ZÁSADY ŘÍZENÍ RIZIK SLOŽITÝCH TECHNOLOGICKÝCH ZAŘÍZENÍ

Dana Procházková

Praha 2017

Recenzenti:

Prof. Ing. Josef Říha, CSc., DrSc.

Doc. Ing. Václav Beran, CSc., DrSc.

ISBN: 978-80-01-06182-4

OBSAH

SEZNAM ZKRATEK

AFIS	Letová informační služba
AHP	Analytical Hierarchy Process
ALARA	As Low As Reasonable Achievable
ALARP	As Low As Reasonable Possible
ARSS	Availability, Reliability, Safety, Security
BOZP	Bezpečnost a ochrana zdraví při práci
CBA	Cost Benefit Analysis
ČR	Česká republika
DSM	Dopravní systém metra
DSS	Decission Support System (Systém pro podporu rozhodování)
EMA	Emergency Management Agency
EPS	Elektrická požární signalizace
EU	European Union
FEMA	Federal Emergency Management Agency
HHM	Hierarchické holografické modelování
HZS	Hasičský záchranný sbor
IAEA	International Atomic Energy Agency - Mezinárodní agentura pro atomovou energii
ISO	International Organization for Standardization
IT	Informační technologie
IZS	Integrovaný záchranný systém
KI	Kritická infrastruktura
MUT	Multiatribute Utility Theory
NASA	National Aeronautics and Space Administration
NEA	Nuclear Energy Agency
OECD	Organizace pro hospodářskou spolupráci a rozvoj
OSM	Ochranný systém metra
OSN	Organizace spojených národů
PSA	Probabilisticc Safety Assessment (Pravděpodobnostní hodnocení bezpečnosti)
PSM	Process Safety Management /Proce pro řízení bezpečnosti)
RAMS	Reliability, Availability, Mantainability, Security
SCBA	Social Cost-Benefit Analysis
SIL	Safety Integrity Level
SMS	Safety Management System (Systém řízení bezpečnosti)
SoS	Systém of Systems (Systém systémů)
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
TQM	Total Quality Management (řízení celkové kvality)
UGTMS	Systém pro řízení městské kolejové dopravy
USA	United States of America
VZLU	Výzkumný a zkušební letecký ústav
WANO	World Association of Nuclear Operators
WB	World Bank
ZZS	Zdravotní záchranná služba

PŘEDMLUVA

Technologická zařízení nebo přesněji technická díla jsou důležitými základními veřejnými aktivy lidského systému, kterým je prostředí, ve kterém žijeme. Cílem lidského snažení je zajistit životy, zdraví, bezpečí a rozvoj lidí. Proto lidé musí pečovat o základní veřejná aktiva a své chování přizpůsobit tak, aby byla zachována koexistence základních systémů (environmentálního, sociálního a technologického), které jsou nezbytné pro existenci a život lidí na naší planetě.

Nejprve si je třeba uvědomit, že lidská společenství od dob historických vždy pečovala o technická díla, infrastruktury a dodavatelské řetězce, které si vybudovala v rámci zvyšování kvality života komunit. Od starověku v celé historii lidstva na různých místech světa jsou zřetelným příkladem předmětného úsilí 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 pracovalo na bezpečnosti. K zásadnímu rozdílu v pojetí došlo v polovině 90. let minulého století, kdy se přešlo 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.

Cílem předložené publikace není popis a analýza historie, ale prosazení poučení ze selhání ochranných technických systémů, které ukazuje jak význam kvality řízení lidí a zdrojů, tak význam materiálně technické základny. Práce se soustřeďuje na technická díla, která zajišťují kvalitu života lidí a při kritických situacích pomáhají lidem přežít jejich útrapy. Na základě shromážděných znalostí zdůrazňuje, že koncept veřejného blaha spočívá v zajištění koexistence tří základních systémů, a to systému životního prostředí, sociálního a technologického.

Je skutečností, že všechna lidská společenství i všechna lidská sídla jsou čas od času postihována škodlivými jevy (pohromami). Rizika s nimi spojená jsou proměnná v čase i prostoru a závisí jak na proměnnosti pohrom, ke které dochází v důsledku dynamického vývoje světa, tak na zranitelnosti lidí a veřejných aktiv, která lidé potřebují k životu, a v neposlední řadě také na možnostech lidí při budování ochranných systémů. Proto vznikla disciplína rizikové inženýrství, jejímž cílem je řídit rizika tak, aby lidská sídla na všech úrovních byla bezpečnými systémy. V důsledku dynamického vývoje světa jde pochopitelně o dynamickou disciplínu, která zohledňuje jak fakt, že pohrom je velké množství a v důsledku rozmanitosti jejich podstaty jejich dopady nejsou stejné, tak fakt, že území a lidská společenství, která je obývají, se odlišují vlastnostmi a proměnnými možnostmi, což se projevuje různou zranitelností aktiv a různými možnostmi lidí v čase a prostoru. Proto každé riziko je místně a časově specifické, a při jeho řízení a ovládání je třeba předmětnou skutečnost zvažovat.

Právě zmíněný fakt ukazuje, že pro řízení a zvládnutí rizik je nutno používat opatření a činnosti, která jsou místně a časově specifické. Lze pouze konstatovat, že uvedený logický závěr je potvrzen i výsledky výzkumů, které se realizovaly v rámci mnoha nákladných projektů EU (např. CASCADE, CIPRnet, EDEN). Předmětné projekty dle dostupné dokumentace zatím potvrdily jen fakta, která jsou logicky odvoditelná z poznatků, které lidstvo shromáždilo během historického vývoje, a to:

- jestliže chceme zajistit bezpečí určitého systému, tj. celku skládajícího se z území a příslušného lidského společenství, tak musíme dané území a jeho obyvatele řádně poznat tím, že se analyzují a vyhodnotí historické pohromy v souvislostech, přičemž se zváží jak zranitelnosti aktiv, tak lidské schopnosti a možnosti v dané době,

- každá země EU si musí vytvořit systém ochrany aktiv i kritické infrastruktury takový, který navazuje na její historicky zavedené systémy ochrany, protože z pochopitelných důvodů není možné navrhnout a zavést jeden univerzální systém ochrany kritické infrastruktury pro všechny země EU (každá unifikace vyžaduje čas, finance, nástroje pro změny a přizpůsobení lidí, a nemusí být přijatelná z hlediska národních tradic a kultur).

Vzhledem k uvedeným skutečnostem je třeba, aby každá země budovala systém řízení bezpečností, který zajišťuje jak ochranu lidí a životního prostředí, tak ochranu technických děl, základních infrastruktur a dodavatelských řetězců. Daný cíl lze efektivně dosáhnout jen kvalifikovaným přístupem a kvalitním řízením aktivit, zdrojů, sil a prostředků, což zajistí pouze dobré vzdělání. Proto předmětná kniha, která je výsledkem projektu ČVUT „OHK2-003/15, Řízení bezpečnosti a ochrana kritických objektů a kritických infrastruktur“, obsahuje jak souhrn znalostí získaný výzkumem, a to vlastním i ze studia odborných prací, tak souhrn nových znalostí vyplývajících z řešení konkrétních praktických úloh, které jsou především zacíleny na podmínky České republiky.

Předložená práce se zaměřuje na problémy praxe, tj. na fyzikální, chemické, biologické a sociální procesy a matematické základy a odvození uvádí jen v nezbytně nutné míře, a to proto, že tvorba matematických vztahů zpravidla znamená postižení jen typických vlastností objektů a zanedbání nezřetelných nebo dosud nezjištěných vlastností. Práce obsahuje syntézu současného poznání a dynamický vývoj světa chápe tak, že neexistují uzavřené neměnné technologické ani jiné systémy v neměnném okolí. Zvažuje nejen proměny prostředí a materiálů v čase, ale i skutečnost, že všechny technologické systémy se mění v důsledku působení jak času, tak výskytem pohrom majících velikosti větší než projektové. Při výskytu nadprojektových pohrom vznikají kritické podmínky, na které nejsou technologické objekty konstruovány a dochází k závažným selháním funkcí technických děl, která působí závažné ztráty lidem, ekonomice, životnímu prostředí i technologickým objektům samotným.

Provedené analýzy dopadů pohrom, a to hlavně havárií a selhání ukazují, že pro bezpečí a rozvoj lidí, je třeba s kritickými podmínkami počítat. Z důvodu omezených možností lidí, lidé jsou schopni technologické objekty vybudovat jako bezpečné systémy jen pro jistý interval podmínek, a pro případ jiných podmínek pak musí vytvářet nástroje, kterými sníží ztráty, újmy a škody na všech veřejných aktivech (tj. i na technických dílech a infrastrukturách, které poskytují výrobky nebo služby, a to ať jsou veřejné nebo soukromé). Proto předmětný výzkum zacílený na zajištění bezpečných technických děl se opírá o poznání chování složitých technologických objektů za různých podmínek na základě sběru a zpracování konkrétních dat s použitím kritického myšlení a metod rizikového inženýrství, a hledá reálné nástroje a postupy, kterými lze buď zabránit realizaci nepřijatelných rizik, anebo zmírnit jejich dopady na veřejná aktiva, tj. i na technická díla.

Předložená práce shrnuje jak výsledky celoživotního systematického studia autorky, tak výsledky projektů vedených vědeckých týmů, které byly vždy zacíleny na bezpečí technologických objektů, infrastruktur a území, a byly vždy prováděny v souladu s rozvojem celosvětového poznání, o které se opíraly.

Výsledky provedeného výzkumu, uvedené v práci jsou: uceleně zpracované poznatky o riziku a bezpečnosti; výsledky konkrétních analýz a hodnocení reálných havárií a selhání technických děl; výsledky simulací chování technických děl při kritických a extrémních podmínkách, tj. velkých havárií a selhání technických děl pomocí přístupů a metod rizikového inženýrství; porovnání schopnosti nástrojů používaných pro zajištění bezpečných technických děl; přehled a příklady vhodných nástrojů rizikového inženýrství, kterými lze zajistit bezpečná technická díla v reálných podmínkách; a zásady pro řízení rizik technických děl na všech úrovních řízení lidské společnosti.

Autorka děkuje ČVUT za grant SGS-2015 (OHK2-003/15, Řízení bezpečnosti a ochrana kritických objektů a kritických infrastruktur). Velmi děkuje všem účastníkům výzkumu (RNDr.

Jan Procházka, PhD., Ing. Zdenko Procházka, CSc., Ing. Tomáš Kertis, Ing. Hana Patáková, Ing. Veronika Strymplová, Ing. Pavel Remeš, Ing. Jan Kopřiva, Ing. Jan Krákora, Ing. Jakub Šimík, Ing. Marek Pražan, Ing. Ekaterina Koshkina, Ing. J. Král, Ing. Věra Samoilová) za sběr dat a poznatků. Velký dík patří recenzentům panu Prof. Ing. Josefu Říhovi, DrSc. a Doc. Ing. Václavu Beranovi, DrSc. za cenné připomínky, a vedoucímu ústavu bezpečnostních technologií a inženýrství panu Doc. Ing. Václavu Jirovskému, CSc. za podmínky pro výzkum.

1. ÚVOD

Velká technická díla, tj. složitá technologická zařízení jsou otevřené složité socio-technologické systémy (anebo v souladu se současným vývojem socio-kyber-technologické systémy), které zahrnují budovy, jejich zařízení, infrastruktury, obslužný personál i systém jejich řízení. Jejich vlastní aktiva tudíž tvoří stavby, jejich prvky, zařízení, obsluha a další personál, konstrukční a kybernetická propojení způsobující požadované vazby a toky mezi vyjmenovanými položkami, znalosti (know-how), provozní postupy, výrobky, rezervy (materiálové, finanční, lidské a další), smlouvy o spolupráci s veřejnou správou, bezpečnostními složkami, výzkumnými institucemi, veřejností atd. Představují otevřený systém skládající se z řady vzájemně se prolínajících otevřených systémů (od r. 2000 se pro jejich formu vžilo označení systém systémů; anglicky system of systems (SoS), v americké angličtině systems system), které se dynamicky mění [1].

Složitost technických děl, tj. systémů systémů (SoS) vychází z požadovaných rysů systémů, a to: velký rozměr; použití více technologií; složité funkční závislosti; velká interoperabilita; velký výkon; a vysoká bezpečnost, tj. funkčnost a spolehlivost i nízké ohrožení chráněných aktiv při podmínkách normálních, abnormálních i kritických.

Je skutečností, že žádné technické dílo není v prostoru a čase osamocené. Je umístěno do území a do lidské společnosti, které ho ovlivňují. Společně vytváří lidský systém, ve kterém se vyskytují pohromy, tj. škodlivé jevy všeho druhu, jejichž velikost se mění v čase a prostoru. Předmětné jevy od jisté velikosti poškozují technická díla a jejich narušení mohou vyvolat domino efekty, které ještě zvýší ztráty na životech lidí a škody na dalších veřejných aktivech (tj. včetně dalších technických děl) lidského systému, který je modelem našeho světa [1].

Cílem lidského snažení je zajistit životy, zdraví, bezpečí a rozvoj lidí. Proto na základě současného poznání [2] lidé musí:

- pečovat o základní veřejná aktiva (životy, zdraví a bezpečí lidí; majetek a veřejné blaho; životní prostředí; infrastruktury a technologie),
- své chování uzpůsobit tak, aby byla zachována koexistence základních systémů (environmentálního, sociálního a technologického), které jsou nezbytné pro existenci a život lidí, tj. pro bezpečný lidský systém, který má rovněž povahu SoS.

K danému cíli lidé používají nástroj „řízení“. Řízení (Management) je velmi široký pojem. Řídit znamená „mít pod svým vedením, ovládat, spravovat, regulovat, usměrňovat“. Od doby zakladatele vědeckého řízení pana Taylora a jeho následovníka pana Fayola [3,4] se základní funkce řízení nezměnily. Vykonavatelem řízení jsou lidé, kteří vedou předmětnou entitu k prosperitě a efektivitě. Předmětná skutečnost platí i pro poloautomatické a automatické řízení, protože jejich algoritmy vytvořil člověk. V reálném světě člověk může dobře řídit své chování a chování děl, která vytvořil, když si uvědomí omezení svých možností a schopností, a podle toho navrhuje a provádí svá opatření a činnosti.

