zvažovat zdroje všech rizik dle přístupu All-Hazard-Approach [13,14]. Do uvedeného souboru patří i škodlivé jevy, které jsou důsledkem vzájemných reakcí daného technického díla s jeho okolím za podmínek normálních, abnormálních i kritických,

Dle poznatků shrnutých v práci [2] je pro úspěšné zvládnutí rizik při provozu složitých technických děl třeba dodržovat požadavky na bezpečný provoz, tj. respektovat pokyny zmíněné výše v odstavci 2.4. Při aplikaci opatření a činností je nezbytné brát v úvahu velikosti projektových pohrom zvážených v projektu, kterými je technicky zajištěna pasivní ochrana, protože účinnost organizačních opatření v oblasti řízení je vždy nižší než u opatření technických, u kterých dosahuje až 80%.

Z pohledu potřeb praxe, je třeba bezpečnost technického díla při provozu udržovat na jisté úrovni a pomocí zlepšování kultury bezpečnosti a resilience ji kontinuálně zvyšovat. Podle práce [45] je resilience (houževnatost) definována takto: *„Houževnatost je potenciál systému, který spočívá ve specifickém uspořádání, které udržuje funkce a zpětné vazby systému, které zahrnují schopnost systému reorganizovat se na základě změn vyvolaných poruchami“.* Řízení resilience, které má dva cíle:

1. Zabránit, aby se systém dostával do nežádoucích stavů v důsledků vnějších poruch a vnější zátěže.
2. Uchovat prvky aktivující systémovou reorganizaci a obnovu v důsledku masivních změn.

Pro zajištění bezpečného provozu technického díla je nutno ve složitém světě dodržovat jistá pravidla, tj. provozní předpisy (provozní řády), které zpracovává provozovatel v souladu s platnou legislativou a má za ně odpovědnost. V řadě oblastí provozní předpisy musí upravovat požadavky zacílené na bezpečnost, které jsou stanoveny zákony (průmysl, doprava, ochrana osob a majetku, ochrana životního prostředí, stavebnictví, veřejný zájem, finanční sektor, obchod apod.).

Provozní předpisy jsou součástí provozní dokumentace technického díla [12]. Respektují doporučení zhotovitele i příslušné legislativní požadavky, tj. zohledňují veřejný zájem, ochranu veřejných aktiv, a ochranu aktiv technického díla, která jsou důležitá pro bezpečnost technického díla, tj. pro spolehlivé plnění úkolů, ke kterým je technické dílo vytvořeno, tj. upravují:

1. Pravidla pro zajištění:

- bezpečného provozu technických zařízení z pohledu technologie, tj. technologické postupy pro používání určitého zařízení, a to za podmínek normálních, abnormálních a kritických,
- a bezpečných výrobků.

2. Pravidla pro zajištění:
   - bezpečného pracoviště, a to za podmínek normálních, abnormálních a kritických
   - a dobrého výkonu.
3. Pravidla pro bezpečí lidí na pracovišti, a to za podmínek normálních, abnormálních a kritických.

Každé technické zařízení umístěné v provozu má jistý úkol, který musí splnit bezpečně, tj. spolehlivě, a přitom neohrozit sebe a své okolí [12]. Je faktem, že každý problém v materiálu, ze kterého je zařízení zhotovené, ovlivňuje plnění daného úkolu. Zkušenosti ukazují, že se tak děje až od určité velikosti problémů. Proto důležitou roli hrají inspekce technických zařízení během provozu. Inspekce označuje lidské činnosti, které spočívají v úředním dohledu, odborném dozoru, věcné kontrole, podrobné kontrolní prohlídce a podobně. Z hlediska bezpečnosti technických děl má velký význam ***Risk Based Inspection (RBI)*** [12].

Předmětná inspekce se soustřeďuje na specifická technická zařízení, jako jsou tlakové nádoby, výměníky tepla a potrubí v průmyslových zařízeních a pomocí metod kvalitativně nebo kvantitativně posuzuje úroveň rizika sledovaného technického zařízení. Tím umožňuje ekonomickou optimalizaci údržby, které se dosahuje tím, že se posuzuje úroveň rizika selhání a v případě, že se jeho úroveň blíží k nepřijatelnému limitu rizika, tak se provádí opravy a údržba. Vychází z výsledků nedestruktivních testů, které se používají se v rámci permanentního monitoringu, při intervalových měření i nárazově při problémech. Obecně je *RBI* součástí řízení rizik a spolehlivosti [12].

Vzhledem k dynamickému vývoji světa, všechna rizika nelze eliminovat, a proto pro zmírnění rizik je třeba používat systém pro podporu rozhodování a plán řízení rizik, jejichž modely jsou v práci [12]. Aplikace DSS umožňuje odhalit zdroje rizik jednotlivých variant provozu technického díla, jejichž realizace může narušit koexistenci technického díla a jeho okolí, a to dnes i v budoucnu. Při výběru optimální varianty hraje roli:

- dosažená úroveň bezpečí a udržitelného rozvoje při aplikaci varianty,
- technická proveditelnost opatření s tím, že se bere vhodnost opatření pro daný systém,
- materiálová náročnost i energetická náročnost,
- rychlost realizace,
- nároky na kvalifikovaný personál,
- nároky na informační zajištění,
- nároky na finance,
- nároky na odpovědnost,
- nároky na řízení / organizaci v území apod.

Rozhodování o výběru varianty usnadní odpovědi na sedm otázek, které jsou uvedeny v odstavci 6.2. Z ekonomického pohledu je vhodné provést rozhodování o vhodné variantě pro dané místo na základě skórování rizik a přínosů technického díla pro provo-

zovatele a veřejnou správu předmětného území po dobu očekávané životnosti technického díla. Rozhodnutím o variantě jsou také určeny zdroje rizik, které se musí dále při provozu průběžně sledovat a řídit.

Vzhledem k dynamickému vývoji světa, je pro zajištění bezpečného procesu provozu technického díla v čase uveden v práci [12] generický model plánu řízení rizik při provozu.

Pozornost při vypořádání rizik je třeba věnovat kritickým místům technických děl, tj. prvkům, komponentám, systémům a jejich propojení, které jsou zásadní pro bezpečný provoz. Jde o položky, které jsou zároveň velmi důležité a velmi zranitelné. Zranitelnost položek se určuje pomocí kontrolních seznamů. Příklad je v tabulce 5; další je v práci [12].

Tabulka 5. Kontrolní seznam pro identifikaci míry zranitelnosti technického díla.

Kritérium	**Hodnocení**
Jaká je citlivost jednotlivých položek kritického majetku na pohromy dle typu?	
Jaká je citlivost jednotlivých položek kritického majetku na fyzický útok?	
Jaká je citlivost jednotlivých položek kritického majetku na útok insiderů?	
Které položky kritického majetku nejsou chráněny?	
Které položky kritického majetku jsou málo chráněny?.	
Jak jsou položky kritického majetku citlivé na kybernetický útok?	
CELKEM	

6.5. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti při údržbě technického díla

Údržba znamená pravidelnou péči, soustavnou činnost za účelem zpomalení fyzického opotřebení a předcházení poruchám a odstraňování drobnějších závad. Údržbou se majetek regeneruje beze změny pořizovací ceny, jejím prováděním nemůže vzniknout nová věc. Hradí se z provozních – běžných – prostředků. Opravy a údržba neznamenají technické zhodnocení majetku.

Výzkum [12] ukázal, že je vysoce nebezpečné, že je stále údržba opomíjená. Nákladově a přínosně řízená údržba společnosti nebo majetku podniku je absolutně podstatná pro maximální ziskovost a dlouhodobé přežití společnosti, podniku nebo infrastruktury [12]. Poznatky shromážděné v odborné literatuře i zkušenosti z praxe [12] ukazují, že zanedbaná nebo nesprávně prováděná údržba vede k růstu zranitelnosti sledované položky, a v praxi pak dochází k častějšímu selhání položky.

Každé technické zařízení se opotřebovává, a to tím rychleji, když plní náročné funkce, anebo pracuje v agresivním prostředí. Proto již projektant při řešení technických záležitostí zvažuje nároky údržby. Z hlediska bezpečnosti musí projekt technického díla i

údržba respektovat místně specifická rizika; model situace je uveden na obrázku 24. Z hlediska potřeb praxe musí být údržba technicky proveditelná a ekonomicky přijatelná [12].

Obr. 24. Koncept projektu objektu a údržby objektu, který respektuje rizika.

O každé položce rozhoduje člověk, a proto je nutno zohlednit předmětné poznání. Je pochopitelné, že s ohledem na dostupné zdroje, údržba musí být z hlediska finančního optimální. Proto dle [46] je třeba vytvořit reprezentativní soubor možných scénářů údržby, určit a vyhodnotit dopady jejich rizik s ohledem na kvalitní chod provozu, a pak z nich vybrat kvalitní, tj. průhlednou, opakovatelnou a správnou metodou optimální scénář údržby z pohledu technického i finančního. Přitom je důležité zvažovat bezpečnost, životnost a spolehlivost zařízení. Jelikož u provozů technických děl se nejedná o statické problémy, ale o problémy dynamické, je vhodné provádět řízení bezpečnosti, ve kterém je obsažena problematika údržby, pomocí indikátorů zvažujících změny v čase.

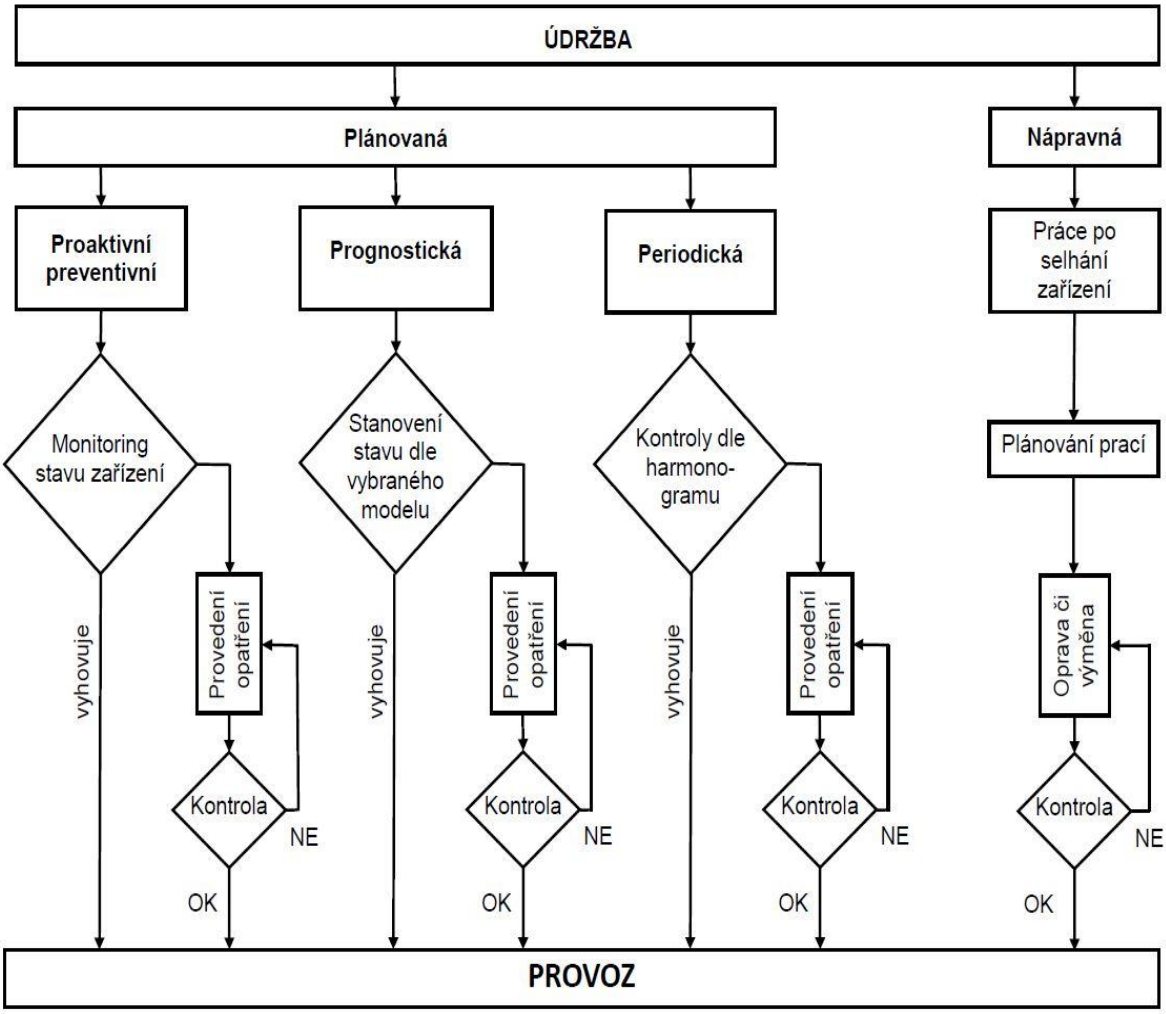
Pro posouzení úrovně údržby jsou nutné dokumentace a inspekce, včetně pravidelných auditů, a to především vnějších. Podle amerických modelů bezpečnost funkcí podniku či zařízení zajišťuje dostupnost (dosažitelnost) a vyžaduje aplikaci konceptu integrální bezpečnosti zahrnující spolehlivost a udržitelnost [12].

Cílem opatření a činností údržby zařízení, komponent a systémů technického díla je zajistit rostoucí požadavky na produkty nebo výrobky, které poskytují. Údržba zvyšuje životnost klíčových komponent i celého systému [12]. Při provádění údržby je třeba dodržovat jisté postupy a v případech, kdy existují nebezpečí jako je možnost exploze, musí být používána specifická ochranná opatření. Proto je třeba údržbu důkladně naplánovat a připravit podle:

- návodů pro obsluhu a údržbu od výrobce,
- konstrukčních a projekčních podkladů,
- pracovního postupu, použitého pracovního prostředků, údajů o přítomných nebezpečných látkách,
- provozních zkušeností,
- zkušeností pracovníků obsluhy a údržby,
- podmínek provozu a místních podmínek,
- provozně poplachových plánů,
- poznatků kontroly o daném pracovním místě,

- rozmístění ochranných prostředků (např. čidel pro signalizaci požáru),
- možných zdrojů ohrožení v místě a jeho okolí, a to včetně okolního vybavení.

V současné době se v kritických technických dílech prosazuje tzv. chytrá údržba [12]. Tato údržba dle [47] se označuje jako proaktivní preventivní údržba a dle prací sledovaných v publikaci [12] jako údržba založená na podmínkách (CBM – condition–based maintenance). Její plán údržby je řízen výsledkem sledování stavu komponent. Údržba se provede, jakmile sledování stavu komponenty ukáže překročení jisté prahové hodnoty popisující stav komponenty (tj. jistou kritičnost). Je založena na neperiodických inspekcích a je cenově výhodná. Obrázek 25 sestavený dle prací [12,46,47] ukazuje rozdělení používaných typů údržby.



Obr. 25. Přehled používaných typů údržby.

Prediktivní/ prognostická používá modely, jejichž seznam je uveden v práci [12], a pomocí kterých se aproximují data z inspekce technických zařízení. Výsledkem je pak degradační křivka, podle které se určuje doba provedení údržby nebo inspekce, tak, aby pravděpodobnosti výskytu selhání komponent a systémů byly přijatelné. Její nevýhodou je, že nebere v úvahu náhlé změny. Proto je v praxi u kritických zařízení

upřednostňována proaktivní preventivní údržba [47], která se opírá o monitoring stavu zařízení a reaguje tak, aby nenastal špatný stav zařízení.

Pro hodnocení kritičnosti technického zařízení se v praxi používá pětistupňová stupnice [19], která je uvedena výše v odstavci 6.3.

Z uvedených poznatků je zřejmé, že proaktivní preventivní údržba položky zajišťuje bezpečnost položky i celého technického díla, když se údržba provede dříve než stav položky je špatný. Takto stanovené požadavky proaktivní preventivní údržby vyžadují monitoring sledované položky a náhradu či údržbu ještě funkční položky. Z ekonomického hlediska je tudíž uvedený typ náročný, a proto je v praxi odůvodněná jen u kritických položek.