Správné řízení lidského systému zacílené na zajištění bezpečí a rozvoje lidí dle [2] znamená, že lidé provádí opatření a činnosti, které zajišťují:

- existenci, tj. rovnováhu v lidském systému,
- 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.

Je pochopitelné, že výše uvedené požadavky jsou kladeny i na technická díla, která patří do veřejných aktiv. Na základě současného poznání [1,2,5] lze uvedený cíl splnit jen tehdy, když lidé při řízení území, technického díla, státu aj.:

- zvažují všechna chráněná aktiva; u technických děl jde jak o veřejná aktiva, tak o vlastní aktiva technických děl, kterými jsou: majetek a technologie, know-how, prosperita, soulad organizace se státem v místě působení (tj. plnění úkolů, ke kterým byla organizace zřízena), konkurenceschopnost, good will apod.,
- používají současné poznání v kontextu teorie systémů,
- řídí své činnosti tak, aby nezpůsobovali jevy, které by vedly k desintegraci až rozpadu lidského systému (tj. nevytvářeli vědomě podmínky pro vznik tzv. organizačních havárií).

Technická díla (objekty i infrastruktury) jsou základním veřejným aktivem, protože:

- zajišťují výrobky a služby, které zkvalitňují život lidí,
- přispívají k: zaměstnanosti; technické vzdělanosti; energetické soběstačnosti; a konkurenceschopnosti,
- vytváří zázemí odezvy na kritické situace (každá odezva potřebuje energii, technické prostředky, finance, dopravní prostředky, materiál apod.).

Proto lidé a všechny řídící struktury lidské společnosti musí dbát o jejich bezpečnost. Z logického důvodu se v předložené publikaci nejprve zmíníme o pohromách, která jsou zdroji rizik pro technická díla samotná i pro lidský systém. Poté shrneme poznatky o práci s riziky a o složitých socio-kyber-technologických systémech, kterými dnešní technická díla jsou. Dále pak shrneme výsledky vlastního studia zacíleného na bezpečnost složitých technologických systémů.

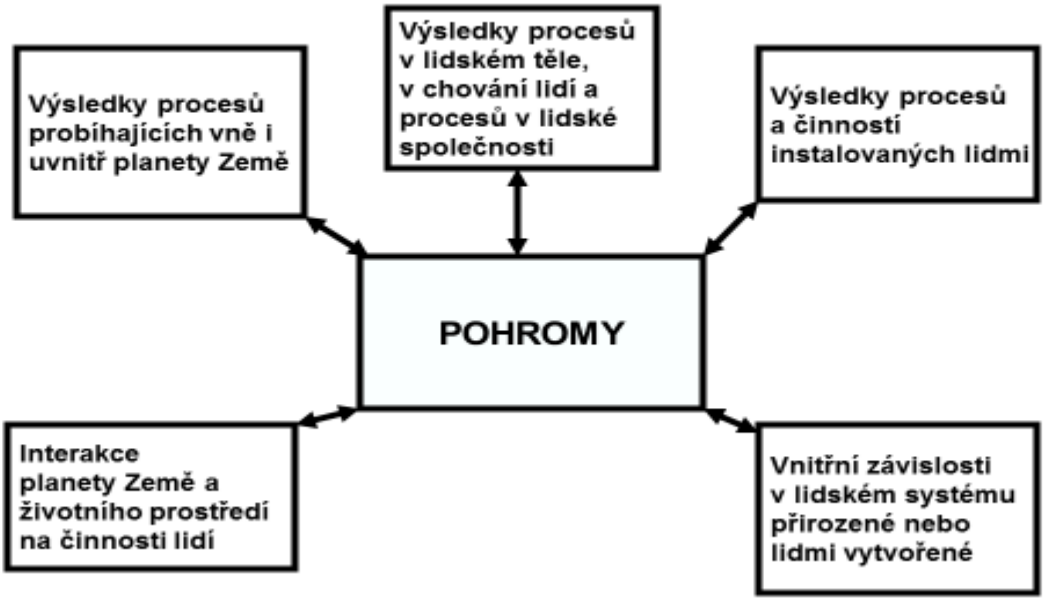
2. POZNATKY SPOJENÉ S RIZIKEM A BEZPEČNOSTÍ

Pro zajištění lidských přání (bezpečí a rozvoj lidí) je třeba především poznat škodlivé jevy, které brání jejich uskutečňování, tj. pohromy. Dále je třeba pochopit a důkladně poznat jejich projevy, tj. možná rizika a na základě shromážděných poznatků navrhnout opatření a činnosti, která jsou lidmi uskutečnitelná v současných podmínkách. Výsledkem zacíleného studia jsou skutečnosti uvedené v dalších odstavcích.

2.1. Pohromy a s nimi spojená nebezpečí, ohrožení a rizika

Na základě současného poznání jsou pohromy výsledky pěti procesů, které probíhají v lidském systému, obrázek 1 [2,5]. Podrobné jednotným způsobem provedené studium pohrom v ČR i v Evropě [6,7] ukázalo jejich rozložení a vlastnosti a také odhalilo nedostatky v jejich řízení. Hlavní nedostatky v řízení pohrom jsou:

- přístup All-Hazard-Approach [6-8]není systematicky aplikován, tj. při zjišťování bezpečí lidí, území i objektu nejsou zvažovány všechny pohromy možné v dané entitě,
- pohromy způsobené člověkem jsou řešeny odděleně od přírodních, technických a dalších, a tím vznikají problémy mezi bezpečností (safety) a zabezpečením (security) entity. Jejich špatné logické pochopení se pak projevuje i ztrátami lidských životů, např. [9],
- dopady a velikost některých pohrom (hlavně v sociální oblasti) jsou podceňovány, což vede ke snížení obranyschopnosti entit,



Obr. 1. Procesy, jejichž výsledkem jsou pohromy v lidském systému.

- systémové, strategické a proaktivní řízení není v řadě případů entit (a to včetně technických děl) implementováno do praxe,
- není sledována koexistence základních životodárných systémů systémů, které mají různou podstatu,
- existují závažné mezery v řízení rizik, inženýrství rizika a ve vyjednávání s riziky (např. neberou se v úvahu všechna důležitá aktiva, proměnnost zranitelností aktiv v čase a prostoru),

- strategie nejsou založeny na dlouhodobých prioritách respektujících veřejný zájem, jejich cíle jsou ovlivňovány politiky nebo lobby,
- postupy aplikace a orientace strategií nejsou pravidelně ověřovány na základě kvalitního monitoringu, což zamezuje přizpůsobení prováděných opatření a činností změnám entit,
- chybí rozumná strategie pro řízení pohrom (tj. pravidla optimalizace opatření s ohledem na konkrétní podmínky a možnosti entity, jelikož např. kvalitní opatření vůči jedné pohromě jsou kontraproduktivní vůči jiné pohromě, která je také možná v entitě [6]),
- řízení pohrom často nerespektuje cyklus výskytu pohrom (velké pohromy se vyskytují zřídka a nepravidelně, proto rozhodování a řízení se musí opírat o dostatečně dlouhé časové řady – teorie o černých labutích nebo královských dracích sice utěšují tvůrce strategií, ale nepředstavují racionální řešení problémů),
- chybí důraz na řešení problémů entit spojených s konkrétními riziky, je jen mnoho diskusí o problémech,
- nedostatek zdrojů pro implementaci lidských potřeb,
- nedostatek nástrojů pro zajištění finanční stability EU,
- nedostatek nástrojů řízení, které podporují ochranu obyvatelstva a udržitelný rozvoj.

Faktem je, že se stále objevují nové zdroje pohrom (jde hlavně o projevy možných propojení mezi systémy v reálném světě), a tím roste počet pohrom. Některé z pohrom mohou lidé zvládnout pomocí preventivních opatření, pro jiné je třeba mít připravena opatření odezvy, zmírňující opatření a standardní zdroje s tím, že pro velké pohromy je třeba mít připraveny nadstandardní zdroje, síly a prostředky [2]; stav v Evropě ukazuje obrázek 2.

Obr. 2. Rozdělení pohrom podle nároků na zvládnutí jejich dopadů.

Na základě současného poznání je třeba věnovat specifickou pozornost rizikům, spojeným s chováním člověka, a to především při řízení a rozhodování [1]. Tzv. organizační havárie jsou dle současného poznání způsobeny jednou nebo několika dále uvedených příčin: řídící pracovník přecenění vlastní rozhodnutí; neznalost a nezkušenost řídícího pracovníka; neschopnost řídícího pracovníka zajistit včasné a správné předání zásadních informací; malé oprávnění řídícího pracovníka při řešení problémů; řídící pracovník podcenění závažnost situace; řídící pracovník při rozhodování nerespektuje zákonitosti přírodní, technické, ekonomické či sociální. Proto je důležité neustálé vytváření kultury bezpečnosti [1,10].

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 zájmů, jejich obnově a k nastartování jejich dalšího rozvoje.

2.2. Nebezpečí, ohrožení a riziko

V oblasti spojené s riziky existují tři pojmy, které jsou jistým způsobem propojeny, a které nejsou v hovorové řeči a ve sdělovacích prostředcích obvykle rozlišovány. V odborné terminologii mají zcela vymezený a vysoce rozdílný význam. Jde o pojmy: nebezpečí, ohrožení a riziko.

Nebezpečí (angl. Danger) označuje stav lidského systému, při kterém vznik újmy, škody či ztráty na chráněných aktivech (zájmech) má vysokou pravděpodobnost (tj. je téměř jisté, že újma, škoda nebo ztráta vznikne) [5]. To znamená, že jde o označení možnosti vzniku újmy, ztráty či škody na jednom aktivu či více aktivech. Nebezpečí je určeno vlastnostmi látek, které se nachází v zařízení, objektu či území, anebo vlastnostmi procesů, které probíhají v zařízení, objektu či území. Je bezprostřední, když vývoj nezadržitelně směřuje k pohromě, a tím k vyvolání nouzové situace; a je plíživé, když vývoj směřuje k pohromě nenápadně a bez zřejmých příznaků [5]. Nebezpečí pro člověka znamenají jak velké jevy (např. živelní pohromy, průmyslové havárie, ekologické či sociální pohromy), tak zdánlivě malé jevy z denního života (pád tašky ze střechy, pád rampouchu nebo sněhu ze střechy, nerovný chodník apod.) [5]. Nebezpečí je míra stavu.

Ohrožení (angl. Hazard) vyjadřuje potenciál pohromy působit újmy, ztráty a škody na chráněných aktivech v daném místě, který je určený normativně. Jde o normativní míru nebezpečí, která je spojená s danou pohromou. Pro potřeby strategického plánování se nejčastěji počítá se stoletou pohromou, tj. ohrožení je velikost pohromy, která se vyskytne jedenkrát za sto let nebo přesněji má periodu návratu 100 let; u speciálních technických děl (přehrady, jaderné elektrárny, průmyslové komplexy s nebezpečnými technologiemi, mosty, tunely apod.) se pak z důvodu bezpečnosti zvažuje ohrožení jako velikost tisícileté či deseti tisícileté pohromy [1,5].

Riziko (angl. Risk) spojené s danou pohromou, činností či procesem je pravděpodobná velikost škod, ztrát a újmy na chráněných aktivech, které v daném místě vzniknou při výskytu pohromy mající velikost normativně stanoveného ohrožení, která je normovaná na stanovenou jednotku území či jednotku počtu jedinců a jednotku času [5]. Rozdíl mezi nebezpečím a rizikem spočívá v tom, že nebezpečí je určité (označuje aktuální stav) a riziko je jen očekávaná možnost.

Z výše uvedeného je zřejmé, že dominantním konceptem naší doby je riziko – jde nám o odvrácení ztrát a škod na chráněných aktivech, a to nejen okamžitých, ale i těch očekávaných v bližší nebo vzdálenější budoucnosti; a proto se často mluví o analýze rizik, řízení rizik, zvládání rizik, vnímání rizik atd. V předmětné oblasti panuje mezi sektory lidských činností dosud velká nejednotnost, která brání objektivnímu porovnávání míry rizika v prostoru i čase. Jedním z problémů je skutečnost, že v některých případech se zvažuje jen jeden chráněný zájem (jedno aktivum), tj. určuje se dílčí riziko, a v jiných případech se zvažuje více chráněných zájmů (aktiv) a určuje se integrované riziko (součet dílčích rizik) či integrální riziko (vycházející ze systémové podstaty entity, tj. rizika jsou spojená s prvky, vazbami a toky v systému) [5].

Protože chápání pojmu „riziko“ není dosud sjednocené, uvádíme příklady měr určitého rizika používané v praxi:

- hodnota pravděpodobnosti výskytu pohromy, s níž jsou spojeny ztráty, škody a újmy na jednom či více sledovaných aktivech,

- číslo z klasifikační škály 0 - 3, 0 - 5, 1 – 10, 1 - 100, kterou se ocení velikost dopadů pohromy, s níž jsou spojeny ztráty, škody a újmy na jednom či více sledovaných aktivech,
- očekávaný počet obětí při pohromě, s níž je spojeno riziko,
- očekávané poškození zdraví při pohromě, s níž je spojeno riziko,
- očekávaná výše škod při pohromě, s níž je spojeno riziko,
- očekávaný počet ztrát, škod a újmy při pohroma, níž je spojeno riziko,
- očekávaný počet ztrát, škod a újmy při pohromě, s níž je spojeno riziko rozpočtená na rok a územní jednotku.

Logické srovnání ukazuje, že výše uvedené míry nejsou vzájemně srovnatelné, což velmi omezuje výběr opatření a činností pro bezpečí a rozvoj lidí, tj. pro zajištění integrální (celkové, komplexní) bezpečnosti území, objektu a státu. Proto pro dosažení bezpečné lidské společnosti je třeba používat pojetí, které bylo uvedeno výše a je propojené se strategickým řízením a plánováním [2].

Další problém spočívá ve skutečnosti, že riziko neexistuje samo o sobě, je vždy vyjádřením vztahu mezi dvěma a více veličinami jako jsou četnost, aktiva, hrozba, ohrožení, zranitelnost, závažnost, dopady, důsledky, kapacity, protiopatření, závažnost a možnost výskytu (kvalitativní odhad) [5], viz příklady:

- R = četnost ∗ důsledky,
- R = závažnost ∗ možnost výskytu,
- R = ohrožení (hrozba) ∗ zranitelnost,
- R = ohrožení (hrozba) ∗ zranitelnost ∗ dopady,
- R = ohrožení (hrozba) ∗ zranitelnost / kapacity,
- R = (ohrožení (hrozba) ∗ zranitelnost) / protiopatření ∗ dopady,
- R = f (ohrožení (hrozba) ∗ zranitelnost / kapacity),
- R = f (aktiva (chráněný zájem)∗ ohrožení (hrozba) ∗ zranitelnost),
- R = četnost ∗ populace ∗ zranitelnost.

Výše uvedené skutečnosti ukazují, že v chápání rizika pozorujeme mnoho rozdílů a společné je jen to, že riziko vychází z obav z nejisté budoucnosti. Proto se riziko chápe v laické veřejnosti jako: nežádoucí událost; výskyt nežádoucí události; příčina nežádoucí události; statistické očekávání nežádoucí události; šance, že se nežádoucí událost vyskytne; možnost újmy, ztrát na životech, zranění nebo škod; pravděpodobnost výskytu nežádoucí události; úroveň nebo míra nežádoucí události; vystavení chráněného zájmu nebezpečí atd. Souhrnně lze říci, že riziko je možné nebezpečí (tj. možný stav vzniku újmy) pro chráněné zájmy (aktiva) a důraz je na slovo „možné“, kdežto samotný výraz „nebezpečí“ označuje jistou aktuální újmu pro chráněné zájmy. Diskusi různých definic rizika lze najít v mnoha pracích; mnohé z nich jsou citovány v [5]. Závěrem lze říci, že:

- v závislosti na kontextové situaci riziko může znamenat: možnost zdravotní, psychické, ekologické, fyzické nebo ekonomické ztráty; pravděpodobnost vzniku takové ztráty; možné nebezpečí, popř. možnou situaci, která zvyšuje četnost a závažnost ztrát; možný zdroj nebezpečí; možný hmotný statek nebo možnou osobu vystavenou ztrátě; možné odchylky od očekávaných ztrát; možnou pravděpodobnost, že se skutečná hodnota ztrát odchýlí od očekávaných hodnot; možné psychologické nejistoty vztahující se ke ztrátám; a možnou hodnotu ztráty v měnových nebo jiných jednotkách,
- riziko je možnost, že na definovaných chráněných zájmech se vyskytnou škody, ztráty a újmy.

Proto pro sestavení jednotného pojetí rizika, které je obsaženo v jeho úvodní definici, musíme zavést určitou úmluvu, která spočívá v tom, že označíme každý škodlivý jev, který narušuje bezpečí a udržitelný rozvoj sledovaného systému a vzniká vně nebo uvnitř sledovaného systému, pohromou. Do pohrom započítáváme i chování a jednání lidí, která vedou k organizačním haváriím. Ohrožení je míra schopnosti (potenciálu) pohromy narušit

bezpečí a udržitelný rozvoj sledovaného systému. Riziko je míra očekávaných ztrát, škod a újmy na chráněných aktivech přepočtená na jednotku území a jednotku času. Pro potřeby strategického řízení se určuje riziko místa / objektu / území pro jednu pohromu nebo pro soubor všech pohrom, které se mohou vyskytnout ve sledovaném místě / objektu / území. Riziko tudíž de facto předurčuje krutost nouzové situace, kterou daná pohroma může vyvolat.

Riziko je místně specifické a určuje se z velikostí místních ohrožení, která vytváří možné pohromy v daném místě s ohledem na míry zranitelnosti místa vůči konkrétním možným pohromám. Z uvedených skutečností vyplývá, že pro kvalifikované řízení území či jiného subjektu je důležité znát riziko, a to v pochopitelném vyjádření. V praxi veřejné správy se osvědčilo vyjádření rizika ve formě údaje, že na základě analýzy a hodnocení rizik v území bylo zjištěno, že na specifikovaném úseku:

- je třeba 5 miliónů každý rok na nápravu škod, způsobených existujícím rizikem,
- každých 10 let zemře 10 lidí v důsledku sledované pohromy,
- každých 5 let škody na majetku způsobené pohromou přesáhnou 5 miliard.

Z právě uvedeného vyplývá, že abychom určili riziko, musíme pochopitelně nejdříve znát velikost ohrožení pro každou pohromu, která je důležitá pro bezpečné území a bezpečnou lidskou společnost a pak zranitelnosti území vůči každé vybrané pohromě, která je předmětem našeho zájmu. Proto postupy pro stanovení velikosti rizik respektují jak podstatu jevů, které jsou jejich zdrojem (tj. charakteristiky a fyzikální podstaty pohrom), tak parametry prostředí, ve kterém se jevy vyskytují. Pro určení ohrožení se používají jak metody založené na matematické statistice, mlhavých množinách, přístupech operační analýzy apod., které inherentně předpokládají určitý model výskytu jevů, tj. nepřipouštějí, že tyto jevy jsou mimořádné, tak i metody založené na scénářích dopadů pohrom simulovaných nebo empirických, viz údaje shrnuté např. v pracích [1,2,5].

Při úvahách v praxi zvažujeme buď jednoduchý případ, a to průběh realizace rizika probíhá stále stejným způsobem, anebo složitější případ, který zvažuje dynamiku vývoje, dle které průběh realizace rizika je proměnný, a to jak v závislosti na změnách parametrů pohrom, tak i v závislosti na momentálních místních a časových podmínkách chráněných aktiv. V prvním případě určujeme jakousi střední hodnotu a její oprávněnost pro použití v praxi spojujeme s podmínkou, že je zvážen nejméně příznivý případ (nacházíme ho v normách a standardech založených na deterministickém přístupu). Druhý přístup odpovídá více skutečnosti, a proto se zvažuje při přípravě všech podkladů pro strategické řízení - určují se variantní scénáře realizace rizika a pravděpodobnosti jejich výskytu; a z nich se jasným matematickým přístupem určuje střední hodnota a její rozptyl (nacházíme ho v normách a standardech založených na pravděpodobnostním přístupu) [5]. Druhý případ se používá v souvislosti s výstavbou kritických objektů (pozn. kritický objekt je objekt, který je zároveň velmi důležitý a velmi zranitelný) [11]. Cílem řízení a vypořádání rizik v daném případě je zajistit, aby nebezpečí spojená s realizací rizika byla přijatelná.

Záměna sledovaných pojmů působí velký zmatek ve společnosti; např. občané a mnohdy i odborníci si neuvědomují, že: pojišťovny zohledňují rizika a ne nebezpečí; riziko označuje normativně určenou velikost ztrát a škod v daném místě či objektu; ohrožení vyjadřuje ztráty a škody, které způsobí pohroma o určité velikosti v daném místě či objektu; a nebezpečí naproti tomu označuje bezprostřední ztráty a škody, které nastanou v daném místě, když se blíží nebo vznikne jistá pohroma.

2.3. Přijatelné riziko

Riziko je nyní dominantním konceptem v naší společnosti. Je spojeno se složitými podmínkami nebo faktory jako jsou: nejistá přírodní ohrožení; nejistoty, které zahrnují věda a

technologie a jejich působení na zdraví a kvalitu života; zranitelnost lidí a nedostatek konzistentního vysvětlení životních strastí a jejich významu; a také lidské hry se strachem, šancemi a možnostmi.

Přijatelná úroveň rizika je subjektivní. U známých a častých pohrom je lidmi vnímaná úroveň rizika blízká skutečné míře rizika. U málo častých a málo známých pohrom je lidmi vnímaná úroveň rizika jako neskutečná a vzdálená. Vnímání rizika ovlivňují i jiné faktory – např. u činností, které děláme dobrovolně (horolezectví, skoky na lyžích apod.), předpokládáme, že úroveň rizika je zanedbatelná. Přijatelnost rizika ve skutečnosti je výsledkem porovnávání několika typů přijatelnosti – technická přijatelnost (spolehlivost a složitost technologií, strojů a zařízení), ekonomická přijatelnost (náklady) a socio-politická přijatelnost (vnímání rizik).

Obecně lze tvrdit, že přijatelné riziko se stanovuje na sociálním a znalostním základě a přitom se zvažují sociální, ekonomické a politické faktory. To mimo jiné znamená, že úroveň přijatelného rizika pro bohaté země či entity je vyšší než pro chudé, protože redukce rizika něco stojí. Proto také platí, že přijatelná úroveň neznamená bezpečnou úroveň rizika, tj. že pravděpodobnost vzniku ztrát, škod a újmy na chráněných aktivech je malá až zanedbatelná.

2.4. Práce s riziky

Historie odhadu rizika je velmi dlouhá a srovnatelná s historií bankovnictví a pojišťovnictví. Např. bez znalosti rizika nelze pojišťovat, nelze poskytovat úvěry, bankovní záruky a jiné finanční služby. Pro posuzování rizik byl vyvinut bezpočet pomocných pracovních pomůcek, metodických návodů, uživatelských příruček a software. Jejich struktura je značně vertikálně a horizontálně diferencována a vyčerpávající klasifikace je obtížná.

Na základě současných znalostí jsou rizika pro potřeby řízení bezpečnosti území, objektu či lidské komunity [1,2,5] stanovena správně a mají zřejmou vypovídací hodnotu, jestliže jsou stanovena:

- s ohledem na všechna definovaná chráněná aktiva (zájmy),
- definovaným postupem,
- na základě kvalifikovaného datového souboru se stanovenou vypovídací hodnotou a hranicí homogenity,
- na základě kvalifikovaného zpracování kvalifikovaného souboru dat pro dané zadání.

Rizika se liší podle toho:

- jaká jsou zvolena chráněná aktiva, zda je sledován jeden chráněný zájem (a pak jde o dílčí riziko), anebo soubor chráněných zájmů (a pak jde o integrované nebo integrální / komplexní riziko),
- jaké pohromy, tj. zdroje rizik se berou v úvahu. Pro některé úlohy postačuje omezený počet pohrom, např. jen těch, které mohou mít nepřijatelné dopady ve sledovaném prostoru třeba dvakrát za sto let apod.

Integrované a integrální riziko se liší přístupem stanovení. Integrované riziko je agregace dílčích rizik (součet, vážený součet aj.) pro zvažovaná chráněná aktiva. Integrální riziko je určené systémovým přístupem, při kterém jsou zváženy vlivy vazeb a toků mezi chráněnými aktivy [5], a proto se mu říká systémové.

Dílčí rizika jsou rozmanitá, např. zdravotní rizika, technologická rizika, riziko požáru atd. Pro výpočet dílčích rizik již existuje řada právních předpisů, norem a standardů a s nimi souvisejících podpůrných software. Např. dílčí rizika, která se musí zohlednit, při žádosti o projekty EU, anebo pro zajištění úspěšnosti projektů PPP (Public Private Partnership), se dělí do sedmi skupin [5]:

1. Bezpečnostní rizika spojená s chováním a činností lidí.

2. Stavebně-technologická a projekční rizika.
3. Kreditní rizika.
4. Tržní rizika.
5. Vnější rizika spojená s přírodními pohromami.
6. Provozní rizika.
7. Rizika spojená s řízením a rozhodováním.

Každá základní skupina dílčích rizik se dále dělí na další dílčí rizika [5]. Výběr z těchto rizik pro konkrétní případ se provádí podle formulace problému a podle stanovených cílů, které jsou v daném případě sledovány, a podle pohrom, které se zvažují jako zdroje rizik. Jestliže předmětem sledování je subsystém krajiny a lidských sídel, je nutno určit chráněné zájmy tohoto subsystému a jako pohromy zvážit všechny jevy, které v subsystému působí nebo mohou působit nepřijatelné dopady, tj. kromě známých živelních a jiných pohrom je třeba zahrnout i interakce vyvolané činnostmi lidí, a to i způsobem zajišťování správy území.

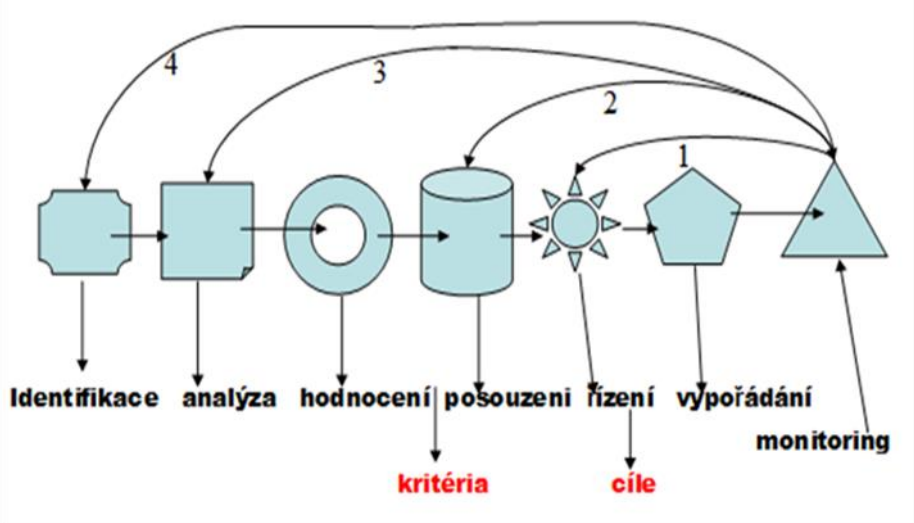
Jelikož cílem předmětné publikace jsou technická díla, tak nám jde o nalezení takového řízení rizik procesů, které jsou důležité pro zajištění bezpečí technického díla i jeho okolí.