Jelikož technická díla mají technická zařízení, komponenty a systémy různého typu a složitosti, která pracují v různých podmínkách, tak základním úkolem při přípravě realizace proaktivní preventivní údržby je sestavit pro každou kritickou položku místně specifickou stupnici na hodnocení stavu. Při jejím sestavování je třeba vycházet z požadavků projektanta, výrobce, provozních zkušeností a platných norem.

6.6. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti při modernizaci technického díla

Rekonstrukce / modernizace je v architektonickém pojetí je rozsáhlá prototypová obnova poškozených, časem opotřebovaných nebo zničených architektonických památek, historických budov nebo jejich částí a na rozdíl od opravy znamená vždy výraznou změnu existujícího stavu [48]. Je již po staletí běžnou praxí. V současné době existuje řada legislativních dokumentů, které definují "rekonstrukci" jako návrat poškozené budovy do dřívějšího stavu zavedením nových materiálů. Úzce souvisí s architektonickými koncepcemi restaurování (oprava stávající stavební struktury) a konzervace (prevence dalšího chátrání), přičemž nejrozsáhlejší formou rekonstrukce je vytvoření repliky zničené stavby. Existují různé přístupy k rekonstrukci, které se liší mírou věrnosti originálu a citlivostí na provedení. Každá rekonstrukce musí být prováděna podle pravidel, která jsou v národní legislativě.

Rekonstrukce jednotlivých entit se musí řídit inženýrskými znalostmi a zkušenostmi, tj. logickým postupem shrnutým v legislativě [19]. Z uvedené knihy vyplývá, že rekonstrukce každého objektu musí zohlednit jak požadavky na projektování, tak zkušenosti z minulého provozu. Někdy je třeba řešit problémy spojené s chybami, které vznikly v původním návrhu. Často je nelze odstranit, ale pouze zmírnit. Proto někdy dochází k mnoha obtížím při rozhodování o projektu rekonstrukce.

Cílem komplexního návrhu rekonstrukce zařízení je vytvořit výrobní proces, který je ziskový, ekonomický, bezpečný a neohrožuje veřejná aktiva, zejména člověka a životní prostředí. Toho lze dosáhnout optimalizací ochranných, ekonomických a funkčních kritérií [19].

Rekonstrukce neboli obnova patří mezi projekty se zvláštními potřebami, jelikož se značně liší od ostatních typů stavebních projektů. Mezi nejdůležitější potřeby se řadí

správné zohlednění harmonogramu výstavby a odklonů dopravy, přeložek inženýrských sítí, zajištění stavebního povolení a vyjádření od všech dotčených orgánů [49]. Dle prací [49,50] je třeba v oblasti proveditelnosti a fázování výstavby provádět dále uvedené činnosti:

1. Přezkoumání proveditelnosti a fázování by mělo zahrnovat celý rozsah obnovy tak, aby byl minimalizován počet nutných změn, které naruší běžný provoz.
2. Přezkoumání etapizace pomáhá zúčastněným stranám prozkoumat proveditelnost plánu realizace a zjistit, zda projekt může být dokončen buď za bezpečného a nepřetržitého provozu objektu nebo během plánovaných výluk. Z toho může v některých případech dojít ke změnám projektu, a to tak, aby bylo možné realizovat jednotlivé fáze projektu výstavby.
3. Výstupem přezkoumání bude seznam omezení, která by měla být během výstavby zohledněna. V této návaznosti by měly být určeny činnosti, které nelze provádět v běžných provozních hodinách. Dále by se měl stanovit předběžný počet a typ požadovaných změn provozu.
4. V každém takto rekonstruovaném objektu musí být projektový tým, který určuje oblasti a zařízení, které nelze současně uzavřít nebo vyřadit z provozu tak, aby byl zajištěn nepřetržitý a bezpečný provoz objektu.
5. Některé starší části objektu mohly být vystavěny z nebezpečných materiálů (azbest, rtuť, olovo), z tohoto důvodu je nutné, aby před zahájením prací byly provedeny správné asanační práce. Proto je zapotřebí přímá a správná komunikace a koordinace mezi objednatelem, zhotovitelem a orgány ochrany životního prostředí. Odstraňování takto nebezpečného materiálu totiž vyžaduje zvláštní povolení a specializované vybavení firem, které se vyloženě na tuto činnost specializují.
6. Pro dodržení milníků je zapotřebí identifikovat materiály, které mají dlouhý interval dodání a položky, které dodává objednatel sám.
7. Dále je zapotřebí určit činnosti, které mají být prováděny v okolních oblastech, jedná se například o přeložky inženýrských sítí nebo provádění prací, které se vyskytují v okolí objektu, tedy spadají pod jiné vlastníky. Tyto činnosti obvykle vyžadují další povolení a mohou práce na projektu značně pozdržet, jelikož má obvykle realizační tým jen malou možnost ovlivnění urychlení procesu žádosti o povolení a kontroly.

V oblasti řízení systému projektů jde o jeden z klíčových vstupů. Zajišťuje přezkoumání a revizi priorit projektu, řízení pracovní zátěže a přidělování sdílených zdrojů (např. speciálních služeb). Proto je třeba sestavit integrovaný a celopodnikový řídicí systém. Jeho nedílnou součástí musí být centralizovaná databáze, která slouží pro ukládání záznamů o projektech nejen, že usnadňuje rozhodování, ale také zvyšuje spolehlivost přijatých rozhodnutí. Do této databáze by měly být zavedeny správné postupy pro standardizaci vstupních údajů z různých oddělení a pro zajištění pravidelné aktualizace záznamů o projektech.

Činnosti, jež mají zvláštní předpoklady nebo vyžadují zvláštní ohledy, by měly být identifikovány včas, a to v raných fázích plánování projektu. Jedná se například o:
- odstranění nebezpečného materiálu (rtuť, olovo, azbest),
- zajištění povolení od dotčených orgánů,
- povolení vjezdu těžké techniky do určitých oblastí,

- schválení signalizačního zabezpečovacího zařízení a dopravního značení v okolí stavby,
- práce v historických oblastech (např. povolení úřadu památkové péče, archeologů apod.).

Důležité je i správné rozvržení pracovní doby a čet na realizaci projektu tak, aby bylo možno plnit milníky v harmonogramu, a zároveň byl dodržován noční klid a eliminovány hlučné práce ve večerních hodinách.

Je důležité poznamenat, že vzhledem k povaze některých projektů obnovy technického díla se mohou speciální služby, jako jsou přerušení provozů, stát jedním z klíčových faktorů ovlivňujících termín dokončení projektu. V těchto případech by se měly používat speciální harmonogramy, jako jsou výhledové harmonogramy s krátkými časovými úseky, které umožňují plánovat a sledovat práce na projektu na úrovni detailů. V opačném případě může nedostupnost zdrojů nebo speciálních služeb nepříznivě ovlivnit využití služeb a vést ke značným zpožděním a škodám.

Správné vedení záznamů je důležité pro současnou analýzu příčin a následků změn a zpoždění projektu. Zavedení účinného systému řízení změn pomůže předejít zbytečným a nákladným šetřením v případě jakýchkoli sporů. Jakmile je zavedena změna, měl by být prozkoumán její dopad na harmonogram projektu a výsledky je třeba řádně a včas sdělit příslušným stranám. Všechny předpoklady a podklady pro analýzy dopadů by měly být rovněž řádně zaznamenány.

Zdroje rizik při rekonstrukci jsou stejné jako při projektování a výstavbě [19]. Zkušenosti ukazují, že velkou roli hrají:
- stavebně-technologická a projektová rizika spojená především s projektovou dokumentací a výstavbou,
- finanční a technická rizika spojená se: samotnými technickými zařízeními a vybavením; kvalitou použitých materiálů; chováním lidí; a údržbou samotné stanice.

Při rekonstrukci stanice technických objektů vznikají další zdroje rizik. Kritická analýza dat o průběhu rekonstrukcí technických děl shromážděná v archivu [16] odhalila, že se jedná o zdroje rizik během reálných prací:

1. Demoliční práce (znečištění azbestem, hlukem, prachem, vibracemi; propady; zasypávání).
2. Betonářské práce (kvalita materiálu; problém kvality prací v zimě a při vysokých teplotách; vibrace atd.).
3. Práce na ocelových konstrukcí (kvalita materiálu; svařování, manipulace s nadrozměrnými konstrukcemi, požár atd.).
4. Izolační práce (problémy práce s horkými materiály, vystavení chemikáliím, vdechování škodlivých látek, oheň, výbuch).
5. Práce uvnitř stanice objektu (přerušení provozu, úraz elektrickým proudem – 22 kV, zkrat, požár).
6. Elektroinstalační práce (úraz elektrickým proudem, zkrat, požár, výbuch).
7. Instalace řídicího systému na požadované úrovni automatizace a s tím spojené nezbytné vybavení snímači, senzory, hardware a software.

8. Organizace a legislativa (nedodržování projektové dokumentace rekonstrukce; zpoždění prací; nízká kvalita řízení; problémy s dodávkami materiálů; nízká kultura bezpečnosti; špatná pracovní morálka atd.).

Pro zpracování plánu rekonstrukce technického zařízení či technického díla je třeba:
- nejprve udělat procesní model rekonstrukce,
- identifikovat zdroje konkrétních rizik,
- zpracovat zadávací podmínky pro projekt rekonstrukce,
- zpracovat projekt a plán řízení rizik, které jsou očekávány při rekonstrukci,
- zpracovat harmonogram rekonstrukce a určit odpovědnosti,
- zavést monitoring rekonstrukce a podle potřeby provádět vypořádání rizik.

6.7. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti při ukončení provozu technického díla

Podle poznatků shrnutých v práci [21] je třeba, aby proces vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití byl bezpečný. Důvodem důrazu na bezpečnost je, že příklady likvidace starých zátěží, které vznikly špatným provedením sledovaného procesu, ukazují, že společnost musí následně vynaložit velmi vysoké náklady na jejich likvidaci z důvodu zajištění bezpečnosti lidí. Sledovaný proces je nákladný. Na základě zkušeností z praxe, lze náklady snížit tím, že proces buse řádně naplánován a připraven předem.

Z důvodu velké rozmanitosti technických děl, konkrétní procesy vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití jsou specifické. Z důvodu ochrany lidí a životního prostředí je nutno při všech činnostech respektovat potřeby občanů a veřejný zájem. Práce [21] navrhuje upravit legislativu, např. stavební zákon by měl ukládat odpovědnému orgánu veřejné správy, aby:
- do každého stavebního povolení a kolaudačního rozhodnutí spojeným s technickým dílem zapracoval povinnost provozovatele vytvářet finanční fond na práce spojené s procesem vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití,
- předmětný fond kontroloval a nedovolil ho vyčerpat na jiné činnosti.

Legislativa musí jasně zdůraznit veřejný zájem a odpovědnost osob a subjektů, které rozhodují příslušné záležitosti. Zároveň musí legislativa dát dostatečnou právní sílu veřejné správě, aby činnosti nutné ve veřejném zájmu mohla vynutit. Současně s tím je třeba zajistit výchovu a vzdělanost v oblasti řízení a vypořádání rizik a cíleně podporovat budování kultury bezpečnosti v českém prostředí, a to hlavně motivací občanů.

Vzhledem k dynamickému vývoji světa, všechna rizika spojená s procesem vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití nelze eliminovat, a proto pro zmírnění rizik je třeba používat systém pro podporu rozhodování a plán řízení rizik, jejichž

modely jsou v práci [21]. Aplikace DSS umožňuje odhalit zdroje rizik jednotlivých variant procesu vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití, jejichž realizace může narušit životní prostředí a ohrozit lidi, a to dnes i v budoucnu. Při výběru optimální varianty, hraje roli:

- dosažená úroveň bezpečí a udržitelného rozvoje při aplikaci varianty,
- technická proveditelnost opatření s tím, že se bere vhodnost opatření pro daný systém,
- materiálová náročnost i energetická náročnost,
- rychlost realizace,
- nároky na kvalifikovaný personál,
- nároky na informační zajištění,
- nároky na finance,
- nároky na odpovědnost,
- nároky na řízení / organizaci v území apod.

Rozhodování o výběru varianty usnadní odpovědi na sedm otázek, které jsou uvedeny v odstavci 6.2. Z ekonomického pohledu je vhodné provést rozhodování o vhodné variantě pro dané místo na základě skórování rizik a přínosů technického díla pro provozovatele a veřejnou správu předmětného území po dobu očekávané životnosti technického díla. Rozhodnutím o variantě jsou také určeny zdroje rizik, které se musí při provozu průběžně sledovat a řídit při realizaci procesu vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití pro realizátora procesu a veřejnou správu předmětného území.

Vzhledem k dynamickému vývoji světa je pro zajištění bezpečného procesu vyřazení technického díla z provozu, vyčištění území a odstranění odpadů a následného předání uvolněného území do dalšího civilního využití v práci [21] uveden generický model plánu řízení rizik při realizaci procesu.

6.8. Netechnická opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla

Jde o opatření a činnosti v oblastech: řízení; plánování; rozdělení kompetencí a odpovědností; organizační uspořádání; hardware; právní a provozní předpisy; informační systémy; software; vedení dokumentace; vzdělávání; a specifický výzkum pro podporu bezpečnosti [12]. Opatření a činnosti z oblasti řízení jsou uvedeny výše, a proto jim není dále věnována zvláštní pozornost. Podrobně jsou zmíněny oblasti, na jejichž kvalitě kvalita řízení, a tím i bezpečnost technického díla závisí.

Práce [2] uvádí příklady software a ukazuje, že každé software bylo vyvinuto pro určité podmínky. Při jeho aplikaci v jiném prostředí, je třeba ověřit podmínky transferu technologií [18]. Nepřesná či chybná software se podílely na řadě havárií a selhání technických zařízení a technických děl [12]. V posledních letech jsou velkým rizikem pro

bezpečnost technických zařízení a technických děl podvodná software, jak ukazují výsledky shrnuté v práci [31]. Problematika ocenění kvality software je velmi široká a rozmanitá. Z hlediska její šíře, není dále sledována.

6.8.1. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla z oblasti plánování

Plánování v technickém díle založené na stanovení možných dopadů a na ceně, kterou technické dílo zaplatí za selhání, je zvláště nutné zaměřit se na ten majetek, který nejvíce vyžaduje investice [12]. Důležité je systémové pojetí, které dovoluje odhalit, že některé prvky, vazby či toky jsou vysoce zásadní pro stabilitu, kontinuitu a rozvoj organizace. V těchto případech je nutno v zájmu bezpečnosti naplánovat a provést specifická opatření a tyto prvky, vazby či toky speciálně zodolnit a případně zálohovat, a to i několikrát [12].

Plánování pro zajištění bezpečného provozu technického díla 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.) [12].

***V případě, ve kterém neexistuje účinná obrana technického díla před pohromou, tj. realizací závažného rizika, je nutností být připraven*.** To znamená, že organizace musí mít připraveny postupy, jimiž se musí provést odezva na situaci zaměřená na stabilizaci zasažené části technického díla 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.

Podle poznatků shromážděných v práci [12], je plánování 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 [12], a to:

1. Analýza rizik, která stanovuje strategická pravidla:
   - základní klasifikace klíčových procesů a zdrojů a jejich zabezpečení,
   - plán zachování funkčnosti.

2. Zajištění dat a informací, aplikace znalostí a návrh cílů.

3. Seznam konkrétních realizačních opatření a návrh postupů na jejich realizaci (lze využít nástroje multikriteriálního rozhodování, např. metoda kritické cesty, Petriho sítě, optimalizační metody síťové analýzy apod.) [3]. Musíme si uvědomit, že např. proces zvládnutí nouzové situace v technickém díle probíhá v jistém, opakujícím se životním cyklu:
   - normální podmínky / provoz technického díla, tj. žádná pohroma,
   - reakce na vznik nouzové situace vyvolané výskytem pohromy,
   - obnova základních funkcí technického díla,
   - prozatímní provoz technického díla,
   - obnova plného provozu technického díla,
   - normální provoz technického díla po obnovení plné funkce.

Obnova plného provozu znamená přechod z nouzového provozu technického díla na plný provoz. Obvykle je nejvíce při plánování opomíjená [12].

Dalším příkladem je formální postup pro proces zvládání konkrétní nouzové situace [12], 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.