Zatímco postupy pro hodnocení ohrožení jsou obecné [5], tak postupy pro určení rizik jsou místně specifické, protože u nich hraje zásadní roli místní zranitelnost. Pro úkoly praxe se pak používá několik úrovní analýzy rizik [5], a to:

A – předběžná analýza rizika,
B – standardní, rychlá a méně přesná analýza rizika,
C – detailní analýza rizika v souhrnném kontextu,
D – individuální a specifická analýza rizika.

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

Koncept práce s riziky, tj. procesní model je zobrazen na obrázku 3. Další modely jsou uvedeny v práci [5], popř. v pracích, které jsou v předmětné práci citovány.



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

Podle úvah současných filosofů, rizika ve společnosti mají svoji objektivní i subjektivní stránku, navíc nestojí mimo kulturní a hodnotové souvislosti (nejsou v tomto směru ani „čistě vědeckým“ problémem a zasluhují pozornost i z hlediska občanské participace). I když moderní společnost uplatňuje onu pohodlnou strategii pojištění a odškodnění, nelze na ni plně spoléhat,

neboť některá rizika jsou schopna zasáhnout podstatu sociálního systému, což platí pro některá rizika bezpečnostní. Proti „zvědečtění bezpečnostní politiky“ nelze nic namítnout, pokud dokážeme být reflexivní, což znamená především odhadovat důsledky jednotlivých aktů a nepodléhat iluzi o možnosti „dokonalého řešení“. Spoléhání veřejnosti na experty (a vědecké instituce) může přivodit oslabení schopnosti podílet se aktivně na řešení problémů a dokonat tak odtržení privátního a veřejného (což se pak projeví jako inherentní riziko, na kterém expertíza ztroskotá). Podle odborných koncepcí při vypořádání s riziky mají dle svých možností povinnosti a odpovědnosti všichni zúčastnění (tj. všechny zájmové skupiny).

Lidé proto mají mít možnost zúčastnit se rozhodování o vypořádání rizik, projevit své potřeby a názory, a to bez obavy z postihů. Obvykle je snaha o zapojení co největšího počtu lidí (i za cenu zvýšených nákladů na počátku procesu), dosahování konsensu a shody. Je to také respektování odlišných názorů a vyjasňování pozic a záměrů různých skupin i jednotlivců. Jestliže zapojujeme do procesu rozhodování veřejnost tak zapojujeme všechny zúčastněné, podle jiných materiálů tzv. podílníky (stakeholders) nebo také dotčené osoby a skupiny. Podílníkem je ten (jedinec, skupina, organizace), kdo může ovlivnit nebo kdo může být ovlivněn (pozitivně i negativně) výsledkem rozhodnutí, plánu, programu nebo i procesem, který k výsledku vede.

Problém nastává v odborných záležitostech, ve kterých podklady pro rozhodování jsou založené na hodnoceních, která jsou složitá a pro řadu normálních občanů nepochopitelná. Situace v těchto případech je proto často válkou lobbistů různých skupin, které usilují o zakázku. Proto je třeba, aby se postupy hodnocení opíraly o legislativu a aby kritéria výběru konkrétních řešení byla zaměřena na veřejně prospěšné cíle (tj. veřejný zájem), umožňovala transparentnost rozhodování při výběru správného řešení s ohledem na zdroje, síly a prostředky veřejné správy, které má k dispozici.

2.5. Poznatky pro řízení rizik zacílené na bezpečný systém

Jelikož lidé si přejí žít v bezpečí a mít zajištěn potenciál pro rozvoj, tak strategické řízení každého státu, území či objektu (tj. i technického díla) se musí zaměřit na dlouhodobou udržitelnost, a na základě poznání provádět zacílenou prací s riziky všeho druhu. Protože doposud neexistuje obecná shoda na formulaci problémů udržitelnosti veřejného blaha (blahobytu) lidské společnosti v kontextu se systémovými službami, je každé dosavadní řešení dočasné, jelikož se neustále balancuje mezi konkurujícími si zájmy a společenskými cíli (jsou-li stanoveny). Je obtížné řešit problémy rozhodování jednoznačně vzhledem k měnícímu se charakteru rozhodovacího procesu [2]. V rozhodování se řeší dále uvedená dilemata:

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

Je obtížné řešit inverzní problémy pro složitost systémů. Zkušenosti ukazují, že když se stanoví a utřídí nějaké příznaky spojené s riziky, vynoří se příznaky nové. Z toho vyplývá, že praktický přístup k řízení udržitelnosti musí být iterační, interaktivní a adaptivní [2,5]. To znamená, že žádná opatření řízení a vypořádání rizik nejsou trvalá, ale jen dočasná, a proto lidé, a zvláště vytvářené řídicí systémy lidské společnosti, musí podmínky monitorovat a antropogenní opatření činnosti a opatření přizpůsobovat situaci.

Cílem strategického, tj. komplexního řízení je za každé situace zajistit ochranu životů, zdraví a bezpečí lidí, majetku, životního prostředí, infrastruktur a technologií, které jsou nezbytné pro přežití lidí, tj. vždy mít schopnost zajistit mobilizaci a koordinaci využití zdrojů (energie, pracovní síla, výrobní schopnosti, jídlo a zemědělství, suroviny, telekomunikace aj.),

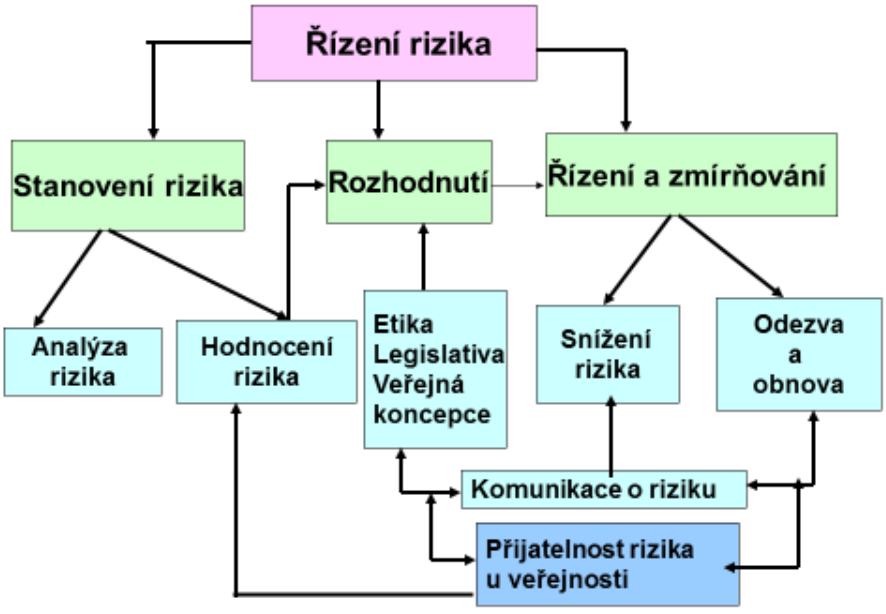
koordinaci činností takových, jako je systém vyrozumění, systém záchrany a zdravotnické služby, které snižují dopady pohrom a také kontinuitu činnosti státní správy a dodržování zákonů. Typy plánování tvořící základní metodické nástroje jednotlivých vzájemně provázaných typů řízení musí vytvářet základnu, ve které jsou výše uvedené cíle zakotvené [2,5].

Pro cíle lidské společnosti, tj. především pro její bezpečí a udržitelný rozvoj je nutno vzájemně kombinovat opatření a činnosti na snižování zranitelnosti, na zvyšování pružné odolnosti (resilience) a schopnosti adaptace, které respektují všechna základní chráněná aktiva (veřejná i podniková) v jednotlivostech i celku. Současným nástrojem založeným na znalostech a zkušenostech je na všech úrovních řízení implementovat proaktivní systém řízení bezpečnosti, ve kterém se upraví práce s riziky do takové formy, která respektuje všechna chráněná aktiva a bere v úvahu existující a prokázané vnitřní závislosti. S ohledem na současné poznání je třeba provádět a sledovat výzkum vnitřních závislostí, které zprostředkovávají sekundární a další dopady pohrom na životy, zdraví a bezpečí lidí [1,2].

Na základě současného poznání a zkušeností musí být svět chápán systémově a pro zajištění bezpečí a rozvoje lidí musí lidská uskupení, tj. obce, kraje, státy a společenství států dobře pracovat s riziky. Pro práci s riziky je třeba zvažovat:

- koncept světa v systémovém pojetí,
- pojmy důležité pro chápání a řízení bezpečnosti,
- zdroje rizik a chápat jejich dopady na chráněná aktiva,
- metody pro hodnocení a posuzování rizik,
- způsoby řízení rizik,
- způsoby inženýrského vypořádání rizik,
- způsoby práce s riziky v čase.

Jak již bylo řečeno, rizik však existuje velké množství, protože jejich zdrojů je velké množství. Navíc rizika stále přibývají a lidská společnost nemá zdroje, síly a prostředky, aby tomu zabránila, tak musí cíleně řídit rizika. Aby řízení bylo úspěšné, tak se musí zaměřit na prioritní rizika a jejich aspekty [5]. Řízení rizik entit není záležitosti, ani jednotlivce, ani jednoho sektoru, jak ukazuje obrázek 4. Předmětný obrázek ukazuje základní strukturu řízení rizik, další členění je v práci [5]. Ze základní struktury je zřejmé, že:



Obr. 4. Základní rámec pro řízení rizik.

- stanovit riziko mohou odborníci, kteří mají znalosti, data a schopnost aplikovat vhodné metody,
- rozhodnout o riziku mohou jen ti, co mají příslušné oprávnění (tj. právně určený subjekt veřejné správy nebo v případě objektu (tj. technického díla) právně určený subjekt podniku, jemuž entita patří,
- řízení a zmírňování, tj. vlastní aplikace opatření a činností vedoucí ke zvládnutí rizika mohou jen odborníci, kteří mají příslušné znalosti, schopnosti, vybavení, zdroje a prostředky.

O roli veřejnosti je pojednáno na jiném místě; jisté je, že je by měla být platným účastníkem při vypořádání rizik, protože jde o její bezpečí a kvalitu života.

Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá v rozdělení opatření a činností na vypořádání rizik do kategorií, ve kterých se příslušná část rizika zajistí tak, že:

- preventivními opatřeními se sníží nebo odvrátí realizace rizika,
- účelovými preventivními opatřeními odezvy a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se zmírní dopady, tj. sníží nebo odvrátí se nepřijatelné dopady při realizaci rizika,
- provedeme pojištění na krytí možných ztrát a škod při realizaci rizika,
- připravíme rezervy na odezvu a obnovu a zálohy pro zajištění přežití lidí a kontinuitu provozu území, objektu či organizace,
- připravíme plán pro odezvu na nepředvídané situace (Contingency Plan) pro případ realizace rizik neřiditelných nebo příliš nákladných, anebo málo častých.

K tomu se rovněž připojuje rozdělení zvládání rizik mezi všechny zúčastněné [1,2,5]. Rozdělení provedení konkrétních opatření a činností ve správném řízení se provádí tak, že se vychází z toho, že za zvládání rizik odpovídají všichni zúčastnění a že zvládání konkrétního rizika je nejlépe přidělit tomu subjektu, který je na to nejlépe připraven [5]. Je zřejmé, že toto je však možné jen v organizaci, ve které je kvalifikované projektové a procesní řízení, tj. činnosti a opatření se aplikují na základě znalostí, a to věcných i z oblasti řízení (tj. činnosti jsou vzájemně provázané, nejsou chyby v komunikaci, každý zúčastněný ví, co má dělat a jak to má dělat) [5].