V těchto souvislostech v případě výskytu nadprojektové pohromy (tj. pohromy, proti které se již nedělají nadstandardní preventivní opatření v územním plánování, projektování, výstavbě a provozování objektu, infrastruktury, v systému péče o zdraví, bezpečí, životní prostředí a veřejné blaho), a proto jsou vybudovány ochranné systémy v rámci nouzového a krizového řízení pro bezpečnost jen vybraných chráněných aktiv (životy a zdraví lidí a majetek). Je proto nutno zdůraznit, že v doposud vybudovaném systému ochrany nejsou dostatečně zohledněny vnitřní vazby jdoucí napříč technického díla a jeho okolím. Tento problém je třeba v zájmu bezpečnosti a rozvoje technického díla vyřešit, tj. odstranit, anebo alespoň snížit na žádoucí úroveň druhotné dopady v řetězcích dopadů, které souvisí s výskytem konkrétních pohrom [12].

Pro každý kritický proces se nejprve pro potřeby řízení musí určit možné scénáře. Za vše odpovídá vrcholový management [12]. 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 technickém díle založené na stanovení cílů, odstranění možných problémů a na ceně, kterou technické dílo zaplatí za selhání, je zvláště nutné zaměřit se na životy lidí, životní prostředí a ten majetek, který nejvíce vyžaduje investice a sledovat dopady na vazby mezi prvky a vazby napříč celého systému infrastruktury. Poslední výzkumy [12] ukazují, že zvláště důležité je sledovat spletitost vnitřních závislostí napříč kritickou infrastrukturou. Při znázornění technického díla jako systému systémů se zjistí, že některé prvky, vazby či toky jsou vysoce zásadní pro stabilitu, kontinuitu a rozvoj technického díla. Proto jim musí být věnována zvláštní pozornost při formulaci opatření a činností, které podporují bezpečnost.

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.

6.8.2. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla z oblasti rozdělení odpovědností

Na základě výzkumu, popsaného v práci [1] z pohledu bezpečí a rozvoje lidí, území i státu je odpovědnost za řízení rizik složitých technických děl a procesů nutno stanovit 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.

Odpovědnosti za řízení rizik technického díla na úseku propojení veřejné správy a managementu technického díla musí být stanoveny pro úrovně řízení:

1. A1 - politická (parlament, vláda, veřejná správa).
2. A2 - strategická (veřejná správa, vlastník, investor, provozovatel).
3. A3 - taktická (veřejná správa, vlastník, investor, provozovatel).
4. A4 - operativní / funkční (provozovatel).
5. A5 - technická (provozovatel).

Odpovědnosti za řízení rizik technického díla na úseku technického díla musí být stanoveny pro úrovně řízení:

1. B1 – vrcholové řízení technického díla.
2. B2 – řízení projektů technického díla.
3. B3 – řízení procesů technického díla.
4. B4 - řízení konkrétních opatření a činností technického díla.

Detaily jsou uvedeny v pracích [1,2]; v práci [1] jsou pro jednotlivé úrovně uvedeny detailně položky, za které daná úroveň odpovídá.

6.8.3. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla z oblasti práva a předpisů

Řízení a vypořádání rizik jsou činnosti, které jsou náročné jak na znalosti, tak na finance. U technických děl, jenž:

- mají potenciál ohrožovat životy, zdraví a bezpečí lidí i životní prostředí,
- jsou zásadní pro zajištění potřeb a služeb pro život, zdraví a bezpečí lidí,

musí z důvodu ochrany lidské společnosti být požadovaná opatření a činnosti, které jsou kodifikovány legislativou, dozorovány státními orgány a popř. vynucovány soudní mocí.

Platné legislativní předpisy v České republice pro zajištění BOZP, ochrany obyvatel, ochrany životního prostředí, ochrany území a bezpečnosti výrobků jsou uvedeny ve Sbírce zákonů; některé z nich jsou detailně analyzovány v pracích [1,8,12,17,19,34].

Pro řadu technických zařízení, systémů a komponent je třeba pro zajištění bezpečnosti dodržovat:

- platné normy – vybrané jsou uvedeny v tabulce 2,
- provozní předpisy, o kterých bylo pojednáno v odstavci 6.4. a v [12],
- zásady dobré inženýrské praxe.

6.8.4. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla z oblasti vzdělávání a výcviku

Poznatky a zkušenosti shrnuté v pracích [1-3] a dalších ukazují, že řízení a vypořádání rizik není triviální záležitost. Jmenované činnosti vyžadují znalosti, zkušenosti, finance a čas na sběr dat, stanovení rizik a práce s riziky. Proto vyžadují znalosti a schopnost znalosti uplatnit podle potřeby praxe. Proto je důležité vzdělání a výcvik.

Vzdělávání je proces získávání určitých schopností a dovedností, spojených se snahou začlenit se do dané kultury a společnosti a aktivně přispívat k jejich rozvoji. Probíhá ve všech fázích lidského životního cyklu. Zasedání Rady EU v Lisabonu ve dnech 23. - 24. března 2000 postavilo vzdělávací politiku do popředí zájmů a cílů Evropské unie a tyto záměry byly potvrzeny na zasedání Rady ve Stockholmu v roce 2001.

Proces vzdělávání tvoří speciálně organizované činnosti probíhající podle stanoveného pořádku a mající určité cíle. Tyto činnosti se vyznačují různými kombinacemi kolektivního a individuálního vyučování, různými stupni samostatnosti osob a různými způsoby řízení učebního procesu. Potřeba dalšího vzdělání plyne z potřeb praxe.

Cíl a obsah vzdělávání, jeho organizace, formy a prostředky se v historické době podstatně měnily v závislosti na potřebách výroby a změnách ve společenských vztazích. Kvalita vzdělání není daná množstvím poznatků, ale jejich ucelenostií a hloubkou.

Hlavním cílem následných hospodářských a vzdělávacích politik Evropské unie je "vytvořit nejvíce konkurence schopnou a nejvíce dynamickou ekonomiku založenou na znalostech a vzdělávání na světě, schopnou udržet hospodářský růst rozšiřováním a zlepšováním pracovních míst a větší sociální soudržností". Rozvinuté země se potýkají s vyčerpatelností zdrojů, a proto si již uvědomují, že vzdělávání je jedním z mála zdrojů, jehož objem lze trvale obnovit a dále zvýšit [52-54].

Potenciál a konkurenceschopnost každé společnosti není jen ve výrobních kapacitách strojů a technologických zařízení, ale především v zaměstnancích a know-how, tedy v

nehmotném majetku. Pro rozvoj potřebuje každý podnik talentovaný personál, který je schopen generovat určité hodnoty. Aby bylo možné splnit očekávané požadavky, musí mít každý jednotlivec určité znalosti, dovednosti a motivaci. To znamená, že pro něj musí být vytvořeny podmínky, aby předmětné aspekty získal a rozvíjel. Základními podmínkami jsou ochrana zdraví a přístup ke vzdělání, protože inovace, které jsou nezbytné z hlediska rozvoje, vyžadují získání nových znalostí a přijetí nových dovedností.

Vzdělávání dospělých začalo v 19. století a kolem roku 1976 již mělo komplexní rámec a bylo chápáno jako vzdělávání a odborná příprava pracovníků v organizacích, jejichž cílem je zlepšit, prohloubit a rozšířit dosažený stupeň pracovních schopností [53]. Dnes je specifická forma vzdělávacích systémů přizpůsobena specifikům a potřebám podniku a legislativě příslušné země.

Pracovní vzdělávání je plánovaný proces úpravy postojů, znalostí a dovedností učením zaměřeným na dosažení efektivního výkonu v určité činnosti nebo rozsahu činností. Jeho cílem z hlediska práce je rozvíjet schopnosti jednotlivce a uspokojovat současné a budoucí potřeby organizace týkající se pracovní síly [55-58].

Např. MAAE [59] začala věnovat velkou pozornost vzdělávání krátce po roce 2000 s ohledem na zvýšenou fluktuaci kritického personálu v jaderných zařízeních. Hlavním cílem bylo zavedení integrovaného přístupu k řízení jaderných zařízení zaměřeného na bezpečný a spolehlivý provoz, který je založen na řízení znalostí. Důraz je nyní kladen na:

- nahrazení zastaralých přístupů novými, které jsou výsledkem výzkumu a provozních zkušeností a jsou bezpečnější
- a podporu kultury bezpečnosti.

Důraz se začal klást na pracovní vzdělávání, zejména na vzdělávání a školení kritického personálu na všech úrovních řízení. Bylo zdůrazněno, že plán vzdělávání a odborné přípravy musí být řešen dlouhodobými potřebami jaderného zařízení [60]. To znamená činnostmi, které souvisejí s bezpečností a kulturou bezpečnosti. Na základě zkušenosti z praxe, plán školení musí být pravidelně přezkoumáván s ohledem na provozní zkušenosti.

Školení personálu jaderných zařízení musí být systematické a musí odrážet potřeby konkrétních pracovních míst, a to jak znalostí, tak dovedností. Musí také zahrnovat provozní i havarijní plánování. Musí vycházet z osvědčených postupů a poučení [61].

Podle [62-64] musí školení poskytovat požadované kompetence pro danou práci, přičemž kompetence znamená kombinaci znalostí, dovedností a postojů a školení pro spolupráci. Jaderný regulační orgán země musí pravidelně kontrolovat kvalitu školení kritického personálu [63]. Vedle toho je vzdělávání v oblast jaderného průmyslu podporováno a organizováno i OECD / NEA, EURATOM a WANO.

6.8.5. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla z oblasti financí

Na základě poznatků shrnutých v pracích [2,12,19] analýzy odborné literatury a zkušeností z praxe [65] opatření pro řízení a vypořádání rizik nejsou levná záležitost. Je třeba finance na:

- odborné práce spojené s identifikací, přípravou a naplánováním opatření a činností,
- vlastní provedení opatření a činností a s tím spojené náklady na personál, technická zařízení a testování.

Vzhledem k tomu, že financí není nikdy dostatek, je třeba s nimi neplýtvat. Proto jak bylo výše uvedeno a z obrázku 14 vyplývá, je třeba se řídit zásadou, že riziko, na jehož vypořádání by byly potřebné finance vyšší než škody, které způsobí, se nevypořádává z důvodu hospodárnosti.

U technických děl, které patří do kritické infrastruktury státu, musí provozovatel dle platné legislativy (zákon č. 110/1998 Sb., zákon č. 240/200 Sb., Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, Nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů) zajistit bezpečnost. Náklady na bezpečnost při údržbě, modernizaci, rekonstrukci i opravě hradí z výdajů na investice. Kvalitní řízení nákladů na předmětné aktivity je v zájmu provozovatele, protože uvedené náklady snižují jeho zisk.

Na základě [37] pozornost při volbě opatření a činností pro řízení a vypořádání rizik ve prospěch bezpečnosti technických děl je třeba sledovat také finanční rizika, protože jejich realizace snižuje hodnotu technického díla. Jde hlavně o kreditní a tržní rizika [2]. Kreditní rizika zahrnují:
- riziko likvidity (schopnost realizátora opatření dostát svým finančním závazkům**)**,
- riziko nesplnění závazků (tzv. riziko dostupnosti), které se dále dělí na:
  - riziko spojené s dostupností (nedodržení závazků soukromým sektorem),
  - riziko spojené se selháním protistrany a ztrátou pro veřejnou správu,
  - riziko spojené se selháním protistrany a ztrátou pro realizátora opatření a činností,
  - riziko spojené s koncentrací realizátora opatření a činností na jednoho dodavatele,
- riziko spojené se zamítnutím podpory od veřejné správy pro realizátora opatření a činností.

Tržní rizika zahrnují:
- riziko poptávky v případě, že dodavatelem je veřejná správa,
- riziko poptávky v případě, že dodavatelem je soukromý subjekt,
- riziko zvýhodnění konkurence,
- ostatní tržní rizika jako jsou:
  - riziko měnové,
  - riziko kurzovní
  - a riziko úrokové.

Podle poznatků z výzkumu havárií a selhání technických děl shromážděných v pracích [12,19], příčinou havárií a selhání bylo šetření s financemi na nesprávném místě – buď se nezvažovala rizika, anebo se realizovala nejméně nákladná varianta, tj. varianta, která zvažovala jen rizika s nízkým ničivým potenciálem. Proto hlavním opatřením v oblasti financí pro bezpečnost technických děl, je v každém životním cyklu technického díla třeba zvažovat variantu, která zajistí ochranu lidí, životního prostředí a kritických objektů a infrastruktur, které jsou důležité pro rozvoj území.

6.8.6. Opatření a činnosti pro řízení a vypořádání rizik ve prospěch bezpečnosti technického díla z oblasti I&C

Jak již bylo uvedeno, automatizace v technických dílech se stále zvětšuje. Její základ tvoří systém I&C (infomační a řídicí systém). Opatření a činnosti pro řízení rizik technických děl ve prospěch bezpečnosti spojené s řídicími systémy byly uvedeny výše. Dále se zmíníme o dílčích problémech, které jsou typické pro sledovanou oblast, a to:
- bezpečnosti informací,
- kybernetické zabezpečení technických děl.

Informace a ještě více znalosti tvoří chráněný zájem (aktivum) stejně jako jiná významná aktiva, a to jak pro lidi, tak pro organizace libovolného typu, státní, veřejné, soukromé aj., a proto požadují přiměřenou ochranu. Bezpečnost informací (informační bezpečnost) technického díla je souhrn opatření a činností, který:
- ochrání informace před krádeží, ztrátou, poškozením, odepřením služby,
- vniknutím do systému zdrojů informací,
- zničením systémů zdrojů informací apod.;
- zajistí kontinuitu informací při provozu,
- minimalizuje provozní škody
- a maximalizuje návratnost investic a příležitostí pro bezpečí a udržitelný rozvoj.

Nejvíce efektivním při řízení bezpečnosti informací navrhovaného systému je využití již ověřené a standardizované metodiky, která usnadňuje a zrychluje návrhovou fázi řešení, jak se s tímto požadavkem vypořádat, a zároveň zaručuje dostatečně kvalitní vyřešení daného požadavku. V oblasti bezpečnosti informací je v předmětném směru návodem norma ISO/IEC 27001. Dle ní se bezpečnost informací opírá o naplnění požadavků na důvěrnost, integritu a dostupnost.

Důvěrnost (Confidentiality) znamená, že s údaji mohou nakládat (resp. je používat) jen osoby k tomu oprávněné. Jde o zajištění toho, že informace jsou přístupné nebo jsou sděleny pouze těm, kteří jsou k tomu oprávnění. Nikdo jiný je nesmí vědět, číst ani jinak používat (někdy se používá, že nikdo nesmí zjistit obsah údaje).

Integrita (Integrity) je zajištění správnosti a úplnosti informací a znamená, že údaje nemohou být měněny neoprávněnými uživateli (někdy se integrita nadřazuje důvěrnosti – např. zjištění bankovního účtu osoby není tak škodlivé jako manipulace s tímto účtem).

Dostupnost (Availability) znamená, že údaje i informace jsou oprávněným uživatelům k dispozici jen tehdy, když jsou potřeba. Zabezpečená kvalitní informace je zbytečná, když se k ní nedostaneme v případě potřeby (obecně platí, že pro řízení je třeba dostat správným lidem správné údaje ve správný čas).

Norma ISO/IEC 27001 popisuje systém řízení zabezpečení informací (Information Security Management System — ISMS). Tento systém je založen na obdobných principech jako systémy QMS (Quality management System) podle normy ISO 9001 nebo EMS (Environment Management System) podle normy ISO 14001, přičemž řada prvků je společná.

Cílem systému ISMS je nastavení řízení procesů spojených se zachováním dostupnosti, integrity a důvěrnosti informací důležitých pro podnik. Často je tento systém chápán jako systém zabývající se pouze bezpečností informačního systému či technologií, ovšem takové chápání je mylné. Systém se zabývá informacemi jako takovými, bez

ohledu na to, jakou mají formu (datovou, papírovou nebo například i formu informací — know–how — uložených v hlavách pracovníku).

Zavádění systému řízení informační bezpečnosti probíhá v etapách:

1. Stanovení rozsahu, strategie a cílů ISMS.
2. Zpracování analýzy rizik.
3. Zpracování bezpečnostních standardů.
4. Implementace bezpečnostních opatření.
5. Monitorování systému.
6. Případná certifikace systému.