2.6. Koncepty řízení a vypořádání rizik zacílené na bezpečná technická díla a bezpečí lidí

Při práci s riziky s cílem zajistit bezpečí a rozvoj lidí je třeba dle současného poznání shrnutého v pracích [1,2,5,10] zvažovat řadu aspektů:

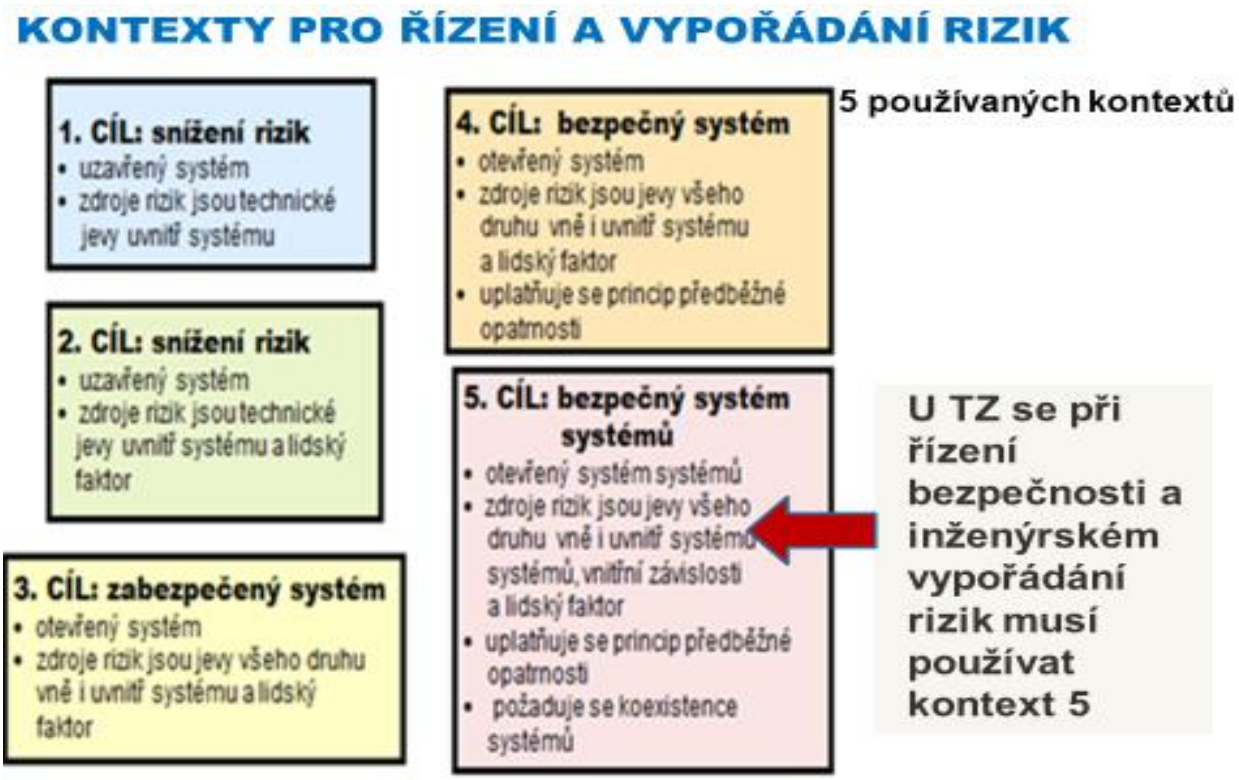
1. Vnímání reality. Je buď mechanistické, nebo systémové. Pro řešení současných problémů je nutné systémové pojetí [1,5,10]. V současné praxi se při řešení konkrétních problémů používají modely reality předpokládající: uzavřený systém; otevřený systém; soubor několika otevřených systémů; systém systémů [1,10].
2. Pojetí zdrojů rizik. Rozlišujeme případy, ve kterých zdroji rizik, tj. pohromami jsou: jen vnitřní jevy technického původu v systému; jen vnitřní jevy technického původu v systému a lidský faktor; vnitřní a vnější jevy a lidský faktor; vnitřní a vnější jevy, lidský faktor a tzv. interdependences, tj. indukovaná škodlivá propojení a škodlivé toky v systému a v propojení systému s okolím; a vnitřní a vnější jevy, lidský faktor a tzv. interdependences, tj. indukovaná škodlivá propojení a škodlivé toky v systému systémů a v jeho propojení s okolím.
3. Systematická práce s riziky zacílená na jejich redukci je doložena od 30. let minulého století. Na základě kritického vyhodnocení současných poznatků, jehož výsledky jsou

shrnuty v pracích [1,2,5,10,11], rozlišujeme pět konceptů, ze kterých vycházíme při vyjednávání s riziky, a to: klasické řízení a inženýrství rizika; klasické řízení a inženýrství rizika zahrnující lidský faktor; řízení a inženýrství zaměřené na bezpečí (zabezpečovací řízení a inženýrství); řízení a inženýrství zaměřené na bezpečnost, tj. takové ovládání a vypořádání rizika, které zajistí jak zabezpečený systém, tak jeho bezpečné okolí; a řízení a inženýrství zaměřené na bezpečnost systému systémů (SoS); obrázek 5. Charakteristiky konceptů a praktické aplikace jsou popsány v citovaných pracích a konkrétní výsledky jsou uloženy v archivu [12].

Z výsledků výzkumu [13], založeného na aplikaci teorie maximálního užitku, který se zabýval hodnocením míry kritičnosti konceptů současného řízení a vypořádání rizik objektů, vyplývá, že žádný z dnes používaných konceptů pro řízení a vypořádání rizik nemá zanedbatelnou míru kritičnosti; tj. míra kritičnosti při aplikaci: klasického konceptu řízení a inženýrského vypořádání rizik je extrémně vysoká; konceptu řízení a inženýrského vypořádání rizik zvažujícího lidský faktor, je velmi vysoká; konceptu řízení a inženýrského vypořádání rizik zaměřeného na zabezpečený systém je vysoká; konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém je střední; a konceptu řízení a inženýrského vypořádání rizik zaměřeného na bezpečný systém systémů je nízká. Uvedený výsledek také znamená, že ani nejpokrokovější koncept, kterým dnes je řízení bezpečnosti systému systémů, nezaručuje zanedbatelnou míru kritičnosti. Důvodem jsou rizika napříč systémů náležejících do systému systémů (SoS) a do propojení SoS s okolím, která nejsme schopni na základě současných znalostí a zkušeností předem všechna odhalit. Z výše uvedených faktů vyplývají základní principy pro práci a riziky, a to: být proaktivní; domýšlet možné důsledky; správně určovat priority z pohledu veřejného zájmu; myslet na zvládnutí nepřijatelných dopadů; zvažovat synergie; a být ostražitý, což odpovídá filosofii prosazované v práci [14]. Proto při stanovení rizika pro strategické rozhodování je nutno používat hierarchický multikriteriální postup; recentní odborné práce používají pojem hierarchické holografické modelování (HHM) [14]. Výsledky pak jsou vysoce kvalitní, protože zohledňují řadu faktorů, které jsou původci neurčitostí. Protože jde o postup náročný na data i zpracovatelské metody, tak se autorka domnívá, že by Rada vlády pro bezpečnostní výzkum měla dát prostředky na předmětnou problematiku odborníkům, kteří mají znalosti a schopnosti předmětné postupy do české praxe zavést.

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

   V případě výskytu kritických podmínek je třeba zvážit příčinu kritických podmínek, tj. odhalit přispěvatele k riziku, který způsobil kritické podmínky a absolvovat proces od počátku. Z obrázku 3 je zřejmá zásadní role monitoringu. V případě, že se zjistí, že riziko je nepřijatelné, je třeba provést změny, jak naznačují zpětné vazby na obrázku 3. 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.



Obr. 5. Koncepty řízení a inženýrského vypořádání rizik [10]; TZ = technologické zařízení.

Je třeba také poznamenat, že kritický je také výběr kvalitativního nebo kvantitativního přístupu při oceňování rizik, protože s kvantifikací rizika se musí zacházet obezřetně, jelikož výpočty rizika vytváří falešný pocit jistoty a bezpečí [5,10], Proto je třeba vždy porovnat pro a proti při použití kvantitativní a kvalitativní analýzy. Pokud se hovoří o kvantifikaci, je třeba zmínit a porovnat úrovně kvantifikace: verbální (velký, malý), ordinální (např. od 1 do 10), bodové hodnocení, intervalové hodnocení, výpočet pravděpodobnosti, výpočet na základě důkazů (Bayesův teorém).

Na základě dosavadních znalostí a zkušeností, shrnutých v práci [10], platí:

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

z prosté zásady: spíše měřit to, co je měřitelné, než to, co je důležité. Pokud důležité je současně měřitelné, tím lépe,

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

6. Orientace na kritické položky. Protože nikdy není dostatek zdrojů, sil a prostředků, tak se v inženýrské praxi orientujeme jen na kritické atributy, tj. jen na nepřijatelná a podmíněně přijatelná rizika [14] a ISO normy založené na projektovém řízení typu TQM (Total Quality Management), tj. ISO 9000, 14000, 18000 a 30000 (seznam vyhodnocených rizik; seznam rizik vyžadujících nejvyšší pozornost; seznam neaktuálních / vyřešených rizik).
7. Počet sledovaných aktiv. V praxi se používají modely: jedno aktivum; více aktiv, jejichž hodnotu lze vyjádřit jednou proměnnou, nejčastěji penězi; více nesouměřitelných aktiv – lidský systém [5,10]. Tj. zvažujeme buď dílčí riziko, anebo složené, které je buď integrované, anebo integrální. Integrované je definovaný součet dílčích rizik a nezahrnuje zpravidla vlivy vazeb a toků v systému. Integrální či komplexní vychází ze systémového pojetí reality, tj. zahrnuje i vlivy vazeb a prvků [5,10], což je případ lidského systému i složitých technologických objektů.
8. Závislost na místě. Riziko je místně specifické a určuje se z velikostí místních ohrožení, která vytváří možné pohromy v daném místě s ohledem na míry zranitelnosti místa a jeho aktiv vůči konkrétním možným pohromám.

V případě několika nesouměřitelných aktiv v otevřeném systému, je nutno použít multikriteriální přístup a hledat optimum [5,15]. Přitom je pravdou, že optimum pro systém s více nesouměřitelnými aktivy nemusí ležet těsně u optim pro jednotlivá aktiva. Specifikum manažerských a inženýrských metod, nástrojů a technik spočívá v tom, že od sebe nelze oddělit charakteristiky jevů, před kterými předmětný objekt musí být chráněn, vlastnosti materiálů, území konstrukcí a zařízení, které tvoří objekt, provozní podmínky a limity, detekci narušení objektů při překročení stanovených limitů a korekční opatření podporující bezpečnost objektu a jeho okolí. Protože jejich cílem je kvalitní řešení v daných podmínkách, musí kloubit exaktní výsledky s výsledky dobré inženýrské praxe, a to především znamená používat pouze ověřené postupy a ověřená data. Proto se v daných případech používají heuristiky, tj. techniky řešení problémů, pro které nemáme algoritmus nebo přesnější metodu. Vycházíme z odhadu, intuice a zkušenosti, a výsledkem je jedno z možných řešení problému (které nemusí být to nejlepší).

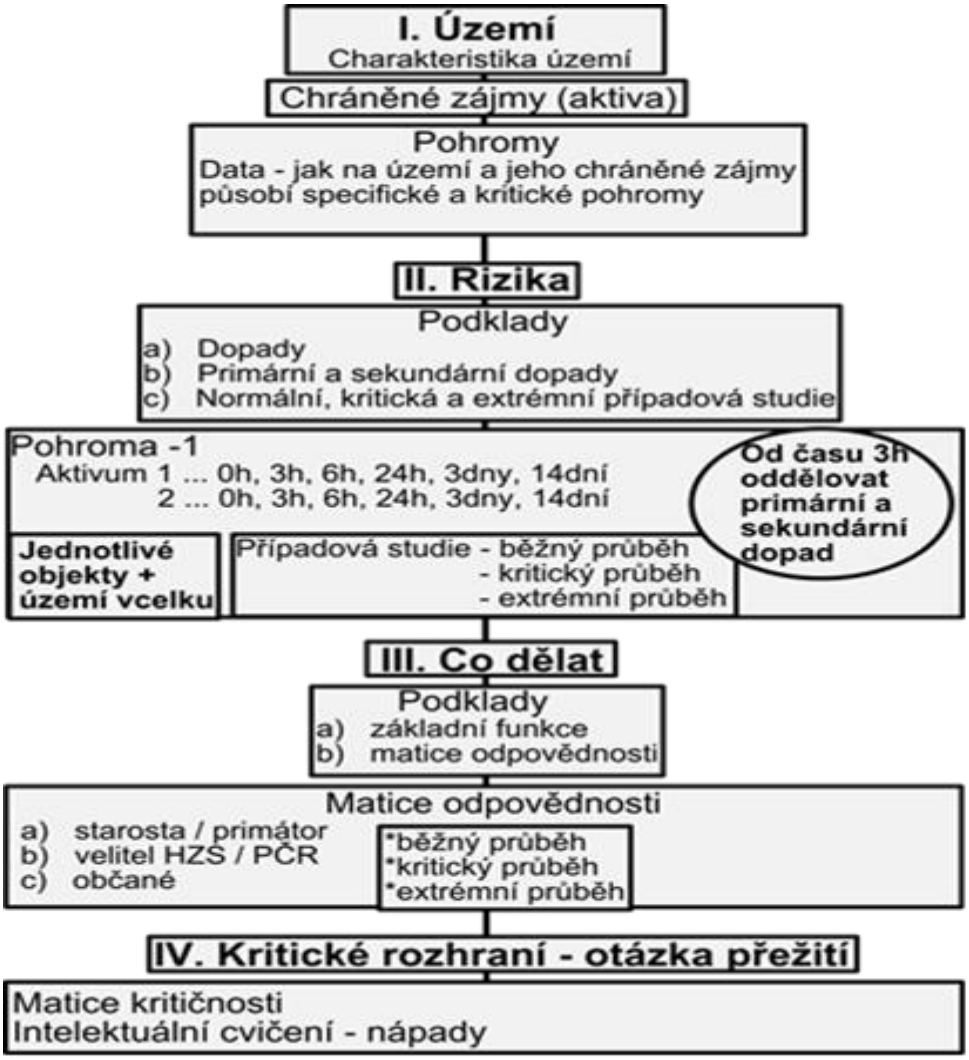
Vlastní inženýrské řešení a výběr metod, nástrojů a technik pro práci s riziky je určeno: počtem a charakterem sledovaných aktiv; volbou konceptu řešení problému; a fázi řízení – prevence, připravenost, odezva, obnova. Jelikož rizika mají různé zdroje, tj. závisí jak na pohromách, tak na místních zranitelnostech,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

- určit pohromy, které mohou systém postihnout a přitom respektovat All Hazard Approach [8] ve formě popsané v [7],
- možné pohromy rozdělit na relevantní, specifické a kritické [2,5,7], obrázek 2,
- aplikovat procesní model pro práci s riziky nebo jeho pokročilé modifikace, jejichž přehled je v práci [5], a určit, pro která rizika se budou dělat opatření a činnosti pro: prevenci; zmírnění; odezvu; obnovu; a která rizika zůstanou nezajištěná nebo jenom pojištěná [5,16],
- provést realizaci opatření a zajistit monitoring s důrazem na údržbu, opravy a včasnou aplikaci nápravných opatření [5].