Aplikací popsaných kroku lze splnit požadavky na bezpečnost informací komplexně a s jistotou, že nebude opomenuta žádná oblast, ze které může informacím hrozit nebezpečí. Systematicky provedená opatření pak dodávají realizovanému systému důvěryhodnost, kterou mohou oprávněně požadovat poskytovatelé vstupních dat.

Při přenosu údajů platí, že existuje několik oprávněných uživatelů (minimálně dva) kteří používají určitý kanál, a útočník, který má, anebo se snaží vytvořit přístup k tomuto komunikačnímu kanálu a cíleně se snaží získat údaje, resp. je změnit podle svého a oklamat oprávněné uživatele.

Propojování informačních systémů způsobem „ad–hoc“, což je v současné době velmi častý případ, nepatří sice mezi nejlepší způsoby, ale vzhledem k jeho četnosti je vhodné se o něm zmínit. Jeho podstata spočívá v tom, že jsou dvě nebo více aplikací mezi sebou propojeny pomocí speciálně vyvinutých rozhraní, která zajišťují vzájemnou aktualizaci databází informačních systémů přes účelově definované datové struktury pro výměnu požadovaných dat. Pro fyzický přenos jsou většinou využity standardní komunikační služby (internet, e-mail).

Způsob propojení informačních systému metodou „ad–hoc“ nelze využít pro vytváření universálního interoperabilního prostředí v širším měřítku s perspektivou jeho dalšího rozvoje a stálého bezpečí, ale pouze jako určité proprietární řešení relativně uzavřených informačních systémů. To znamená, že nejsou použitelné ani tam, kde jde o komerční bezpečnost a ani pro bezpečnostní činnosti realizované bezpečnostními subjekty popsanými ve speciálních zákonech o Armádě ČR, o Policii ČR, Městské a obecní policii, o vězeňské službě či celní správě. Obsahy těchto zákonů jasně vymezují, co je svěřeno a za jakých okolností výhradně těmto subjektům a nelze proto jejich činnost měnit či nahrazovat jinou bezpečnostní formou.

Pozitivní vymezení se naopak opírá o existenci takových bezpečnostních činností, které de facto existují nezávisle na těchto subjektech a dokonce se dále spontánně vyvíjejí dle potřeb obyvatelstva, trhu nebo logicky plynou z právní úpravy společenských vztahů. Do pozitivního vymezení patří ochrana majetku jedince, převoz peněz a cenností fyzickým a právnických osobám, detektivní služby, které plní přímo dikci občanského soudního řádu §120, kde je dána povinnost účastníků řízení označit důkazy, sloužící k prokázání svých tvrzení. Je tedy logické, že potřeba evokuje soukromě bezpečnostní činnosti těch jedinců, u kterých taková potřeba vzniká. Nesmíme však zaměňovat termín soukromá bezpečnostní činnost a komerční bezpečnostní činnost v libovolném sledu. Soukromou bezpečností činnost je jakákoliv soukromá bezpečnostní aktivita, kterou realizuje fyzická či právnická osoba ve svůj prospěch nebo ve prospěch

jiného subjektu, který ji svou bezpečnostní problematiku svěřil. Příkladem jsou vlastní firemní ochranky, vlastní firemní vyšetřovací, detektivní týmy. Obsahem takové bezpečnostní služby jsou bezpečnostní metody, technologie a prostředky, které nejsou výhradně zákonem určeny k výkonu státních složek. U prostředků tzv. povolených je dokonce možné, že soukromá ochranka bude disponovat bezpečnostními prostředky či technologiemi zdatnějšími než se kterými disponuje armáda či policie.

Samostatný problém tvoří kybernetický prostor a kybernetická bezpečnost, o kterých se zmíníme jen z důvodu úplnosti. Podrobné informace lze získat např. v práci [66]. Dle ní kybernetický prostor je uměle vytvořen na základě komunikace jedinců a komunit a je dnes neoddělitelnou součástí života společnosti. Hlavní problémy spojené s kyberprostorem jsou:
- množství rozmanitých zákonitostí, které jsou spletité a nejsou známé,
- kybernetická kriminalita a její posuzování v současném právním systému,
- používání a zneužití informací (např. sociální sítě),
- kybernetický terorismus
- a kybernetické války.

Protože na internet a další kybernetické sítě jsou napojené řídicí systémy kritické infrastruktury, která je důležitá pro ochranu osob a majetku, 4 tak problém kybernetické bezpečnosti se dotýká každého člověka i každé instituce.

Koncept kybernetické bezpečnosti, který zajišťuje ochranu dat, informací i znalostí pokrývá velmi širokou oblast. Konkrétní forma ochrany je závislá na kontextu dat. Je rozdíl mezi údaji na papíru a mezi datovým souborem v počítači. Proto je nejprve nutné identifikovat možná rizika. K tomu je třeba v konkrétních podmínkách [2]:
- identifikovat chráněné zájmy (aktiva) důležité pro kybernetickou bezpečnost,
- identifikovat škodlivé jevy (pohromy), které mohou poškodit stanovená aktiva,
- identifikovat zranitelnosti kybernetického prostředí, které zesílí působení pohrom a zvýší riziko,
- identifikovat dopady pohrom na aktiva a z nich plynoucí ztráty, škody a újmy, a to i v oblasti důvěrnosti, integrity a dostupnosti dat, informací a znalostí.

Poté je třeba identifikovaná rizika analyzovat a vyhodnotit, tj. určit velikost ztrát, škod a újmy na aktiva, pravděpodobnost jejich výskytu (tj. pravděpodobnost výskytu selhání kybernetické bezpečnosti), navrhnout a implementovat účinná a realistická opatření k řízení rizik kyberprostoru.

Je proto důležité, aby systém řízení bezpečnosti (SMS) každé organizace i každého technického díla pamatoval také na kybernetickou bezpečnost. Nutnost zabývat se touto problematikou vyplynula z častého napadání počítačových systémů hackery, kteří ohrožovali mimo vlastní počítačový systém (řídicí systém) a přes něho další systémy (řízené systémy).

Současně není možné přehlížet novodobé bezpečnostní hrozby, jako jsou kybernetický terorismus a informační válka. Praxe ukázala, že slabým místem vyspělých států světa mohou být počítačové řídící, komunikační a informační systémy. Kybernetický útok proti těmto systémům samostatný nebo kombinovaný s konvenčním úderem by přinesl maximální ztráty na lidských životech a závratné ekonomické a materiální škody. Cílem teroristických útoků se nejspíše stane narušení důležitých počítačových sítí řídících center armády, policie, záchranných služeb, pohotovostních služeb, ropovodů, elektráren, vodáren, přehrad apod. Zničení těla hráze přehrady vyžaduje výbuš-

niny o mohutnosti účinku několik tun nebo kilotun trinitrotoluenu, nebo maximální otevření všech výpustních otvorů pomocí počítače. Výsledek působení milionů kubíků vody v obou případech bude velmi podobný.

Moderní informační a komunikační technologie, zejména internet, byly experty EU vyhodnoceny, jako veliká podpora terorismu. EU se zavázala bojovat s terorismem a přijala návrh rámcového rozhodnutí Rady „Council Framework Decision on Combating Terrorism“, kterým chce Evropská Komise docílit snížení akceschopnosti teroristických aktivistů a podporovatelů terorismu. Jsou uvedeny důvody:

- internet se používá k inspiraci a mobilizaci místních teroristických sítí a jednotlivců v Evropě i v celém světě a rovněž slouží jako zdroj informací o teroristických prostředcích a metodách,
- aktivity v podobě podněcování ke spáchání teroristického trestného činu, náboru pro terorismus a výcviku k terorismu jsou mnohem častější, přičemž náklady na ně i rizika s nimi spojená jsou velmi nízké,
- v posledních letech se teroristická hrozba zvýšila a rychle rozrostla v důsledku změn ve způsobu činnosti aktivistů a podporovatelů terorismu, včetně náhrady strukturovaných a hierarchických skupin poloautonomními buňkami, které jsou navzájem volně propojeny. Takové buňky se propojují do mezinárodních sítí a stále více používají nové technologie, zejména internet,
- podněcování ke spáchání teroristických trestných činů, nábor pro terorismus a výcvik k terorismu jsou úmyslnými trestnými činy.

Rozhodnutí Rady EU obsahuje následující ustanovení:

1. Každý členský stát Evropské unie musí přijmout nezbytná opatření, aby zajistil, že trestné činy spojené s terorismem zahrnují následující úmyslné činy:
   - podněcování ke spáchání teroristického trestného činu,
   - nábor pro terorismus,
   - výcvik k terorismu,
   - krádež za přitěžujících okolností s cílem spáchat teroristický trestný čin,
   - vydírání s cílem spáchat teroristický trestný čin,
   - vyhotovení nepravých správních dokumentů s cílem spáchat teroristický trestný čin.
2. U činu, který má být trestný, jak je stanoveno výše v odstavci 1, není nezbytné, aby byl teroristický trestný čin skutečně spáchán.
3. Každý členský stát musí přijmout nezbytná opatření, aby zajistil trestnost pokusu o spáchání teroristického trestného činu. Členské státy EU měly přijmout nezbytná opatření pro zajištění souladu s tímto návrhem rámcového rozhodnutí do 31. prosince 2008.

Pro účely tohoto rámcového rozhodnutí se rozumí:

- *„podněcováním ke spáchání teroristického trestného činu*“ šíření nebo jiné zpřístupnění zprávy veřejnosti s úmyslem podnítit spáchání terorísticky trestného činu, kdy takové jednání, ať již přímo či nepřímo obhajuje teroristické trestné činy, způsobí nebezpečí spáchání jednoho či více takových trestných činů,
- „*náborem pro terorismus*“ získání jiné osoby ke spáchání terorísticky trestného činu,

- „*výcvikem k terorismu*“ poskytování pokynů k výrobě či používání výbušnin, střelných či jiných zbraní nebo škodlivých či nebezpečných látek, případně jiných specifických metod či postupů za účelem spáchání teroristicky trestného činu s vědomím, že poskytované dovednosti jsou určeny k použití za tímto účelem.

EU chce docílit znepřístupnění informací týkající se terorismu i tím, že vydává zákaz pro poskytovatele internetových služeb zpřístupnit jakýkoliv materiál týkající se podněcování ke spáchání teroristicky trestných činů, nábor nebo výcvik pro terorismus.

Srovnáním s listinami základních práv a svobod občanů EU i ČR jsou dle práce [67] veškeré navrhované změny jsou v mezích zákonů a jiných právních předpisů vztahujících se k tomuto problému.

6.9. Specifické postupy pro řízení a vypořádání rizik technického díla ve prospěch bezpečnosti

V současné době jsou v praxi prosazovány modelové postupy: risk-based design; risk-based operation; risk-based inspections; a risk-based maintenance [2,7,12,26,68-74]. Dále se zmíníme o prvních dvou, protože risk-based maintenance je popsána výše v odstavci 6.5.

6.9.1. Risk-based design technického díla

Na základě výše uvedených znalostí a zkušeností z praxe, shrnutých v pracích [1,12,19,68-74] práce [75] uvádí techniku sestavování návrhu technického díla či zařízení založeného na řízení rizik takto:

1. Vytvořit seznam součástí (prvky, komponenty) a systémů, které splňují normy a budou spojovány do dílčích celků.
2. Pro všechny položky v seznamu součástí a systémů (bod 1), které splňují stanovené normy a standardy určit limity a podmínky z hlediska jejich provozu na určitém místě, pokud jde o:
   - materiál, ze kterého mají být vyrobeny,
   - požadavky na provozuschopnost,
   - požadavky na pracovní režim, ve kterém budou pracovat,
   - požadavky na obsluhu
   - a možná další rizika (vnitřní požár nebo výbuch a důležitá vnější rizika).
3. Pro všechny položky v seznamu součástí a systémů (bod 1) určit pro zdroje rizik specifické pro lokalitu či místo, ve kterém technické dílo či zařízení bude umístěno se zvážením přístupu All-Hazard-Approach [13,14], velikosti a charakteristiky dílčích rizik.
4. Pro všechny zdroje rizika (bod 3) stanovit scénáře dopadů pro nejméně příznivé podmínky; a pokud některé dopady rizik nejsou přijatelné, je nutné zvýšit požadavky na materiál, ze kterého jsou zhotoveny komponenty či systémy tak, aby tato rizika byla přijatelná. Není-li to možné, je třeba vložit do projektu technického díla

či zařízení opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní kvalitní odezvu na realizaci příslušného rizika při provozu.

5. Vytvořit propojení komponent a model jejich propojení, který splňuje normy a požadavky na inherentní bezpečnost.
6. Pro všechna propojení (bod 5) určit limity a podmínky z hlediska jejich:
   - materiálového složení,
   - způsobu provedení (volné, těsné nebo složité),
   - metody propojení (svary, šrouby, nýty, lepení atd.)
   - a realizace možných dalších rizik (vnitřní požár nebo výbuch, lidský faktor a vnější rizika).
7. Pro zdroje rizik (bod 3) stanovit scénáře dopadů dílčích rizik pro všechna propojení (bod 5) a integrované riziko pro celek, který je vytvořen propojením komponent či systémů; nejsou-li dílčí rizika a integrované riziko přijatelné, je nezbytné zvýšit požadavky na materiál či způsob provedení propojení komponent či systémů tak, aby tato rizika byla přijatelná. Není-li to možné, je třeba vložit do projektu technického díla či zařízení opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní kvalitní odezvu na realizaci příslušného rizika při provozu.
8. Pro zdroje rizik (bod 3) určit pro každý výrobní proces scénáře dopadů procesu pro nejméně příznivé podmínky, které ukazují dopady integrálního rizika (tj. rizika procesu). V případě, že integrované riziko není přijatelné, zvýšit nároky na projekt u:
   - komponent výrobního procesu,
   - pracovního režimu
   - a obsluhy, aby rizika mohla být přijatelná.

   Není-li to možné, je třeba vložit do projektu technického díla či zařízení opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní kvalitní odezvu na realizaci příslušného rizika při provozu.
9. Pro zdroje rizik (bod 3) určit integrální riziko, tj. celkové riziko technického díla či zařízení. Pokud je riziko přijatelné pouze podmíněně (ALARP), provádět změny technologie, které umožní okamžitou reakci s cílem navrátit se do normálního stavu. V případě nepřijatelného rizika je nutné se vrátit k úpravě rizik procesů, dílčích rizik komponentů, systémů a jejich propojení a zavést do projektu technického díla či zařízení opatření (opatrně, aby se nevytvořil zdroj dalších rizik), která umožní realizaci principů jako je “selži bezpečně”, tj. neprováděj nebezpečný úkon, informuj obsluhu a popř. začni provádět stanovené úkony odezvy.
10. S ohledem na zdroje rizika (bod 3) určit požadavky na systém řízení, tj. pro I&C i obsluhu za běžných, abnormálních a kritických podmínek. Zde je nutné, aby v každém okamžiku byly pro řízení k dispozici správné informace o stavu zařízení a okamžitých provozních podmínkách hlavně kritických zařízení a kritických procesů.

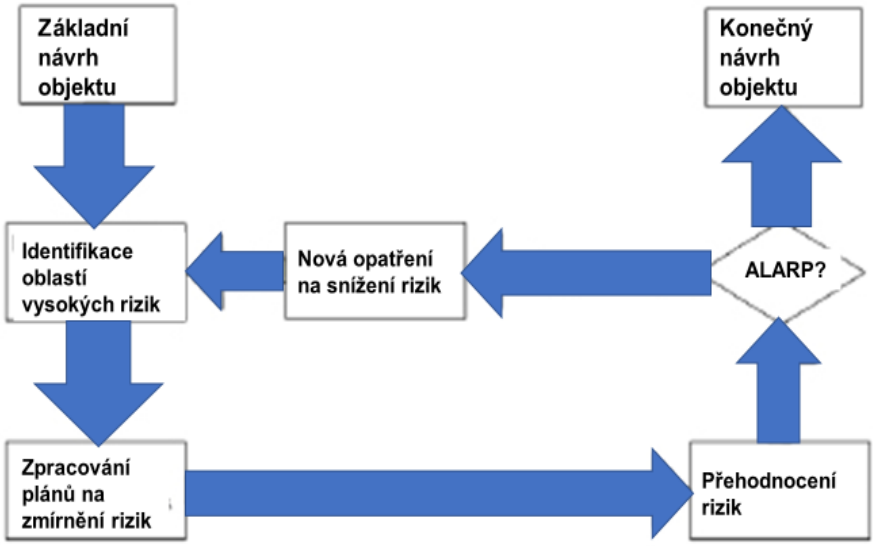
Uvedený postup generace projektu technického díla či zařízení je zobrazen na obrázku 26. Návrh založený na riziku dle [70] využívá sedm principů odolnosti:

- zálohování,
- vložení schopnosti elegantní a řízené degradace,
- vložení schopnosti návratu ze zhoršeného stavu,
- flexibilitu systému i organizace,
- vložení schopnosti řídit mezní podmínky v blízkosti rozhraní výkonu a bezpečnosti,

- vložení optimálních modelů řízení, snížení složitosti a omezení možných nežádoucích vazeb.