Celkový postup, detailně popsaný v práci [10] je zobrazen na obrázku 6. Obrázek 6 ukazuje, že v první fázi se stanoví charakteristiky území a charakteristiky možných pohrom (v ČR pro oblast územního plánování existují jednotným způsobem zpracované územně analytické podklady obcí v grafické podobě, které jsou pro stát v archivu v Brně, a které lze použít pro běžné potřeby; pro kritické objekty je nutno dělat vlastní detailní průzkum a studie, protože předmětné podklady jsou příliš hrubé a nezohledňují všechny přispěvatele k celkovému riziku [11]); v druhé fázi se určí rizika na základě zvážení ohrožení, které představují možné pohromy dle možné velikosti, a zvážení místních zranitelností, a to území i veřejných aktiv; ve třetí fázi se zváží jednak účinnost aplikovaných preventivních, zmírňujících, reaktivních a obnovovacích opatření a činností, a jednak zajištění odpovědností a kvalita podpor pro kvalitní odezvu; ve čtvrté části se hledají způsoby řešení možných situací, které mají rysy, jež mohou ohrozit přežití lidí a nejsou řešeny v předchozích krocích. V případě vložení technologických objektů do území je právě v části III třeba řešit koexistenci objektu s územím, tj. provádět prevenci domino efektů a jiných dopadů, které mohou za jistých podmínek nastat (vzhledem k dynamickému vývoji světa jde o řízení rizik celé řady procesů).

První dva kroky postupu dle vyznačeného modelu na obrázku 6 se dělají pro každou pohromu odděleně. Ve třetím kroku se provádí hodnocení opatření a činností vůči jednotlivým pohromám a zvažuje se fakt, že některá opatření a činnosti jsou v reálném území konfliktní, a proto se provádí jejich optimalizace při zvážení všech možných pohrom do velikostí, kterou jsou hodnoty projektových pohrom. Vyžadují se doklady o zajištění odezvy, jejím materiálním, technickém, personálním a znalostním zajištění, a také průkaz příslušných kompetencí a odpovědností. Ve čtvrtém kroku se zvažují nadprojektové pohromy a závažnost jejich dopadů, identifikují se rozhraní pro vznik sociální krize a hledají se nápady pro zajištění přežití obyvatel území. Jelikož vyžadujeme, aby objekty, které lidé vytváří, byly bezpečné objekty, tak stejný postup platí i pro ně, tj. v části třetí musí prokázat, že i při svých kritických podmínkách objektů se provedou ochranná opatření, aby dopady předmětné pohromy zesílené selháním objektu na okolí byly přijatelné.

Procesní model zobrazený na obrázku 6, vyjadřující způsob zajištění bezpečného lidského systému, byl vyzkoušen v praxi specifickým šetřením, kterého se zúčastnilo 123 specialistů z 24 členských zemí EU pro: kategorie území - vesnické osídlení, městská zástavba, průmyslový region, zemědělský region, a zalesněné území s tím, že kategorie se určuje dle převládajícího charakteru daného území; a osm vybraných pohrom (povodeň, zemětřesení, ztráta kontroly nad nebezpečnými látkami, výpadek elektřiny, výpadek kybernetické infrastruktury, hromadné onemocnění, úmyslný útok na lidskou společnost, selhání vazeb v lidské společnosti) o velikosti podprojektové, projektové a nadprojektové, a osvědčil se [17,18]. Proto se rozšířil v části III vyznačené na obrázku 6 tak, že se do něho přidaly požadavky pro bezpečné složité objekty [1,12] a jeho výsledky se použily pro zvýšení odolnosti konkrétních objektů, a tím i bezpečnosti konkrétních složitých objektů.



Obr. 6. Postup práce s riziky zacílený na zajištění přežití lidí [10].

Základní nástroje pro zajištění bezpečí území, bezpečí technického díla i jejich dobré koexistence zajišťují specifické nástroje, kterými jsou bezpečnostní plán (strategický plán zacílený na rozvoj příslušné zvažované entity) a jeho dílčí plány jako jsou územní plán; nouzové plány, tj. plány odezvy na konkrétní pohromy; a krizové plány, tj. plány odezvy na extrémní pohromy [1,2,5,10,11], jejichž nedílnou součástí u technologických objektů a kritických infrastruktur jsou plány kontinuity, jejichž cílem je zajistit schopnost entity obnovit dostatečně rychle činnost technologického objektu, aby nedošlo ke ztrátě obslužnosti území, produktů, konkurenceschopnosti území, zaměstnanosti, které logicky vedou ke snížení rozvojového potenciálu daného území [1,10,11].

Pro posuzování rizik byl vyvinut bezpočet pomocných pracovních pomůcek, metodických návodů, uživatelských příruček a softwarů; seznam je v práci [5,15] a v pracích v nich citovaných. Odpovídají na otázky:

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

Postupy pro určení rizika vychází ze vztahu $\boldsymbol{R = H \times V}$, tj. závisí na určení ohrožení $\boldsymbol{H}$ (Hazard) a zranitelnosti $\boldsymbol{V}$ (vulnerability); u teroristických útoků tam ještě přibývá úmysl útočníka $\boldsymbol{I}$ (tj. $\boldsymbol{R = H \times V \times I}$). Při určování ohrožení používáme jednoduché odhady, výpočty založené na scénářích pohrom a také velmi náročné postupy založené na teorii extrémních hodnot a na různých modelech entity: lineární (liniové); stromové; síťové; a vícekriteriální, pro něž vytváříme systémy pro podporu rozhodování [5,15]. Důležité je jakou hodnotu ohrožení určujeme, používá se: střední, očekávaná na nějaké úrovni četnosti výskytu; a maximální možná. Je zřejmé, že při zvážení různých hodnot zajistíme jinou úroveň ochrany sledované entity, tj. území nebo technického díla.

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

Pro potřeby strategického rozhodování lze v zásadě rozdělit dva základní přístupy, a to:

1. Určení ohrožení od pohromy $\boldsymbol{H}$ a periody návratu $\boldsymbol{\tau}$ (v rocích) metodami založenými na teorii velkých čísel, teorii extrémů, teorii mlhavých množin, teorii chaosu, teorii fraktálů apod. Podle místní zranitelnosti chráněných aktiv v definovaném území (např. čtverec 10 x 10 km; kružnice o poloměru 5 km) stanovíme celkovou škodu pro ohrožení $\boldsymbol{H}$ (v penězích) označenou $\boldsymbol{S}$. Riziko $\boldsymbol{R}$ je pak dané vztahem:

   $$\boldsymbol{R = S * \tau^{-1}.}$$

2. Určení scénáře pohromy o velikosti největší očekávané pohromy (lze podle požadavků normativu použít pravděpodobnou velikost očekávané pohromy nebo hodnotu normativně stanovené pohromy nebo nejméně příznivé pohromy) a dle dat pro dané území určit:
   - podle chráněných aktiv a jejich zranitelnosti vůči dopadům ve scénáři pohromy celkovou škodu zasaženého území (v penězích) $\boldsymbol{S}$,
   - podle odborných údajů z databází nebo expertních odhadů určit četnost výskytu největší očekávané pohromy $\boldsymbol{f}$ normovanou na 1 rok.

   Riziko $\boldsymbol{R}$ je pak dané vztahem:

   $$\boldsymbol{R = S * f.}$$

Je logické, že abychom mohli s rizikem vyjednávat, tak ho musíme identifikovat, analyzovat, ocenit a pochopit v souvislostech. Proto ohodnocení dopadů pohrom v konkrétním území je základní součástí jakéhokoliv pokusu o kvantifikaci a hodnocení rizika. Hodnocení rizika je strukturovaná procedura, která se pokouší odpovědět na dále uvedené otázky:

- jaké ztráty, škody a újmy budou na chráněných aktivech?
- jak často se to stane?
- jak zareagují bezpečnostní systémy v území či jiné sledované entitě?
- jaké ztráty, škody a újmy budou na chráněných aktivech, když selžou bezpečnostní systémy v území či jiné sledované entitě?

Aby hodnoty rizika měly jasnou vypovídací hodnotu, tak je důležité mít nejenom nástroj, ale také jasně definovanou hodnotovou stupnici jak pro klasifikaci dílčích položek, tak pro souhrn položek. Poznámka: nejčastější chyba v českých poměrech je, že se nedefinuje stupnice nebo se použije vágní stupnice, tj. veškeré údaje o riziku jsou subjektivní (nejen v archivu [12], ale i v řadě publikací je řada příkladů, kdy stupnice není definovaná).

V práci [5] jsou uvedeny přesné postupy a též příklad postupu pro stanovení rizika při pohromě v určitém území, který je nejčastěji používán v normách. Z důvodu porozumění uvedeme chápání dvou pojmů. Řízení rizik chápeme jako proces určení opatření a činností vedoucích k ochraně před riziky; člověk ho prováděl od samého počátku uvědomělého konání. Inženýrství (inženýring) rizika chápeme jako realizaci opatření a činností pro vypořádání rizik způsobem stanoveným řízením rizik, dle disponibilních možností a dle podmínek v místě řešení. Úkolem řízení rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Úkolem inženýrství rizika je opatření realizovat a zajistit jejich spolehlivost a funkčnost.

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

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

Dosažení cíle znamená dobře řídit a správně rozhodovat, přičemž dobré řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici [2,5]. Poznámka: nejčastější chyba v českých poměrech – neprověřuje se kvalita datových souborů a vzájemný vztah mezi přesností dat a citlivostí metody [12].

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

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

1. Pro koho má být riziko přijatelné?; pro původce rizika, pro politiky nebo pro veřejnou správu?
2. Kdo stanoví přijatelnost?; politici rozhodují o tom, co je zákonné, a tudíž by neměli rozhodovat o tom, co je přijatelné,
3. Zda při stanovení přijatelnosti rizik byla diskutována aktuálně tolerovatelná rizika, netolerovatelné prahové hodnoty a postoje veřejnosti k rizikům.

Rizika byla, jsou a budou a neustále se budou objevovat nová. Řízení rizika, které způsobují pohromy, vyžaduje rozměr a měření rizika, které berou v úvahu nejen fyzické škody, oběti a ekvivalent ekonomických ztrát, ale i sociální, organizační a institucionální faktory. Řada současných technik na určování rizika nereprezentuje holistický přístup a většina z nich nezvažuje vazby a toky mezi prvky systému za zranitelné položky, které zvyšují škody, ztráty a újmy. Je si třeba uvědomit, že riziko je rozdělené na lokální, regionální i státní úroveň [5].

Je zřejmé, že nejsme-li schopni riziko identifikovat a analyzovat, nejsme schopni se proti němu účinně bránit. Chyba, které se dopustíme při analýze rizika, se přenáší do nouzových a krizových plánů, do plánů kontinuity a snižuje jejich hodnotu ve vztahu k plánovaným opatřením směřujícím především k ochraně lidských životů a zdraví, ale i v oblasti akceschopnosti záchranných složek podílejících se na realizaci záchranných operací. Na závěr

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

2.7. Oblasti vyžadující opatření pro zvládnutí rizik primárně ohrožujících lidi

Výsledky projektu FOCUS [7], řešeného v rámci EU odhalily velmi mnoho slabých míst spojených s vypořádáním rizik, a to právě i v oblastech, které bezprostředně souvisí s bezpečnostními a zdravotními riziky a významně ovlivňují ostatní veřejná aktiva [6,7,19]. V dané souvislosti byly zjištěny závažné nedostatky v řízení jevů jako: zneužití moci; rozpad společnosti na netolerantní skupiny; zneužití technologií; zneužití pravomoci; nelegální vstupy do informačních systémů; kybernetická kriminalita; teroristické útoky; korupce ve vládě a veřejné správě včetně politické sféry; závažná ekonomická kriminalita zahrnující praní špinavých peněz a daňové úniky; obchodování s lidmi a ilegální migrace; ilegální výroba a distribuce psychotropních látek; extremismus; všechny formy diskriminace a netolerance; zneužití genového inženýrství.

Výsledky výzkumu v EU, uvedené v práci [7], ukazují, že je třeba věnovat značné úsilí např.:

- možnému selhání péče o lidi, které zprostředkovaně dříve či později dolehne na provoz technologických objektů. Jde např. o selhání zdravotnické a sociální péče, protože chybí systematické řešení problémů: mladých lidí (zaměstnanost a uplatnění ve společnosti); seniorů; skupin lidí, kteří nejsou ochotni se podřídit pravidlům většinové společnosti; a přípravě na velké pandemie a epidemie, a nevyléčitelné nemoci u lidí, zvířat nebo rostlin,
- defektům, které vyvolává zvyšování fyzické zranitelnosti lidí velkým tlakem na pracovní výkony lidí,
- defektům v chování lidí, které nabývají velkých rozměrů, tj. vzájemné nepatřičné chování jednotlivce nebo skupin jednotlivců jako jsou: neoprávněné přivlastňování majetku; usmrcení lidského jedince; šikana; náboženská a jiná nesnášenlivost; kriminální činy jako: vandalismus a protizákonné podnikání, loupeže a přepadání, nelegální vstupy, neoprávněné použití majetku či služeb, krádeže a podvody, zastrašování a vydírání, ničení a sabotáže, teror vůči jednotlivci; teroristické útoky; lokální a další ozbrojené konflikty,
- neřízené populační explozi lidí – v EU se řeší jen demografický šok a odhad časového horizontu jistého bodu zvratu, tzn. začátek absolutního poklesu obyvatelstva Evropy a ČR,
- ilegální migraci velkých skupin lidí – je třeba řešit otázky spojené se zajištěním pitné vody a potravin a problémy zapojení lidí z jiných kultur do pracovního procesu, ve kterém se tvoří hodnoty a též bezpečnostnímu rozměru imigrace,
- defektům způsobeným nedokonalostmi v řízení lidských činností jako jsou: selhání vzdělávací infrastruktury; selhání infrastruktury výzkumu; selhání veřejné správy; selhání dodavatelských řetězců.