Do návrhu je nutné zahrnout program pro zvyšování bezpečnosti, který zajistí:

- bezpečnost a funkčnost všech zařízení tak, aby odpovídaly svému poslání,
- identifikaci, vyhodnocení, eliminaci nebo regulaci potenciálních rizik na přijatelné úrovni pro důležitá zařízení, systémy a jejich různé části,
- řízení rizik, které zahrnuje všechny možné pohromy se zdroji uvnitř i vně složitých systémů, které nelze eliminovat,
- ochranu personálu, osob v okolí, zařízení a majetku,
- použití nových materiálů nebo výrobků a zkušebních technik pouze způsobem, který je spojen pouze s minimálním rizikem,
- vložení bezpečnostních faktorů, které zajišťují nápravná opatření vedoucí ke zlepšení
- a zohlednění všech vhodných historických údajů o zajištění bezpečnosti, které byly vytvořeny podobnými programy zvyšujícími bezpečnost.



Obr. 26. Vývojový diagram projektování založeného na riziku.

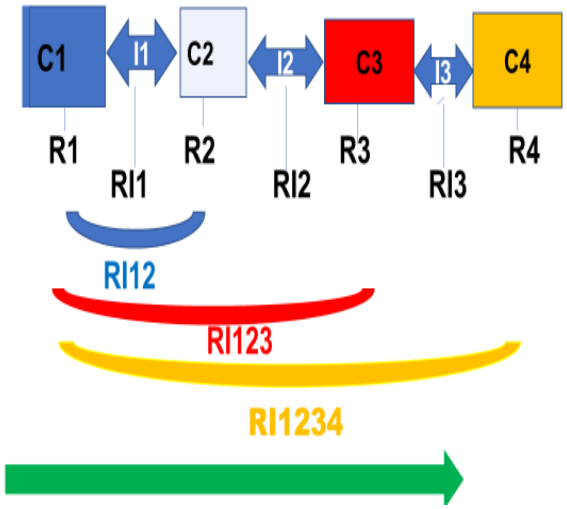
Z technického hlediska se stanoví podmínky a limity provozu, instalují se bezpečnostní systémy (aktivní, pasivní a hybridní) a zajistí se vhodné zálohy; dle [70,76] se řeší:

- jaké bezpečnostní systémy jsou vhodné a jaká musí být jejich záloha,
- kde / na kterých místech fungují bezpečnostní systémy nejefektivněji,
- proč je používat právě tam a ne jinde, v jakých mezích spolehlivě fungují.

Příklad procesu projektování je zobrazen na jednoduchém obrázku 27. Nejprve se sestaví pro dané technické zařízení systém pro podporu rozhodování o rizicích jednotlivých komponent a jejich propojení, pak se určí kritéria pro stupnici pro hodnocení míry rizika – tabulka 6; a následně se postupně vytváří projekt. Proces sestavování projektu je následující:

- navrhnou se komponenty: C1, C2, C3, C4 a jejich propojení podle norem,
- podle scénářů pohrom (vnějších i vnitřních škodlivých jevů včetně lidského faktoru) se stanoví rizika komponent: R1, R2, R3, R4 a jejich propojení: RI1, RI2, RI3 a posoudí se dle tabulky 6. V případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení,

- podle DSS se určí riziko souboru propojení RI12 a posoudí se dle tabulky 6. V případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení,
- podle DSS se určí riziko souboru propojení RI123 a posoudí se dle tabulky 6. V případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení,
- podle DSS se určí riziko souboru propojení RI1234 a posoudí se dle tabulky 6. V případě, že rizika nejsou přijatelná, tak se provedou korekce, např. v materiálu či způsobu propojení.



Obr. 27. Schéma procesu projektování založeného na řízení rizik. Zelená šipka zobrazuje postup vytváření projektu.

Tabulka 6. Hodnotová stupnice pro stanovení míry rizika.

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

Podle zjištěných hodnot rizika se výsledky posouzení rizika řadí do tří skupin:
- riziko přijatelné – kategorie 0 a 1,
- riziko ALARA, tj. podmíněně přijatelné – kategorie 2 a 3
- a riziko nepřijatelné – kategorie 4 a 5.

Jeli riziko přijatelné, tak není třeba dělat žádná další opatření na zmírnění rizika. Pro provoz je třeba udělat doporučení, že předmětné riziko je třeba pravidelně sledovat, protože dynamické změny a opotřebení při provozu mohou zvýšit riziko. Je-li riziko

ALARA, tak je třeba v projektu zabudovat technické prvky, které umožní odezvu v případě realizace rizika. V případě nepřijatelného rizika, je nutné provést korekce, např. v materiálu, konstrukci či způsobu propojení a znovu riziko posoudit.

Podle poznatků a zkušeností shromážděných v pracích [19,68-76] při daném typu projektování, projektant musí mít kompetence pro:
- uplatňování výsledků metod analýzy a hodnocení rizik,
- provádění metodiky analýzy a hodnocení rizik přizpůsobených problému,
- řešení mimořádných situací a krizí,
- analýzu situací / činností / nehod,
- přeměnu politiky na skutečnou akci,
- přeměnu statistik nehod na akční plány,
- strategické plánování,
- stanovení hierarchie problémů,
- nalezení správných informací a poznatků,
- provádění kritických analýz,
- navrhování správných řešení,
- komunikaci,
- provádění syntézy a přizpůsobování znění určeného veřejnosti,
- dodržování etiky.

Podle stejných zdrojů projektant při každém rozhodování o riziku ve prospěch bezpečnosti musí zvažovat:
- všechny faktory a procesy, které mohou být nebezpečné a jak často se mohou vyskytnout,
- jak velké mohou být jejich dopady,
- jak lze snížit velikost dopadů nebo četnost výskytu,
- zda navrhovaná opatření nemohou být zdrojem nových nebezpečí,
- kterými technickými a řídicími systémy lze ovládat ohrožení, kterým nelze zabránit.

6.9.2. Risk-based operation technického díla

Na základě prací [1,12,68-74,76] provoz založený na řízení rizik se opírá integrované řízení procesů – obrázek 12 a o plán řízení rizik sestavený podle ISO 31000. Při sestavování konceptu provozu založeného na permanentním řízení rizik je třeba propojit normy a výsledky řízení rizik ve prospěch bezpečnosti.

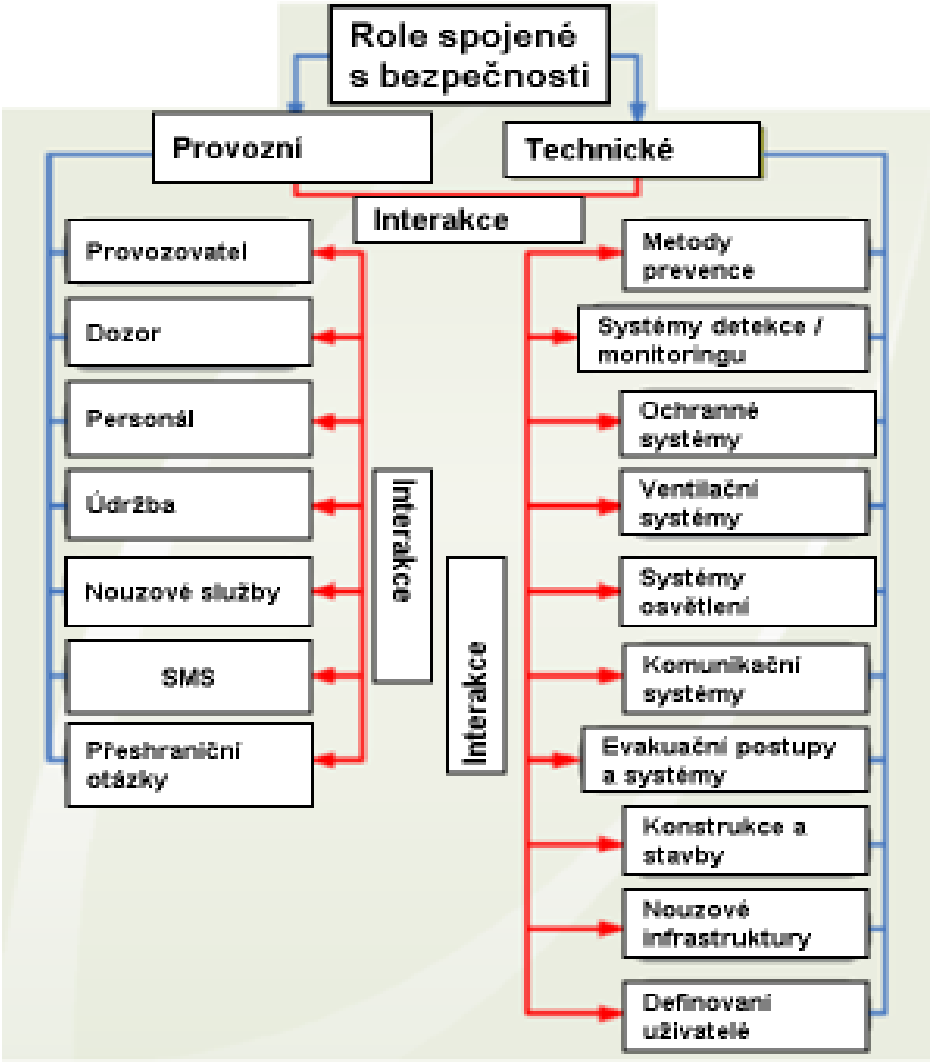
Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika. Systém řízení bezpečnosti SMS kritického prvku musí obsahovat úkoly uvedené na obrázku 20 a proces řízení rizik na obrázku 21. Příklady plánu řízení rizik jsou v příloze 2.

Podle pravidel správného řízení shrnutých v práci [77], které je prosazované v Evropské unii:
- za zvládání rizik odpovídají všichni zúčastnění (od politiků přes pracovníky správy, vedení technických děl až po techniky a občany)
- a zvládání konkrétního rizika se přiděluje tomu subjektu, který je na to nejlépe připraven.

Proto je velmi důležité rozdělení rolí a odpovědností souvisejících s bezpečností. Obrázek 28, zpracovaný podle zásad uvedených v práci [78] ukazuje rozdělení rolí spojených s bezpečností v technickém díle při provozu.

6.10. Způsob provádění opatření pro řízení a vypořádání rizik technického díla ve prospěch bezpečnosti

Řízení bezpečnosti je proaktivní strategický nástroj sloužící k zajištění bezpečnosti a udržitelného rozvoje lidské společnosti i technických děl. Opírá se o řízení a vypořádání rizik. S ohledem na omezené zdroje společnosti i provozovatelů technických děl prosazuje preventivní a zmírňující opatření přednostně proti závažným dopadům pohrom na chráněné zájmy, a to i v případě, že jsou málo pravděpodobné, tj. zahrnuje princip předběžné opatrnosti.



Obr. 28. Role zúčastněných spojené s bezpečností; SMS je systém řízení bezpečnosti celku (safety management systém).

6.10.1. Řízení projektů

Evropská unie prosazuje správné řízení věcí ve prospěch veřejného zájmu i zájmu organizace provozující technické dílo, které má na základě současného poznání formu řízení projektů (projektového řízení) a řízení procesů (procesního řízení) organizace,

která provozuje technické dílo. Řízení projektů i řízení procesů je realizované provázaným souborem opatření a činností, ve kterém hlavní roli hraje vyjednávání s riziky [79,80].

K dosažení žádoucího cíle, tj. bezpečné organizace, která má potenciál udržitelně se dále rozvíjet, je nutné:
- znát a při řízení organizace provozující technické dílo zvažovat všechna možná vnitřní i vnější rizika pro předmětnou organizaci, lidský faktor, a to v jednotlivostech i v souvislostech,
- správně se všemi riziky vyjednávat,
- mít správně nastavené řízení a vypořádání rizik.

Koncept komplexního řízení technických děl, který je založen na principech správného řízení, formulovalo OECD v roku 2002 [24]. V tomto systému řízení bezpečnosti technického díla platí premisy:
- technické dílo i technické zařízení je otevřený systém systémů,
- chráněné zájmy technického díla (aktiva) jsou všechny základní veřejné zájmy a v případě entity zřízené státem k určitému úkolu další zájmy,
- bezpečné technické dílo má všechny chráněné zájmy, o které musí pečovat, v bezpečí a s potenciálem udržitelného rozvoje.

Pozdější práce, např. [26] k procesům stanoveným OECD přidaly proces fyzického a kybernetického zabezpečení technického díla či technického zařízení.

Komplexní systém řízení bezpečnosti navíc respektuje skutečnost, že každé technické dílo, jako část lidského systému je v dynamicky proměnném světě. To znamená, že pro řízení technického díla je třeba zvažovat:
- koncept řízení systému systémů,
- řízení technického díla chápat jako strategické řízení bezpečnosti, které se provádí integrovaným řízením zásadních procesů [20,24,26].

Řízení projektů je koncept a soubor nejlepších postupů při řízení projektů, který se vyvíjel po celou lidskou historii. V současné době je projektové řízení (řízení projektů) považováno za optimální přístup k řešení problematiky projektového charakteru [81]. Řízení projektů je složeno z řízení procesů, které lze zařadit do několika typických skupin procesů. Každý proces potřebuje nějaké vstupy, pomocí nichž a pomocí procedur nebo nástrojů, znalostí a dovedností lidí produkuje výstupy. Výstupy z procesů jsou výstupy z projektu nebo výstupy pro jiné procesy [81].

Projektové řízení je způsob řízení entity pomocí projektů. Je to vysoce účinný nástroj řízení změn, komplexní koncepce efektivního dosahování projektových cílů, která umožní manažerům dosáhnout odpovídajíc kvality výstupu s minimálními nároky na čas, finance a ostatní zdroje [82]. Zahrnuje řízení jednotlivých projektů a vytvoření organizační struktury a koordinaci projektů z hlediska termínů a disponibilních zdrojů.

Projekty se skládají z procesů, které se dělí na dvě základní skupiny, a to procesy řízení a produktově orientované procesy. Procesy řízení projektů popisují, organizují a vykonávají práci na projektu a zahrnují iniciační procesy, plánovací procesy, realizační procesy, kontrolní procesy a závěrečné procesy. Produktově orientované procesy specifikují a vytvářejí produkt procesu a jsou typicky definovány pomocí životního cyklu projektu a mění se podle oblasti aplikace.

Zásady projektového řízení jsou shrnuty do tzv. oblastí znalostí. Projektové řízení rozlišuje devět oblastí znalostí: řízení integrace; řízení rozsahu; řízení času; řízení nákladů; řízení kvality; řízení lidských zdrojů; řízení komunikace; řízení rizik; a řízení nákupu [82].

Podle současných poznatků se používá dělení: řízení rozsahu (celkový rozsah bývá dán apriori technickými, přírodními, ekonomickými nebo jinými důvody); řízení času; řízení nákladů; řízení kvality; řízení komunikace; řízení rizik; a řízení zdrojů, a to:

- časových,
- lidských,
- materiálních a
- know how.

Propojení projektového a procesního přístupu si představujeme tak, že projektové řízení je složeno z procesů, které je možno zařadit do několika typických skupin procesů. Každý proces potřebuje nějaké vstupy, pomocí nichž a pomocí procedur nebo nástrojů a znalostí a dovedností lidí produkuje výstupy. Výstupy z procesů jsou výstupy z projektu nebo vstupy pro jiné procesy. Pro podporu řízení jsou v současné době zpracovávány procesní modely [83] a projektové modely [82].

Řízení procesů je soubor činností, které definují proces (proces = koordinovaný a standardizovaný tok činností pro dosažení cílů organizace), formulují odpovědnosti, vyhodnocují výkonnost procesů a hledají příležitosti pro zlepšení procesů [83]. Je založeno na řízení znalostí.

Znalosti (vědění) jsou dnes považovány za základní zdroj bohatství. Řízení znalostí je systematický proces hledání, vybírání, organizování, analýzy a prezentování informací způsobem, který zlepšuje porozumění pracovníka specifické oblasti zájmu. Je typické nejen pro akademickou půdu a pro vědecké a výzkumné ústavy, ale i pro podniky, které se snaží o rozvoj.

Řízení znalostí (Knowledge Management) v sobě koncentruje všechny přínosy procesního řízení a snaží se rozvinout způsob jak vědomostní kapitál pojmenovat, získávat, udržovat a využívat [84,85]. Řízení založené na znalostech, se zaměřuje na všeobecné rozvíjení lidského kapitálu: připravenost pracovníka podávat požadované výkony (způsobilost, kompetence), zvyšování inteligence pracovního týmu apod. Rozhodujícími kritérii jsou zejména odpovědnost vycházející z dovedností a širokých znalostí, kvalitní plnění úkolů a ochota se trvale učit. V řízení znalostí hmotné statky nemají prvořadou úlohu. Pro řízení jsou důležitější nehmotné statky, tj. intelektuální bohatství, kterým jsou dovednosti, schopnosti, zkušenosti a znalosti. Uvedené hodnoty mají nejvýznamnější vliv na splnění nebo nesplnění úkolů a dosažení cíle za předpokladu, že je vše technikou a materiálem zabezpečeno.

Proto se procesní přístup založený na řízení znalostí nezaměřuje na výsledky, ale na příčiny. Řízení procesů je založené na rozpracování koncepce a metodologie. Uplatnění prvků řízení znalostí v rozhodovacím procesu řídícího pracovníka vede k přechodu od individuálního rozhodování ke skupinovému přístupu. Důležitá je role řídícího pracovníka, který takový proces musí usměrňovat k přijetí kvalitního rozhodnutí. Je však třeba vzít v úvahu, že takový postup je nejenom časově náročnější, ale je také náročnější na přípravu jednotlivých členů procesního týmu včetně řídícího pracovníka.

Ze zkušeností při uplatňování prvků procesního řízení v podnikové sféře vyplynulo, že při rozhodování rutinním je individuální rozhodnutí výhodnější, pro přípravu rozhodnutí neprogramového (tj. složitého a nestandardního) je žádoucí volit metodu skupinového rozhodování (vytvoření procesního týmu). V obou případech však je řídící pracovník vždy za rozhodnutí odpovědný. Při skupinovém rozhodování musí být také vytvořeno vhodné prostředí, které bude podporovat tvůrčí schopnosti skupiny. Je důležité, aby řídící pracovník uměl potlačit vliv neschopných, neznalých a líných, ale ambiciózních jedinců, kteří pro prosazení svých ambicí útočí na znalé a pracovité. Řídící pracovník musí při týmovém rozhodování dbát na:

- podporování původnosti a neobvyklosti řešení,
- řízení skupiny tak, aby byly odděleny zdroje od obsahu informací,
- zabezpečení uplatnění nezávislého osobního úsudku a zkušeností,
- udržování otevřené komunikace, posilování sebedůvěry, zabránění zesměšňování,
- nepovolit rychlá řešení a krátkodobé výsledky,
- dosažení konsenzu. Pokud to není možné, přijmout a implementovat rozhodnutí po důsledném vyhodnocení všech okolností, které mohou mít vliv na dosažení cíle.

Rozlišujeme tři základní úrovně řízení, které je nutné sladit, a to úroveň strategická, která určuje základní směry vývoje, ze kterých vyplývá, které procesy je nezbytné upravit nebo vytvořit, jaké organizační změny bude nezbytné provést, kde získat know-how, finanční zdroje atd. Řízení procesů pomáhá utřídit činnosti nutné pro realizaci dlouhodobých záměrů. Hledají se odpovědi na otázky jak procesy nastavit, v jakém stavu je udržovat a jak musejí tyto procesy navzájem spolupracovat. Operativní řízení rozhoduje o konkrétním rozmístění zdrojů v procesu (lidských, technologických, finančních) a také o výkonu jednotlivých činností v rámci nastavených procesů (jak provést konkrétní operaci). Snahou je zajistit transfer znalostí a dovedností mezi pracovníky. Významného efektu a ***konkurenční výhody organizace dosáhne teprve sladěním všech tří úrovní řízení.*** Jde o to dosáhnout stavu, kdy procesy budou definovány a řízeny na základě strategie a operativní řízení nebude jen hašením mimořádných událostí. Procesy pak budou zdokonalovány na základě poznatků přenášených z operativy. Nové poznatky pramenící z řízení procesů se pak rychle promítnou zpět do strategie a vyvolají další zásadní změnu ve vývoji podniku.

Řízení procesů je založeno na principu integrace činností do ucelených procesů. Tedy i dílčí operace je třeba takto sjednotit. Procesy jsou ovládané procesními týmy. Každý procesní tým řídí procesy na svém stupni a podřízeným skupinám dává úkoly, které vedou k naplnění cíle. Přitom všechny procesní týmy musí být motivovány k dosažení optimálních výsledků a všechny stupně musí při dosahování dílčích výsledků sledovat splnění konečného cíle. V procesním řízení existují vedle sebe dva systémy řízení, a to funkční a procesní, což činí řízení složitějším.

Projekt je časově, nákladově a zdrojově omezený soubor procesů realizovaný za účelem vytvoření definovaných výstupů (rámec naplnění projektových cílů) co do kvality, standardů a požadavků. Cíle projektu jsou základními parametry projektu. Je proto velmi nutné na ně klást odpovídající důraz. Cíle by měly být SMART: Specific – specifikované; Measurable – měřitelné; Aligned – akceptovatelné; Realistic – realizovatelné; a Timed – termínované, tzn. časově vymezené [86].

Řízení projektu je formální proces identifikace, koordinace a průběžného nasazení lidských a jiných zdrojů s cílem dosažení projektových cílů podle časového rozvrhu, při dodržení stanovených nákladů a kvalitativních požadavků. Řízení projektu podle [87]

vyžaduje pět odlišných manažerských činností: definování projektových cílů; tvorba časového plánu projektu a finančního rozpočtu; vedení – řízení lidských zdrojů; sledování (monitorování) – kontrola stavu a postupu projektových prací, aby byly včas zjištěny odchylky od plánu a mohlo se včas přistoupit k jejich korekci; ukončení – ověření, že hotový úkol odpovídá aktuální definici toho, co se mělo udělat a uzavření všech nedokončených prací.

Moderní řízení věcí veřejných opírající se projektové a procesní řízení používá obecný proces (Problem Solving Process) [88], který je součástí best-practice (dobré praxe, tj. nejlepších zkušeností) a je celosvětově široce užíván. Jedná se o proces, který svou obecností přesahuje problematiku projektů a projektového řízení a sestává z dále uvedených bodů: identifikace a definice problému; sběr a analýza dat; analýza příčin problému; definice cílového stavu řešení problému; návrhy řešení problému a výběr řešení; popis řešení; a možnosti pro ověření správnosti řešení.

6.10.2. Obsah výzkumné zprávy k projektu

Obsah výzkumné zprávy k projektu z inženýrské oblasti, zpracovaný dle analýz prací [78-88], je stručně uveden v tabulce 7.

Tabulka 7. Obsah výzkumné zprávy k projektu z technické oblasti.

Název projektu	
Název kapitoly	**Obsah kapitoly**
1.Úvod	Popsat: jaký problém projekt řeší?; proč je třeba problém řešit?; a co je cílem řešení?
2. Zhodnocení dosavadních poznatků	Uvést: rešerši; a teorii, které se týkají řešeného problému a způsobů jeho řešení.
3. Cíle řešení a výstupy	Problém je třeba řešit na současné úrovní poznání, tj. jde o aplikaci risk management a risk engineering (stručně popsat, o co jde). Na základě technické pomůcky SMART [89], cíle řešení projektu by měly být: S – specific (konkrétní a jasně definované); M – measurable (měřitelné, aby bylo možno zjistit, zda cílů bylo dosaženo); A- achievable (dosažitelné – dostatek zaměstnanců, finančních prostředků a dalších potřebných věcí); R – realistic (realistické); a T- time specific (časově ukotvené, sledovatelné – harmonogram) Charakterizovat stručně obory řešení problému: technické; organizační; metodické; personální; vzdělávací; řízení (včetně automatizace); ekonomické; právní; a popř. další.
4. Data	Stručně popsat: - objekt řešení; zdroje dat; a uvést situační schéma objektu, - data: technická (objekty, zdroje rizik); organizační (předpisy, zdroje rizik); metodické (zdroje rizik); personální (zaměstnanci, další zaměstnané osoby, jiní); vzdělávací (zdroje rizik); řízení (zdroje rizik – nezapomenout na automatizaci a komunikaci); ekonomická (zdroje rizik; z čeho se bude platit); právní (zdroje rizik); a popř. další.

5. Použité metody ke zpracování dat a k řešení problému	Stručně popsat metody pro řešení v oblasti: technické (pracovní postupy, harmonogram prací, metody testování); organizační (metoda koordinace, pracovní předpisy pro jednotlivé procesy, metody komunikace); metodické (situační schéma, kontrolní seznamy, What If, scénáře, DSS); personální (kritické osoby, podpůrný personál, náhradníci); vzdělávací (školení, praktický výcvik); řízení (integrované řízení procesů v čase včetně ovládání automatizace); ekonomické (zaměstnanci, materiál, režie, údržba, služby, vzdělání, provozní náklady); právní (návrh legislativy, jestliže nelze dle současné); a popř. další.
6. Výsledky	Přehledně uvést výsledky: - z oblastí: technické (postupy prací – projekt a jeho procesy včetně procesu komunikace); organizační (postupy, předpisy, plán řízení rizik, plán komunikace); personální (počet zaměstnanců a nároky na jejich znalosti a dovednosti, počet dalších osob a nároky na jejich znalosti a dovednosti, jiní a nároky na jejich znalosti a dovednosti); vzdělávací (seznam vzdělávaných, program vzdělávání, plán vzdělávání, způsob testování znalostí a dovedností); řízení (kontrolní seznamy pro řízení jednotlivých procesů, DSS pro rozhodování o rizicích celého projektu, včetně automatizace a komunikace); ekonomické (hrubý odhad na základě dosavadních zkušeností z ekonomické praxe); právní; a popř. další, - a jejich propojení.
7. Závěr	Uvést: - co vyžaduje realizace projektu – investice, materiální zajištění, lidské zdroje, údržbu, náklady na akci, - podle čeho bude řešení projektu probíhat, - kdo za řešení projektu odpovídá - a jaké jsou přínosy pro technické dílo, region a stát (dlouhodobé).
Literatura	

7. ZÁVĚR

Těžiště práce je kapitola 6, která shrnuje technická i netechnická opatření a činnosti pro řízení a vypořádání rizik technických děl ve prospěch bezpečnosti pomocí metodik inženýrství založeném na práci s riziky. Ukazuje také, že opatření a činnosti je vhodné provádět postupy založenými na projektovém a procesním řízení.

Při práci s riziky si je třeba uvědomit, že úkolem řízení a vypořádání rizik je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Podle Mezinárodní organizace pro standardizaci (ISO) kvalifikované řízení rizik technického díla musí: být součástí systému řízení sledovaného technického díla; být součástí každého procesu rozhodování sledovaného technického díla; explicitně zvažovat nejistoty a neurčitosti v procesech a podmínkách sledovaného technického díla a jeho okolí; být systematické a strukturované; vycházet z nejlepších dostupných informací; být dynamické a vhodně reagovat na různé změny; být uzpůsobeno místním podmínkám a legislativním požadavkům; respektovat vliv člověka (lidský faktor) na technické dílo; a mít schopnost neustálého zlepšování.

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.

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, plány kontinuity a plány odezvy na nadprojektové havárie) [12,19]. Pro důležité technické objekty se používá koncept bezpečnosti kritických objektů založený na komplexním přístupu, zvaném obrana do hloubky [19].

Ačkoliv koncept integrální bezpečnosti se rozšiřuje v praxi pomalu z důvodů uvedených v práci [12], je třeba ho prosazovat, protože do pojetí integrální bezpečnosti patří i život podporující funkce, jejichž rizika s ohledem na zdraví člověka, ekosystémy a bezpečnost systému se minimalizují. Popsaný model pro řízení bezpečnosti objektů (a to hlavně kritických) ukazuje způsob řízení rizik, aby se předešlo, anebo alespoň zmírnilo možným nežádoucím a nepřijatelným dopadům. Jeho respektování zajišťuje, že všichni zúčastnění chápou řízení rizik ve prospěch bezpečnosti stejně. Jednotné chápání rizik, způsobů a cílů jejich řízení dovoluje odstranit příčiny havárií, které vznikly různým chápáním rizik specialisty různých oborů. Proto jeho respektováním lze zajistit zvládnutí (odstranění, zmírnění či připravenost na včasnou odezvu):

- slabin v zabezpečení vůči vnějším vlivům,
- vnitřních náhodných poruch systému
- vnitřních systémových poruch zařízení,
- poruch v procesech,
- lidských chyb,

- nedostatku zdrojů,
- konfliktů mezi požadavky na bezpečnost a zabezpečení,
- chybné nebo nedostatečné identifikace ovlivňujících činitelů,
- chybné práce s riziky (volba metody, definice stupnice, ohodnocení rizika),
- neodpovědnosti manažerů či personálu,
- nekompetence manažerů či kritického personálu,
- závislosti a nedůvěryhodnosti řešitelských subjektů.

Konkrétní technická opatření prováděná na základě řízení a vypořádání rizik ve prospěch bezpečnosti 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 a závěry z řízení rizik ve prospěch bezpečnosti. Specifickou pozornost u technických děl je třeba věnovat tlakovým nádobám, regulačním ventilům, potrubím, kontejnmentům či jiným ochranným obálkám, jejichž bezpečnost je zásadní pro ochranu lidí a životního prostředí.

Na závěr je třeba uvést, že řízení a vypořádání rizik ve prospěch bezpečnosti je třeba dále vylepšit, protože:

- poznatky a výsledky výzkumu v práci [8] ukazují, 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,
  - 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,
- mnoho příkladů v pracích [1,12,16,19] 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 (μ-σ, μ + σ) pokrývá 68.5 % případů; interval (μ-2σ, μ + 2σ) pokrývá 85.4 % případů; a interval (μ-3σ, μ + 3σ) pokrývá 99.8 % případů [20], kde μ je medián a σ standardní odchylka,
- 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 [1].

LITERATURA

[1] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 978-80-01-06182-4. Praha: ČVUT 2017, 364 p. Doi:10.14 311%2FBK.9788 001061824

[2] PROCHÁZKOVÁ D. *Analýza, řízení a vypořádání rizik spojených s technickými díly*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. Doi:10.14311%2 FBK.9788001064 801

[3] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369 p.

[4] UN. *Human Development Report*. New York: UN 1994, www.un.org.

[5] EU. Maastricht Treaty (C 191, 29.7.1992, pp.s. 1–112) ve znění pozdějších předpisů

[6] CLINTON, B. Presidential Decision Directive 63. Washington: White House 1988, 18 p.

[7] EPRI. *Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications.* Revision 1 to EPRI NP-5652 and TR-102260. Palo Alto: EPRI 2014, 378 p.

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

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

[10] HAIMES, Y. Y. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis.* 29 (2009), 12, pp. 1647–1654.

[11] FAWCETT, H. H. Hazardous and Toxic Materials. Safe Handling and Disposal. New York: Willey 1984.

[12] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁ-ZKA, Z., OU-HRABKA, L. *Řízení rizik procesů spojených s provozem technického díla během jeho životnosti.* ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p., Doi:10.143 11%2FBK.9788001066751

[13] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.