Příčiny uvedených nedostatků v oblasti vrcholového řízení byly identifikovány takto:

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

2.8. Řízení rizik zacílené na bezpečné systémy

Při zajišťování bezpečnosti kritických objektů rozlišujeme v praxi podle cíle práce s riziky dva koncepty, a to řízení rizik a řízení bezpečnosti, přičemž je skutečností, že druhý jmenovaný naplňuje cíle lidí lépe [2,5]. Je to způsobeno tím, že riziko a bezpečnost jsou sice v určitém vztahu, ale nejsou komplementárními veličinami [11], protože bezpečnost lze zvýšit, aniž bychom snížili riziko, např. aplikací varovacích systémů zvýšíme bezpečnost, ale riziko nesnížíme. Komplementární veličinou k bezpečnosti je kritičnost. Kritičnost je chápaná jako mezní stav systému, který je významný pro stabilitu systému [10] a posuzuje se podle:

- možných škod na životech a zdraví lidí. Usuzuje se na ní dle škod možných při haváriích, v jaderných nebo chemických provozech,
- ztráty funkčnosti cílené činnosti, která má jisté poslání (mission). Usuzuje se na ni dle rozsahu postiženého území, např. při selhání navigačního systému,
- ekonomických škod při podnikání. Usuzuje se na ni např. dle ztrát, které způsobí nefunkčnost bank.

2.8.1. Postup pro zajištění bezpečnosti

V praxi používáme a v encyklopediích nalezneme pojmy: mezinárodní bezpečnost, kolektivní bezpečnost, technická bezpečnost, bezpečnost při práci, požární bezpečnost, jaderná bezpečnost, chemická bezpečnost, kybernetická bezpečnost, informační bezpečnost, bezpečnost při těžbě surovin, veterinární bezpečnost, veřejná bezpečnost apod. Např. mezinárodní bezpečnost je chápána jako soubor norem, opatření a institucí v oblasti mezinárodních vztahů, které mají umožnit pokojný život a rozvoj států, zajišťovat jejich územní celistvost, politickou nezávislost a mírové soužití.

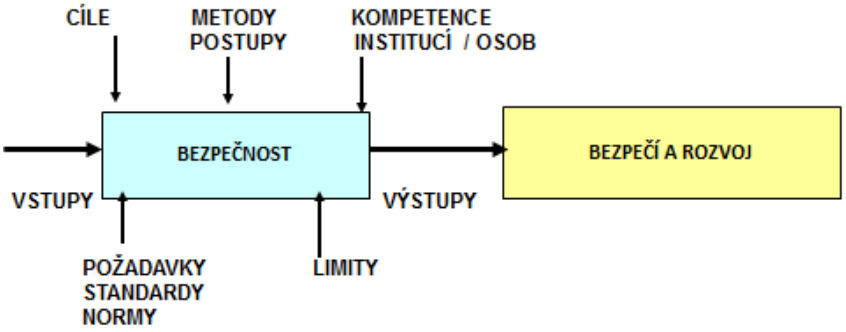
V některých odborných pracích je bezpečnost chápaná jako vlastnost, která vystupuje na úrovni systému. Jindy zase je chápaná jako charakteristika daného systému, pro kterou platí, že bezpečné zařízení nebo bezpečný systém je spolehlivý, ale spolehlivý systém ještě nemusí být bezpečný. Spolehlivost je definovaná jako charakteristika daného objektu vyjádřená pomocí pravděpodobnosti, že tento bude vykonávat specifikovaným způsobem funkce, které jsou na něm požadovány během stanoveného časového intervalu a za stanovených resp. předpokládaných podmínek.

Většina lidí vnímá bezpečnost také zcela jinak, tj. velmi subjektivně, protože na ně spíše doléhají obtíže každodenního života než obavy spojené s výskytem extrémních pohrom. Člověk je a byl vždy nějak ohrožován živelními pohromami, morem, apod., a proto otázky spojené s bezpečností člověka, tj. lidskou bezpečností nejsou jen nějakou dnešní specifikou. Během historického vývoje se měnilo poznání i požadavky na bezpečnost i institucionální možnosti zmírňující vše, co může bezpečnost ohrozit.

Ve zvažovaném pojetí světa platí, že když se zaměříme jen na určitou oblast, tak sledujeme dílčí bezpečnost. Když bezpečnost určitého celku chápeme jako součet dílčích bezpečností, tak dostaneme integrovanou bezpečnost. Jestliže bezpečnost celku chápeme jako celistvou bezpečnost systému, tak dostaneme integrální bezpečnost. Je zřejmé, že opatření uvedených bezpečností nejsou nutně totožná, protože se opírají o rozdílné přístupy při vyjednávání s riziky. Na základě současného poznání je cílem správného řízení věcí veřejných zajištění integrální bezpečnosti [2].

Koncept na zajištění integrální bezpečnosti lidského systému (tj. lidské bezpečnosti) se opírá o základní paradigma, že vývoj lidského systému v čase a prostoru je z hlediska člověka a jeho přání narušován jevy, které jsou systému vrozené / inherentní a mají od určité velikosti nežádoucí, tj. pro člověka nepřijatelné dopady, tj. působí újmu, škody a ztráty na chráněných aktivech, které se projevují jako oběti, rozmanité škody a ztráty na chráněných aktivech.

Ze systémového hlediska je zajištění bezpečnosti základním požadavkem na systém jako celek, nikoli jen požadavkem na jeho komponenty, a poměrně snadno se dá odvodit systémové schéma řízení bezpečnosti v určité situaci uvedené na obrázku 7. Z obrázku je zřejmé, že tím jaká opatření používáme k zajištění bezpečnosti, tím určujeme výsledek, tj. bezpečí jako stav systému.



Obr. 7. Procesní model vytváření aktuální bezpečnosti, jeho vstupy a výstupy.

Znovu zdůrazníme, že úkolem vypořádání rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Snižování rizika je vždy spojeno se zvyšováním nákladů. Proto řízení rizika je vedeno snahou najít hranici, na kterou je únosné riziko ještě snížit, aby vynaložené náklady byly společensky přijatelné. Z pohledu praxe je třeba se dohodnout na tom, jaké požadavky bude výstup z hodnocení rizika splňovat. Při hodnocení rizik je nutné se snažit stanovené požadavky dodržovat a případné nedodržení odůvodnit. Jedná se především o splnění požadavků: provedení hodnocení v požadované šíři a kvalitě v souladu s přijatou metodikou hodnocení; úplnost hodnocení; zahrnutí nejnovějších poznatků vědy; odhad nejistot i neurčitostí v případě použití extrapolací; jednotné vyjádření charakteristik rizika; a průhlednost provedení procesu hodnocení rizik.

Svět je však složitý systém systémů ve vertikální i horizontální rovině, a proto jeho chování je heuristické, tj. je značně proměnné v závislosti na vnitřních a vnějších podmínkách, což znamená, že za určitých situací vznikají neočekávané jevy, které v reálném životě mohou přinést citelné ztráty a škody, protože jsou důsledky jevů, se kterými člověk na základě svých znalostí nepočítá [1,5,10], protože nejsou detekovatelné stochastickými metodami, které pracují s náhodnými nejistotami. Teprve dnes u zvláště složitých systémů systémů hledáme způsoby, abychom zabránili: atypickým haváriím; kaskádovitým selháním infrastruktur; eskalaci dopadů na chráněná aktiva; nebo nežádoucím propojením v kritických objektech, tj. snažíme se vyrovnat s riziky, jejichž zdroji jsou neurčitosti (tj. znalostní nejistoty). Jak již bylo dříve řečeno, používáme k tomu multikriteriální přístupy [1,5,15].

Na základě komplexní analýzy a kritického posouzení několika tisíc odborných prací a výsledků z praxe, jejichž výsledky jsou v pracích [1,2,5,10,11], je nutné při řešení problémů bezpečnosti kritických objektů použít systémový přístup (tj. zaměřit se na integrální riziko) a nejprve vybrat správný koncept práce s riziky (tj. kontext, v němž rizika sledujeme) a poté respektovat logický model práce s riziky. Klíčové koncepty inženýrství zaměřeného 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 zajištujících 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.

Z hlediska lidských možností, tj. disponibilních prostředků na vypořádání rizika se musí provádět optimalizace, kterou určují přístupy ALARP a ALARA [1,10,11].

2.8.2. Koncept zajištění bezpečnosti objektu

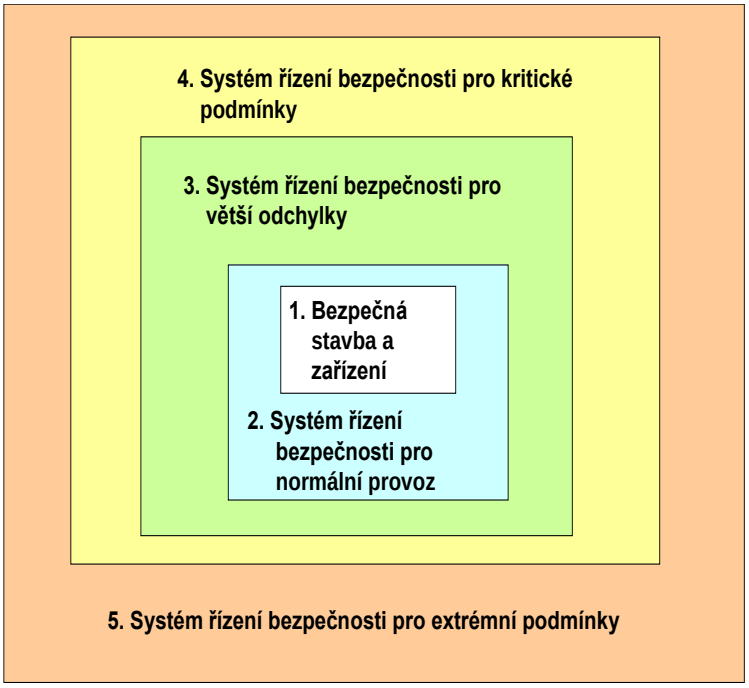
Zajištění bezpečnosti jistého objektu na základě recentních znalostí, shromážděných v práci [1] provádíme způsobem, že propojujeme dva přístupy, a to All-Hazard-Approach a Defence-In-Depth. Jestliže vezmeme v úvahu koncepty stanovené OSN [20] a EU [21], tak strategické řízení území či jiného systému znamená řízení bezpečnosti příslušné entity. Přístup All-Hazard-Approach [8] ve formě specifikované pro Evropu [7] znamená zvažovat při řízení bezpečnosti všechny možné druhy pohrom, tj. jevů, které mohou způsobit škody, ztráty a újmy člověku a aktivům, na kterých závisí jeho život.

Protože složité socio-kyber-technologické objekty jsou důležité pro lidi při stabilizaci situace, obnově území po pohromě a pro další rozvoj (konkurenceschopnost, zaměstnanost apod.), tak je třeba dbát i o zajištění kontinuity kritických objektů. Jelikož zde vznikají konflikty, tak se zpracovává speciální nástroj, kterým je plán řízení rizik [16].

Na základě znalostí uvedených v pracích [1,2,5,10,11,22-25] a syntézou údajů získaných výzkumem, popsaným v práci [17], je navržen procesní model pro řízení bezpečnosti entity, který zohledňuje přežití lidí při kritických podmínkách, obrázek 8. Na základě zkušeností z praxe, autorka metodou analogie uspořádala základní principy pro řízení bezpečnosti kritických objektů typu systém systémů (obrázek 8) takto:

1. V návrhu, výstavbě a konstrukci inherentně používat principy bezpečného projektu (přístupy: All-Hazard-Aproach, 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; správná práce s riziky; a monitoring, ve kterém jsou zabudovány korekční opatření a činnosti). Důležité je sestavení zadávacích podmínek spojených s daným územím, které vyjadřují způsob ocenění místních zranitelností vůči všem relevantním pohromám, které mohou postihnout dané místo (tj. aplikace All-Hazard-Approach). Na základě recentního poznání, shrnutého v pracích [10-12], 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. 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.



Obr. 8. Pětistupňový systém řízení bezpečnosti složitého objektu.

Pro úspěšné zvládnutí rizik u technologických systémů je podle [26] 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) - lze aplikací pracovních postupů podle daných přijatých standardů a výcvikem ve 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, ale také improvizovat,
- při nemožnosti zvládnout zařízení, musí být personál schopen odstavit technologii tak, že zajistí, co nejmenší ztráty u technologie a aktivovat vnější nouzový plán (tj. aplikovat ochranná opatření a činnosti, uvolnit rezervy, provést evakuaci).

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 úrovní musí být takový, aby zvládnul vyvážit působení určených jevů. Součástí ochrany do hloubky jsou proto všechny činnosti při umísťování, navrhování, stavbě, výrobě, konstrukci, zkušebním provozu, uvedení do trvalého provozu, provozu a odstavení z provozu u posuzovaného objektu, infrastruktury či technologie. Bezpečný systém systémů se zajišťuje pomocí souborů a systémů bariér a režimových opatření. 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.

Ochrana do hloubky zahrnuje všechny činnosti zacílené na bezpečnost při umísťování, navrhování, výrobě, konstrukci, uvedení do provozu, provozu a odstavení z provozu u technologických děl. Pro zajištění bezpečného systému systémů používá systémy bariér a režimová opatření. Jejím cílem je kompenzovat lidská a technologická selhání, udržovat účinné bariéry, které odvrátí poškození zařízení i bariér samotných; a ochránit lidi a životní prostředí, když bariéry nesplní své úlohy. Cílem první úrovně ochrany (oblast 2 na obrázku 8) zabudované do SMS 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 8) 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 8) 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 8) 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).

2.8.3. Procesní model pro řízení bezpečnosti technologického objektu v čase

Na základě současného poznání jsou používané technologické objekty a infrastruktury (tj. bodové, plošné, liniové či síťové entity) otevřené systémy systémů, tj. soubory vzájemně propojených otevřených systémů [1]. Každý ze systémů je tvořen prvky a jejich propojeními, které vytváří vazby a toky mezi prvky. Pomocí logických vazeb a spřažení vytvořených pomocí toků dosahuje tvůrce systému (tj. člověk) toho, že systém plní dané úkoly, tj. vytváří výrobky nebo poskytuje služby. Kromě požadovaných propojení však za jistých podmínek mohou vzniknout nepřijatelná propojení, které vedou k menšímu či většímu poškození systému, při kterém systém neplní úkoly a dokonce ohrožuje sebe a své okolí. Proto se v současné době vytváří technologické objekty a infrastruktury jako bezpečné nebo zabezpečené systémy.