[14] EU. *FOCUS Project*. Brussels: EU 2012, http://www.focusproject.eu/documents /14976/-5d763378-1198-4dc9-86ff-c46959712f8a

[15] LACKO, B. Analýza rizik a situační povědomí. In: *Rizika podnikových procesů 2015*. ISBN: 978-80-7414-967-2. Ústí nad Labem: UJEP 2015, pp. 27-34.

[16] ČVUT. Databáze pohrom, havárií a selhání technických děl a opatření odezvy na uvedené jevy. *Archiv.* Praha: ČVUT 2024.

[17] PROCHÁZKOVÁ, D., PROCHÁZKA, J., ŘÍHA, J., BERAN, V., PROCHÁZKA, Z.: Řízení rizik procesů spojených se specifikací a umístěním technického díla do území. ISBN: 978-80-01-06467-2. Praha: ČVUT 2018, 134 p. Doi:10.14311 %2FBK.9788001064672

[18] PROCHÁZKOVÁ, D. Šetření podstaty stížností a konfliktů týkajících se technických řešení. *Kontrola MSK ČR 1992*. MSK ČR Praha, 95 p.

[19] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. In: *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. Doi:10.14311%2FBK .9788001066096

[20] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.

[21] PROCHÁZKOVÁ, D., PROCHÁZKA, J., ŘÍHA, J., BERAN, V., PROCHÁZKA, Z. *Řízení rizik spojených s ukončením provozu technického díla a s předáním území do dalšího užívání.* ISBN 978-80-01-06527-3. Praha: ČVUT 2018, 114 p. Doi: 10.14311%2FBK.9788001065273

[22] EU. *Seveso III Directive (2012/18/ EU).* Brussels: EU 2012.

[23] US DOE. *DOE -HDBK-110196. Handbook. No 20585*- Tennessee: US DOE 1996, 180 p.

[24] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Autho-rities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191 p.

[25] LACKO, B., DOLEŽAL, J., BARTOŠKA, J. Advanced prediction of project by dyprep method. *Mendel Journal series.* ISSN 1803-3814. (2015), 21, pp. 213-216.

[26] PROCHÁZKOVÁ D. Generic Model for Management of Safety of Technical Installations Powered by Small Modular Reactors. *Design, Construction, Maintenance.* ISSN 2732-9984. 3 (2023).p, pp. 7-12. Doi:10.37394/232022. 2023.3.2

[27] PROCHÁZKOVÁ D., PROCHÁZKA, J. Optimální nástroj pro řízení rizik systémů závisí na jejich složitosti. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 355-367. Doi: 10.14311/ BK.97880 01069066

[28] COASE, R. H. The Problem of Social Cost. *Journal of Law and Economics,* 3 (1960), pp. 1-44.

[29] HOLLNAGEL, E., WOODS, D.D. *Resilience Engineering*. ISBN 978-131560-5685. London: CRC Press 2017, 416 p.

[30] RASMUSSEN, J. Risk Management in a Dynamic Society. *Safety Science*, 27 (1997), 2, pp.183-213.

[31] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Dobrá praxe spojená s identifikací podezřelých a podvodných položek a ochranou před jejich umístěním do jaderných zařízení.* Zpráva pro SÚJB-02203/0002. Praha: ČVUT FS 2022, 80 p.

[32] REASON, J. Human Error. Cambridge: Cambridge University Press, 1990.

[33] PROCHÁZKOVÁ D. Propojení norem a výsledků řízení rizik ve prospěch bezpečnosti. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 7-19. http://hdl.handle.net/10467/98461. doi.org/10.14311/ BK.9788001069066.

[34] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury.* ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.

[35] DOSKOČIL, R., LACKO, B. Root Cause Analysis in Post Project Phases as Application of Knowledge Management. *Sustainability,* ISSN 2071-1050. 11 (2019), 6, pp. 1-15.

[36] DOSKOČIL, R., LACKO, B. Risk Management and Knowledge Management as Critical Success Factors of Sustainability Projects. *Sustainability.* ISSN: 2071-1050. 10 (2018), 5, pp. 1-13.

[37] EU. *Katalog rizik PPP projektů*. Praha: Ministerstvo financí ČR 2004, 31 p.

[38] DAVIDOVÁ, O., LACKO, B. Fuzzy Logic Control Application for The Risk Quantification Of Projects for Automation. In: *Advances in Intelligent Systems and Computing.* ISBN 978-3-319-97887-1.Cham: Springer, 2019, pp. 320-326.

[39] LACKO, B. Process Approach to Test A Soft Computing Software Products. In: *Fifth international conference on soft computing applied in computer and economic environments.* ISBN 80-7314-108- 6. Kunovice: European Polytechnical Institute Kunovice 2007. pp. 101-106.

[40] PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. ČVUT, Praha 2011, ISBN: 978-80-01-04843-6, 301p.

[41] ANDERSON, R. *Security Engineering- A Guide to Building Dependable Distributed Systems.* ISBN 978-0-470-068552-6. J. Willey, 2008, 1001p.

[42] ROLAND, H. E., MORIARITY, B. *System Safety Engineering and Management.* ISBN 0-471-6186-0. J. Willey, 1990, 321p.

[43] IAEA. *Safety Guides and Technical Documents*. Vienna: IAEA 1954 – 2024.

[44] AFROUSS, A., PORTELLI, A., GUARNIERI, F. What Can We Learn about "Engineering Thinking in Extreme Situations" from the Testimony by the Fukushima. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879 -1. London: Taylor &Francis Group 2015, pp. 103-110.

[45] WALKER, T. Resilience Management in Social-Ecological System. *Conservation Ecology*, 6 (2002),1. http://www.consecol.org

[46] 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.

[47] EPRI. *Guideline on Proactive Maintenance. Technical Report*. Palo Alto: EPRI 2001, 82 p.

[48] https://cs.wikipedia.org/w/index.php?title=Rekonstrukce_(stavebnictv%C3%AD) &action=edit

[49] ANTROIT CONSULTANTS. *Planning and Scheduling of Subway Rehabilitation Projects.* https://www.adroitprojectconsultants.com/2017/04/26/planning-scheduling-subway-rehabilitation-projects/?fbclid=IwAR0aRraWW_spl7d0Oh1cqQx 5OOA CLsoVfHcmfXuhYgx0fRKq3CgFcx9JGzI

[50] ANTROIT CONSULTANTS. *Considerations in developing phasing plan in subway rehabilitation projects.* https://www.adroitprojectconsultants.com/2018/ 07/07/considerations-in-developing-phasing-plan-in-subway-rehabilitation-projects/?fbclid=IwAR2ZhvxZtMyS_Vy5cO-PYz3YfxSbqG6_AvxWyOfMqbdTLT5dQSar3I5uEZIA

[51] BECKER, G. *Human Capital: a Theoretical and Empirical Analysis, with Special Reference to Education.* ISBN 0-226-04120-4. Chicago: The University of Chicago Press 1993, 390 p.

[52] DE LA FUENTE, A., CICCONE, A. Human Capital in a Global and Knowledge-based Economy. *Final report*. Universita Pompeu Fabra, Instituto de Análisis Económico 2002.

[53] OECD. *Investment in Human Capital through Post-Compulsory Education and Training: Selected Efficie-ncy and Equity Aspects*. Paris: OECD 2002, 60 p.

[54] VYCHOVA, H., MERTL, J. Relationships of Education and Health in the Context of Economic Development. *Politická ekonomie*, 57 (2009), No 1, pp.58-78.

[55] CLIFFORD, J., THORPE, S. *Workplace Learning & Development: Delivering Competitive Advantage to Your Organization.* ISBN 978-0-7494-4633-8.London: Cogan Publishers 2007.

[56] EU. *Archives.* http://europa.eu/legislation_summaries/education_training_youth/general.framework/ef 0016_cs.htm.

[57] OECD. *Beyond Rhetoric: Adult Learning Policies and Practices*. ISBN 92-64-19943-8. Paris: OECD 2003.

[58] PHILIPS, J. J. *Handbook of Training Evaluation and Measurement Methods*. ISBN 978-0-88415-387-0. New York: Routledge 2011.

[59] IAEA. *Guide to Knowledge Management Strategies and Approaches in Nuclear Energy Organizations and Facilities. NG-G-6.1*. ISBN 978-92-0-125821-2. Vienna: IAEA 2022, 82 p.

[60] IAEA. *Recruitment, Qualification and Training of Personnel for Nuclear Power Plants. SSg-75*. ISBN 978-92-0137222-2.Vienna: IAEA 2022, 66 p.

[61] IAEA. *Nuclear Educational Networks: Experience Gained and Lessons Learned. TECDOC-2007*. ISBN 978-92-0-135422-8. Vienna: IAEA 2022,110 p.

[62] IAEA. *Commissioning for Nuclear Power Plants: Training and Human Resource Considerations*; IAEA Nuclear Energy Series NG-T-2.2. ISBN 978-92-0-103608-7. Vienna: IAEA 2008.

[63] IAEA. *Systematic Approach to Training for Nuclear Facility Personnel: Processes, Methodology and Practices. NG-T-28*. ISBN 978-92-0-113520 -9. Vienna: IAEA 2021, 188 p.

[64] IAEA. *Mentoring and Coaching for Knowledge Management in Nuclear Organizations. TECDOC-1999*. ISBN 978-92-0-123822-1. Vienna: IAEA 2022, 126 p.

[65] PROCHÁZKOVÁ, D. *Archiv řešených úloh z oblasti řízení bezpečnosti a krizového řízení.* Praha: ČVUT, fakulta dopravní, ústav bezpečnostních technologií a inženýrství

[66] JIROVSKÝ, V. *Společnost ve virtuálním světě*. Praha: Konference CYTER2010.

[67] RAŠKA, Z., SERAFÍN, J. Opatření EU na prevenci zneužívání internetu k teroristickým účelům. In: *Ochrana obyvatelstva 2008*. Ostrava: VŠB, pp. 335-340.

[68] BRITO, M. P., AVEN, T., BARALDI, P., CEPIN, M., ZIO,E.; EDS. *Proceedings the 33rd European Safety and Reliability Conference*. ISBN 978-981-18-8071-1. Singapore: Research Publishing 2023, 3578 p.

[69] CEPIN, M. and R. BRIS; eds. *Safety and Reliability – Theory and Applications.* ISBN 978-1-138-62937-0. London: Taylor & Francis Group 2017, 3627 p.

[70] HAUGEN, S., J. VINNEM, A. BARROS, T. KONGSVIK and A. VAN GULIJK; eds. *Safe Societies in a Changing World.* ISBN 978-1-351-17466-4. ISBN 978-1-62276-436-5. London: Taylor & Francis Group 2018, 3234 p.; https://www.ntnu. edu/esrel2018.

[71]BEER, M., ZIO, E.; eds. *Proceedings of the 29th European Safety and Reliability Conference* (ESREL). ISBN 978-981-11-2724-3. Singapore: ESRA, Research Publishing 2019, 4315 p., e:enquiries @rps online.com.sg

[72]BARALDI, P., DI MAIO, F., ZIO, E.; eds. *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020*

PSAM15). ISBN 978-981-14-8593-0. Singapore: ESRA, Research Publishing 2021, 5067 p., enquiries@rps online.com.sg

[73]CASTANIER, B., CEPIN, M., BIGAUD, D., BERENGUER, C.; eds. *Proceedings of the 31st European Safety and Reliability Conference.* ISBN 978-981-18-2016-8. Singapore: ESRA, Research Publishing 2021, 3473 p., enquiries@ rpsonline.com.sg

[74]LEVA, M. C., PATELLI, E., PODOFILLINI, L., WILSON, S.; eds. *Proceedings of the 32nd European Safety And Reliability Conference* (ESREL 2022). ISBN 978-981-18-5183-4. Singapore: ESRA, Research Publishing 2022, 3413 p., enquiries@rpsonline.com.sg

[75] PROCHÁZKOVÁ D. Projektování technických děl založené na řízení rizik.. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-80-01-06906-6. Praha: ČVUT 2021, pp. 49-69. Doi.org/10.14311/BK.97 88001069066.

[76] WALLS, L., M. REVIE and T. BEDFORD; eds. *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. ISBN 978-1-315-37498-7. London: CRC Press 2016, 2942 p.

[77] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN 978-80-01-04844-3. Praha: ČVUT 2011, 483 p.

[78] EU, 2006. *Project Safe-T. Safety in Tunnels Thenmatic Network*, 2003-2006. Brussels: EU. www.safetunnel.net

[79] US PROJECT MANAGEMENT INSTITUTE. *A Guide to the Project Management Body of Knowledge*. Washington: US Project Management Institute 2004.

[80] EU. *The Seventh Frame Research Programme 2007-2013.Brussels, 2006.*

[81] MÁCHAL, P., KOPEČKOVÁ, M., PRESOVÁ, R. *Světové standardy projektového řízení: pro malé a střední firmy*. ISBN 978-80-247-5321-8Praha: Grada Publishing 2015.

[82] FIALA, P. *Projektové řízení modely, metody, analýzy*. ISBN 80-86419-24-X. Praha: Professional Publishing 2004, 276 p.

[83] ŘEPA, V. *Podnikové procesy: Procesní řízení a modelování.* Praha: Grada Publishing 2007.

[84] BUREŠ, V. *Znalostní management a proces jeho zavádění*. Praha: Grada Publishing 2007.

[85] HISLOP, D. *Knowledge Management in Organizations: A Critical Introduction.* ISBN 978-019-9691937. Oxford: Oxford University Press 2013.

[86] SVOZILOVÁ, A. *Projektový management.* ISBN 80-247-1501-5. Praha: Grada Publishing, a.s., 2006, 424 p.

[87] ROSENAU, D. *Řízení projektů.* ISBN 80-7226-218-1. Brno: Computer press 2003, 344 p.

[88] NICKOLS, F. *Thirteen Problem Solving Models*. https://www.uapd.edu.

[89]DORAN, G. T. There's a S.M.A.R.T. Way to Write Management's Goals and Objectives. Management Review. 70 (1981), 11, pp. 35-36.

Příloha 1 – Příklady kontrolních seznamů

Kontrolní seznam pro posuzování kritičnosti technického díla.

Otázka	**Odpověď**	
	ANO	**NE**
Konají se v daném technickém díle kritické činnosti?		
Je prováděno hodnocení rizik pravidelně a po každé větší nehodě?		
Jsou v daném technickém díle kritická nebo hodnotná zařízení?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně umístěná?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně vyrobena?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně instalována?		
Jsou kritická nebo hodnotná zařízení v daném technickém díle správně a bezpečně provozována?		
Jsou všechna propojení mezi kritickými nebo hodnotnými zařízeními v daném technickém díle správně a bezpečně naprojektována, provedena a provozována?		
Jsou správně zabezpečeny kybernetické sítě technického díla?		
Mají všechna kritická nebo hodnotná zařízení v daném technickém díle zálohy?		
Je technické dílo fyzicky zabezpečeno?		
Jsou jasně stanoveny odpovědnosti za provoz technického díla?		
Jsou jasně stanoveny odpovědnosti za provoz kritických nebo hodnotných zařízení v daném technickém díle?		
Je dokumentace technického díla a všech kritických nebo hodnotných zařízení úplná a správná?		
Je prováděna proaktivní preventivní údržba všech kritických nebo hodnotných zařízení technického díla?		
Je zaveden integrovaný systém řízení bezpečnosti technického díla?		
CELKEM		

Kontrolní seznam pro posuzování požární bezpečnosti technického díla.

Otázka	**Odpověď**	
	ANO	**NE**
Je požární útvar technického díla dobře obeznámen se zařízeními, jejich umístěním a se specifickými ohroženími v technickém díle?		
Je požární poplachový systém technického díla certifikován tak, jak je požadováno?		

Je požární poplachový systém technického díla testován alespoň jednou ročně?		
Používá-li požární poplachový systém technického díla vnitřní stoupací potrubí a ventily, jsou pravidelně kontrolovány?		
Používá-li požární poplachový systém technického díla venkovní neveřejné požární hydranty, jsou alespoň jednou ročně odzkoušeny a je dle plánu prováděna rutinní preventivní údržba?		
Jsou požární dveře a požární uzávěry v technickém díle v dobrém provozním stavu?		
Jsou požární dveře a požární uzávěry v technickém díle nezatarasené (tj. volné) a jsou chráněné proti zatarasení včetně jejich protiváh (vyvážení)?		
Jsou automatické řídící ventily vodního sprinklerového systému, tlaku vzduchu a tlaku vody v technickém díle kontrolovány týdně / periodicky tak, jak je požadováno?		
Je údržba automatických sprinklerových systémů v technickém díle přidělena odpovědným osobám nebo je svěřena kontraktorovi?		
V případě, že údržba automatických sprinklerových systémů v technickém díle je přidělena kontraktorovi, je tento řádně poučen, aby se choval tak, aby nezpůsobil nehodu?		
Jsou hlavice sprinklerů v technickém díle chráněny kovovými kryty, když jsou vystaveny fyzickému poškození?		
Je v technickém díle řádně udržován prostor pod sprinklerovými hlavicemi?		
Jsou přenosné hasicí přístroje v technickém díle k dispozici v adekvátním množství a v odpovídajících typech?		
Jsou hasicí přístroje v technickém díle připevněny ve snadno dosažitelné poloze?		
Jsou hasicí přístroje v technickém díle pravidelně plněny a označeny visačkou o inspekci?		
Jsou zaměstnanci technického díla pravidelně instruováni o použití hasicích přístrojů a o postupech požární ochrany?		
Jsou prováděna pravidelná cvičení akceschopnosti požární techniky technického díla?		
Odpovídá požární technika i personál požadavkům, které vyžaduje požární ochrana technického díla?		
CELKEM		

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

Otázka	**Odpověď**	
	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 přijatelnosti 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 sedm procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; dokumentace a šetření havárií; a kybernetické a fyzické zabezpečení?		
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)?		
Má SMS správce technického díla proces pro zabezpečení technického díla, který obsahuje podprocesy pro: fyzické zabezpečení; a kybernetické zabezpečení.		
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 nouzové 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		

Pozn.: Další kontrolní seznamy lze nalézt v publikacích:

PROCHÁZKOVÁ, D., ŠESTÁK, B. *Kontrolní seznamy. Nástroj rizikového inženýrství*. ISBN 80-7251-225-0. Praha: PA ČR 2006. 319 p.

PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. ISBN 978-80-01-04841-2. Praha: ČVUT 2011. 40 5 p.

PROCHÁZKOVÁ D. *Analýza, řízení a vypořádání rizik spojených s technickými díly*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. Doi:10.14311%2FBK.9788001064801

PROCHÁZKOVÁ, D. Řízení rizik - Kontrolní seznamy a jejich využití při výstavbě a provozu potrubí. In: *Potrubí 2023*. ISBN 978-80-87140-65-9. Líbeznice: Medim s.r.o. 2023, pp. 7-26.

PROCHÁZKOVÁ, D. Vybrané kontrolní seznamy pro řízení rizik strojních a elektrických zařízení. In: *Řízení rizik procesů, zařízení a složitých technických děl zacílené na bezpečnost 2023.* ISBN 978-80-01-07239-4. Praha: ČVUT 2023, pp. 144-166. Doi: 10.14311/BK.9788001072394

Příloha 2 – Příklady plánů pro řízení rizik

Plán řízení rizik pro letadlo.

Použité zkratky: NTSB = National Transportation Safety Board; ŘLP = Řízení letového provozu; SAS = Skybrary aviation safety.

Příčina rizika	**Nejvyšší dopady rizika**	**Ocenění pravděpodobnosti výskytu a dopadů nejvyššího rizika**	**Opatření pro zmírnění rizika a určené odpovědnosti**
Oblast rizika – organizační			
Ztráta orientace	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku	***Pravděpodobnost:*** malá ***Dopady:*** velké	***Opatření:*** použití náhradních způsobů orientace - dle reliéfu terému a požádání o pomoc řízení letového provozu [1]. ***Provede:*** pilot [1]. ***Odpovědnost:*** pilot [1].
Chybné vyhodnocení situace	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** střední ***Dopady:*** velké	***Opatření:*** provedení opravného manévru [2]. ***Provede:*** pilot [1]. ***Odpovědnost:*** pilot [1].
Špatná spolupráce posádky	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** střední	***Opatření:*** okamžité zavedení pořádku a později změna posádky [2]. ***Provede:*** velitel letadla [2]. ***Odpovědnost:*** velitel letadla [2].
Nezvla-datelný cestující	***Dopravní nehoda*** se:	***Pravděpodobnost:*** střední	***Opatření:*** pohovor, přikurtování k sedadlu, popř. oddělení od

	- ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Dopady:*** střední	ostatních, přistání na vhodném letišti [3]. ***Provede:*** velitel letadla [3]. ***Odpovědnost:*** velitel letadla [3].
Oblast rizika – technická			
Výpadek motoru	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** střední	***Opatření:*** zahájit nouzové klesání a vyslání zprávy na řízení letového provozu [2,4-6]. ***Provede:*** pilot „letící" [2,4-6]. ***Odpovědnost:*** pilot „letící" [2,4-6].
Nefun-kční výškoměr	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** střední	***Opatření:*** použití záložních systémů určení polohy [5]. ***Provede:*** pilot [5]. ***Odpovědnost:*** pilot [5].
Úbytek kyslíku na palubě	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** vysoká	***Opatření:***spuštění kyslíhových masek, vyslání zprávy na řízení letového provozu [7]. ***Provede:*** pilot [7]. ***Odpovědnost:*** pilot [7].
Oblast rizika – narušení bezpečnosti z vnitřních příčin			
Požár v kabině	***Dopravní nehoda*** se:	***Pravděpodobnost:*** malá	***Opatření:*** použití hasících přístrojů na palubě , vyslání zprávy na řízení letového

	- ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Dopady:*** velmi vysoké	provozu, snaha o rychlé přistání [8]. ***Provede:*** velitel letadla [8]. ***Odpovědnost:*** velitel letadla [8].
Požár v zavaza-dlovém prostoru	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** velmi vysoké	***Opatření:*** nouzové přistání na nejbližším vhodném letišti [1]. ***Provede:*** velitel letadla [1]. ***Odpovědnost:*** velitel letadla [1].
Oblast rizika – narušení bezpečnosti z vnějších příčin			
Velké propadnutí letounu	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** střední	***Opatření:*** opravný zásah v řízení letadla [9]. ***Provede:*** pilot „letící" [9]. ***Odpovědnost:*** pilot „letící" [9].
Velký elektrický výboj	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** vysoké	***Opatření:*** okamžité převzetí manuálního řízení [8]. ***Provede:*** pilot [8]. ***Odpovědnost:*** pilot [8].
Útok cizího letadla	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí,	***Pravděpodobnost:*** malá ***Dopady:*** velmi vysoké	***Opatření:*** nouzové přistání na nejbližším vhodném letišti [10]. ***Provede:*** pilot „letící" [10]. ***Odpovědnost:*** pilot „letící" [10].

	- náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.		
Oblast rizika – kybernetická propojení			
Ztráta spojení	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** střední ***Dopady:*** střední	***Opatření:*** nastavení nouzového kódu odpovídače letadla [8]. ***Provede:*** pilot „letící" [8]. **Odpovědnost:** pilot „letící" [8].
Hackerský útok na systém řízení letadla	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** velmi vysoké	***Opatření:*** aplikace manuálního řízení [3]. ***Provede:*** pilot „letící" [3]. ***Odpovědnost:*** pilot „letící" [3].
Podivné hlášení – neobvyklá aktivace senzorů	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** malá ***Dopady:*** velmi vysoké	***Opatření:*** prověření varovných systémů, vyslání zpráva na řízení letového provozu [6]. ***Provede:*** velitel letadla [6]. ***Odpovědnost:*** velitel letadla [6].

Plán řízení rizik pro letiště.

Oblast rizika	**Příčina rizika**	**Dopady nejvyššího rizika**	**Ocenění pravděpodobnosti výskytu a dopadů nejvyššího rizika**	**Opatření na zmírnění rizika a určené odpovědnosti**

Organizační	Neposkytnutí nebo poskytnutí nesprávné informace letadlu	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** nízká ***Dopady:*** velmi vysoké	***Opatření:*** provést urychleně opravné hlášení [11]. ***Provede:*** pracovník pověřený vedoucím směny na řízení letového provozu [11]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu [11].
	Umístění letadla na nesprávnou dráhu	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** nízká ***Dopady:*** vysoké	***Opatření:*** urychlené uvolnění dráhy a vyzvání pilota přistávajícího letadla k posečkání a opatrnosti [12]. ***Provede:*** pracovník pověřený vedoucím směny na řízení letového provozu [12]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu [12].
	Neschopnost pomoci letadlu v nesnázích	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu,	***Pravděpodobnost:*** nízká ***Dopady:*** velmi vysoké	***Opatření:*** okamžité odstartování nouzových opatření a činnosti nouzových služeb; později zajistit kvalitní výcvik řídících letového provozu [11]. ***Provede:*** pracovník pověřený vedoucím směny na řízení letového provozu [11]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu; později ředitel výcviku řízení letového provozu [11] zajistí výcvik.

		- náklady na odškodnění pozůstalých, - náklady na škody na majetku.		
	Zmatek na pracovišti řízení letového provozu z důvodu vnějšího zásahu jako je např. požár	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** nízká ***Dopady:*** velmi vysoké	**Opatření:** přijmout opatření pro nouzový režim, tj. varovat letadla v přímém řízení a zajistit urychlený přechod na náhradní pracoviště a urychleně zahájit činnost [11]. **Provede:** pracovník pověřený vedoucím směny na řízení letového provozu [11]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu [11].
Technická	Špatný stav dráhového systému letiště	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** nízká ***Dopady:*** velmi vysoké	***Opatření:*** okamžitě uzavřít poškozené dráhy [3]. ***Provede:*** pracovník pověřený ředitelem letiště [3]. ***Odpovědnost:*** ředitel letiště [3].
	Špatné rozmístění techniky na letišti	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku,	***Pravděpodobnost:*** nízká ***Dopady:*** střední až vysoké	***Opatření:*** provést nápravná opatření a zajistit vydání výstražných zpráv NOTAM o stavu letiště [3]. ***Provede:*** pracovník pověřený provozním ředitelem letiště [3].

		- poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.		***Odpovědnost:*** provozní ředitel letiště [3].
	Nefunkční varovný systém	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** nízká ***Dopady:*** velmi vysoké	***Opatření:*** okamžitě provést nápravu, tj. aktivovat náhradní varovné systémy; později cvičit letový i pozemní personál na práci s nefunkčními technickými systémy [3]. ***Provede:*** pracovník pověřený vedoucím směny na řízení letového provozu [3]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu; později ředitel výcviku řízení letového provozu [3].
Vnější podmínky	Mlha	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** střední ***Dopady:*** vysoké	***Opatření:*** uvést v činnost všechny pozemní radary a pomocná zařízení pro orientaci na letišti [13]. ***Provede:*** pracovník pověřený : technickým ředitelem letiště [13]. ***Odpovědnost:*** technický ředitel letiště [13].

	Zaplavení / zasnežení letiště	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** nízká ***Dopady:*** vysoké	***Opatření:*** provést okamžité uzavření letiště, varovat letadla v přímém řízení a zahájit odklízecí práce [12]. ***Provede:*** pracovníci pověření vedoucím směny na řízení letového provozu, a za odklízení ředitelem údržby letiště [12]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu, za odklízení ředitel údržby letiště [12].
	Fyzický útok na letiště nebo na jeho dispečerské stanoviště	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** střední ***Dopady:*** vysoké	***Opatření:*** nařídit okamžitý zásah bezpečnostních složek [3]. ***Provede:*** pracovník pověřený vedoucím směny na řízení letového provozu [3]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu [3].
Kybernetická	Ztráta spojení	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu,	***Pravděpodobnost:*** střední ***Dopady:*** střední	***Opatření:*** aktivovat nouzové systémy, a to včetně manuálních a mechanických prostředků s cílem pomoci letadlu; později cvičit pozemní personál na bezpečné zacházení s letadlem bez spojení [8]. ***Provede:*** pracovník pověřený vedoucím směny na řízení letového provozu [8].

		- náklady na odškodnění pozůstalých, - náklady na škody na majetku.		***Odpovědnost:*** vedoucí směny na řízení letového provozu; později ředitel výcviku řízení letového provozu [8].
	Hackerský útok na systém řízení letového provozu	***Dopravní nehoda*** se: - ztrátami na lidských životech či poškození zdraví, - škodami na majetku, - poškození složek životního prostředí, - náklady na odezvu, - náklady na odškodnění pozůstalých, - náklady na škody na majetku.	***Pravděpodobnost:*** nízká ***Dopady:*** velmi vysoké	***Opatření:*** aktivovat nouzové systémy, a to včetně manuálních a mechanických prostředků s cílem pomoci letadlu; později cvičit technický personál na okamžité odvrácení hackerského útoku [3]. ***Provede:*** pracovník pověřený vedoucím směny na řízení letového provozu [3]. ***Odpovědnost:*** vedoucí směny na řízení letového provozu; později technický ředitel řízení letového provozu [3].

Literatura

[1] NATIONAL TRANSPORTATION SAFETY BOARD. *Loss of Thrust in Both Engines, US Airways Flight 1549 Airbus Industrie A320-214, N106US.* http://www. ntsb.gov/investigations/AccidentReports/ Pages/AAR1003.aspx

[2] NATIONAL TRANSPORTATION SAFETY BOARD. *Controlled Flight Into Terrain, Korean Air Flight 801, Boeing 747-300, HL7468.* http://www.ntsb.gov/investigations/AccidentReports/Pages/AAR0001. aspx

[3] IATA. http://www.iata.org/

[4] MIKA, L. Letecká provozní bezpečnost ve světě v roce 2015*. Letectví + kosmonautika.* ISSN 0024-1156. 92 (2016), pp. 50-52.

[5] SKYBRARY AVIATION SAFETY. *A332, en-route, Atlantic Ocean. 2009.* http:// www.skybrary.aero/ index.php/A332,_en-route,_Atlantic_Ocean,_2009

[6] SKYBRARY AVIATION SAFETY. *MD83 En Route South East of Gossi, Mali 2014.* http://www.skybrary.aero/index.php/MD83_En_route_south_east_of_Gossi,_Mali_2014

[7] SKYBRARY AVIATION SAFETY. *B733, en-route, Grammatiko Greece, 2005.* http://www.skybrary. aero/index.php/B733,_enroute,_Grammatiko_Greece, _2005

[8] ŘÍZENÍ LETOVÉHO PROVOZU ČR. *Interní databáze událostí v letovém provozu.* Jeneč: ŘLP 2016.

[9] NATIONAL TRANSPORTATION SAFETY BOARD. *In-Flight Separation of Vertical Stabilizer American Airlines Flight 587, Airbus Industrie A300-605R, N1405 3.* http://www.ntsb.gov/investigations/ AccidentReports/Pages/AAR0404.aspx

[10] DUTCH SAFETY BOARD. *Investigation Crash MH17, 17 July 2014 Donetsk.* http://www.onderzoeks raad.nl/en/onderzoek/2049/investigation-crash-mh17-17-july-2014

[11] SKYBRARY AVIATION SAFETY. *T154 / B752, en-route, Uberlingen Germany, 2002.* http://www.sky brary. ero/index.php/T154_/_B752,_enroute,_Uberlingen_Germany,_2002

[12] SKYBRARY AVIATION SAFETY. *B744, Taipei Taiwan, 2000.* http://www.sky brary.aero/index.php /B744,_Taipei_Taiwan,_2000

[13] SKYBRARY AVIATION SAFETY. *MD87 / C525, Milan Linate, 2001.* http://www .skybrary.aero/index. php/MD87_/_C525,_Milan_Linate,_2001

Podrobnosti jsou v publikaci: PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. ISBN 978-80-01-06995-0. Praha: DSPACE ČVUT 2022, 129 p., http://hdl.handle.net/10467/100674, doi:10.14311/BK.9788001069950.

Titul:	Vypořádání rizik v inženýrských oborech
Autorský kolektiv:	Doc. RNDr. Dana Procházková, CSc., DrSc.
Recenzenti:	Doc. Ing. Branislav Lacko, CSc. Doc. Ing. Petr Šrytr, CSc.
Vydavatel:	DSPACE ČVUT v Praze
Počet kopií:	Open Access
Počet stránek:	130
Rok vydání:	2024

ISBN: 978-80-01-07272-1