Na základě práce [1] bezpečný systém je chápán jako systém, který je zabezpečen vůči všem vnitřním a vnějším pohromám včetně lidského faktoru, tj. všem škodlivým jevům, a který ani při svých kritických podmínkách neohrožuje sebe a své okolí, tj. prostor, ve kterém žijí lidé. To znamená, že bezpečnost systému je vlastnost systému, která je nadřazena spolehlivosti. Proto 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 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. Tvorba a provoz bezpečného systému jsou podstatně náročnější na

znalosti, zdroje, síly a prostředky, a proto v běžné praxi jsou používány zabezpečené systémy, které jsou v případě potřeby doplněny organizačními opatřeními, která zajišťují ochranu veřejných aktiv, když předmětné systémy ohrožují sebe a své okolí [1,10].

Řešení žádného úkolu není možné uskutečnit izolovaně, tj. bez ohledu na okolí. Proto se dnes provádí strategické řízení, jehož základní principy jsou ukázány na obrázcích 9 a 10. Obrázek 9 ukazuje základní mezníky, které rozhodují o tom, zda chování entity je bezpečné nebo nebezpečné při výskytu nebezpečné situace. Obrázek 10 ukazuje představu o řízení bezpečnosti entity sestavenou na základě výše uvedených poznatků o řízení rizik.

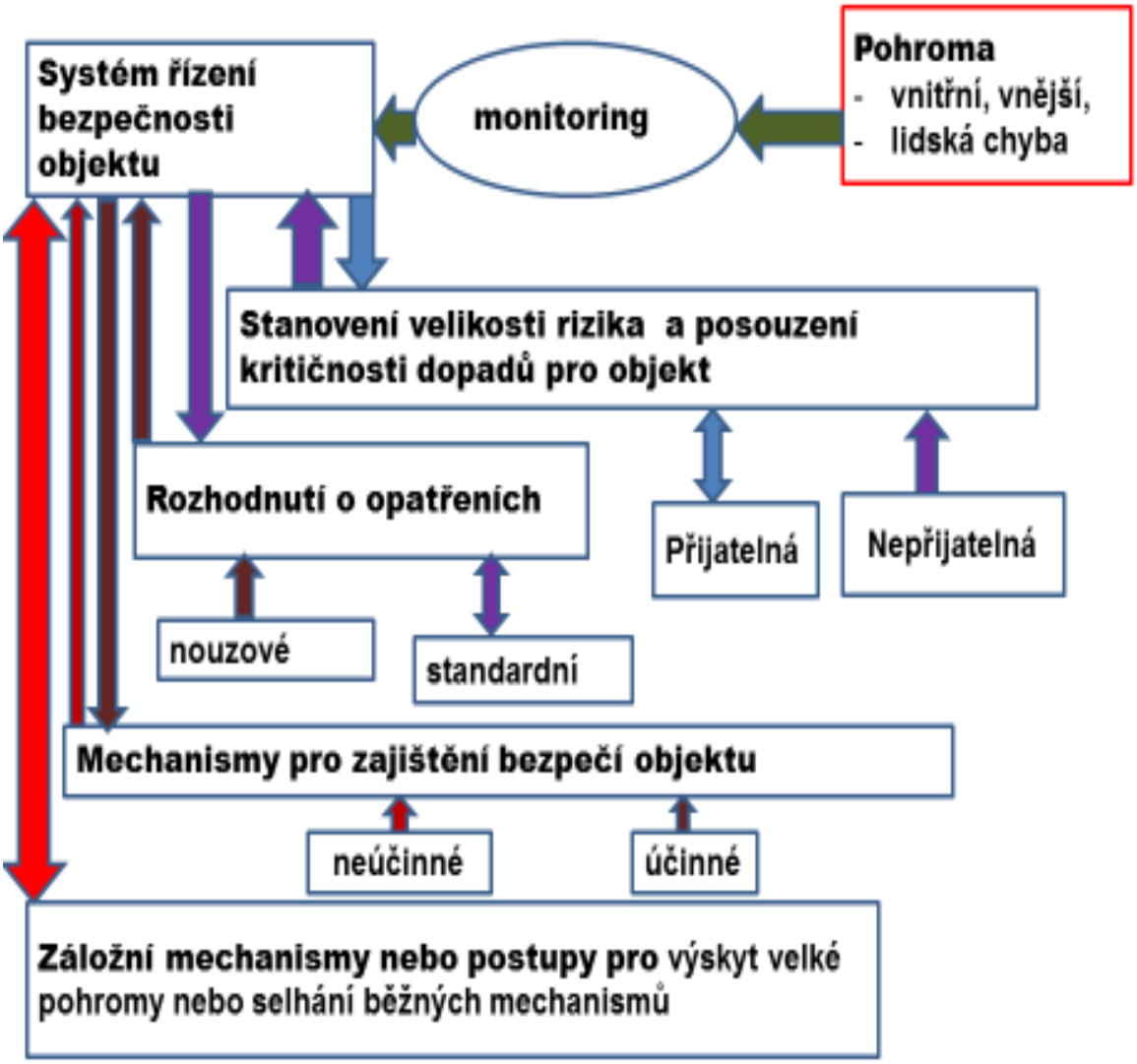
Obr. 9. Mezníky rozhodující o bezpečném nebo nebezpečném chování entity při výskytu nebezpečné situace.

Na základě současného poznání, shrnutého v pracích [1,2,5,10,11,27-30], systém řízení bezpečnosti (tzv. SMS – Safety Management System) komplexního 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 [1,27,29]. Jeho model je na obrázku 11. Skládá se z šesti procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií. Uvedené procesy se dále dělí na podprocesy:

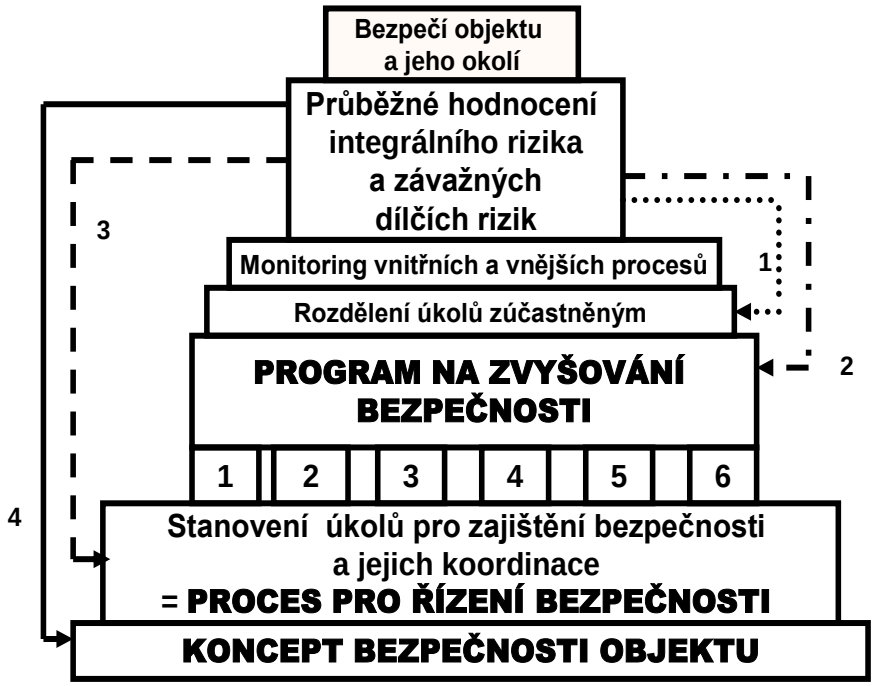
1. První proces se skládá z podprocesů pro: celkovou koncepci; dosahování dílčích cílů bezpečnosti; vedení / správu bezpečnosti; systém řízení bezpečnosti; personál a zahrnuje

úseky pro: řízení lidských zdrojů, výcvik a vzdělání, vnitřní komunikaci / informovanost a pracovní prostředí; revize a hodnocení plnění cílů v bezpečnosti.

2. Druhý proces se skládá z podprocesů 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.
3. Třetí proces zahrnuje podprocesy pro: výzkum a vývoj; projektování a montáže; inherentně bezpečnější procesy; technické standardy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů.
4. Čtvrtý proces obsahuje podprocesy pro: spolupráci se správními úřady; spolupráci s veřejností a dalšími zúčastněnými (včetně akademických pracovišť); a spolupráci s dalšími podniky.
5. Pátý proces 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.
6. Šestý proces má 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).



Obr. 10. Představa o způsobu řízení bezpečnosti entity.



Obr. 11. Model řízení bezpečnosti komplexního kritického objektu v čase. Procesy: 1- koncepce a řízení; 2 - administrativní postupy;3 - technické záležitosti; 4 - vnější spolupráce; 5 - nouzová připravenost; a 6 - dokumentace a šetření havárií.

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.

Tým expertů včetně autorky ověřil použitelnost modelu na datech shromážděných v archivu [12]. Z obrázku 11 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 11. 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.

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

Integrita bezpečnosti je definována jako „pravděpodobnost systému souvisejícího s bezpečností uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu“. Většinou se sleduje ve spojení s lidskými chybami v různých etapách životního cyklu systému. Patří sem např. chyby specifikace, chyby návrhu, chyby instalace, chyby údržby, chyby modifikace. Posouzení integrity bezpečnosti souvisí s posouzením, jak

systém bezpečně selže. Tj. posuzuje pravděpodobnost výskytu bezpečného selhání a nebezpečného selhání. Spolehlivost ve smyslu reliability není samotná schopná zajistit SIL. Specifické nástroje řízení používající techniky zacílené na kontinuální hodnocení rizik zajišťují, že systém se vyhne chybám a omylům. Integrita (celistvost) bezpečnosti je tudíž základní mírou bezpečnosti technického díla.

Způsob řízení bezpečnosti (SMS) technologického objektu se opírá o koncepci prevence pohrom či alespoň jejich závažných dopadů [1,2,27], 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 pohromami na všech organizačních úrovních kritického objektu a opatření na zajištění výcviku, která jsou sladěna s identifikovanými potřebami výcviku.
2. Plány pro systematické identifikování závažných nebezpečí spojených s možnými pohromami a z nich plynoucích rizik, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti).
3. Plány a postupy pro zajištění bezpečnosti všech komponent, systémů a funkcí v kritickém objektu a v jeho okolí, a to včetně údržby objektů, zařízení.
4. Plány na implementaci změn v kritickém objektu a v objektech i zařízeních, které jsou v okolí.
5. Plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na možné nouzové situace.
6. 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.
7. Plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků kritického objektu.

Znalosti získané studiem havárií [1,12] ukazují, že velkou pozornost musíme věnovat chování lidí i lidským opatřením a činnostem a způsobu jejich řízení a provádění, abychom předcházeli organizačním haváriím. Bezpečnostní kultura tak souvisí s organizační kulturou, která je souborem dohodnutých pravidel uplatňovaných v řízení organizačních jednotek a podílí se na vytváření norem institucionálního chování. Znamená správné aplikování znalostí, přemýšlení a správné reakce na reálné situace. Nejde totiž jenom o dodržování norem a předpisů zacílených na spolehlivost našich opatření a činností, protože tím můžeme přehlédnout jevy, které normy a předpisy nevidí. Jde o chování založené na řízení znalostí [28].

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie. Analýzy havárií: rozlomení plošiny Alpha v r. 1988 v Severním moři; havárie skladu leteckého petroleje v Buncefieldu 11. 12. 2005; neobjasněné námořní, vlakové a letecké havárie v posledních letech; havárie v jaderné elektrárně Fukushima 11. 3. 2011 (pozn. – byla podceněna velikost tsunami, nebyly respektovány vypočtené scénáře havárií), ukázaly, že řada odborníků bývá postižena provozní slepotou a po splnění požadavků norem a standardů nevidí zbylá rizika nebo rizika spojená s různými vazbami a spřaženími s okolím [1]. Např. prosté srovnání intervalů používaných při pravděpodobnostních hodnoceních ukazuje, že dle [12] interval: $(-\sigma, +\sigma)$ pokrývá jen 68.5 % případů; $(-2\sigma, +2\sigma)$ pokrývá 85.4 % případů; a $(-3\sigma, +3\sigma)$ pokrývá 99.8 % případů.

Proto je třeba vzít v úvahu, že v současné době provozované a budované socio-kyber-technologické objekty jsou bezpečné jen v určitém intervalu podmínek. Jestliže se vyskytnou podmínky mimo tento interval, technologické objekty se dostávají do nestabilních stavů, při kterých se objevují neočekávané pohromy, jako jsou enormně silné škodlivé jevy a kaskády

selhání bez zjevné příčiny. Z důvodu zajištění jejich bezpečnosti musíme připustit, že kromě náhodných nejistot vypořádaných pravděpodobnostními přístupy, existují i epistemické (znalostní) nejistoty, tj. neurčitosti, které ovlivňují jejich chování.

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

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

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

3. SLOŽITÉ SOCIO-KYBER-TECHNOLOGICKÉ SYSTÉMY, JEJICH RIZIKA A BEZPEČNOST

Námi sledované složité socio-kyber-technologické (možná lépe socio-kyber-technické) systémy zahrnují jednak složité objekty a jednak infrastruktury, které mohou pracovat samostatně a dohromady pak plní zcela jedinečný úkol, který je vzdálený od úkolů jednotlivých složitých systémů (např. systémy pro výrobu, distribuci a spotřebu elektřiny, plynu apod.). Podle prací uvedených v [1] jsou pro ně důležité dvě systémové vlastnosti, a to interaktivní složitost a těsná spojení. Složité interakce jsou neplánované, neočekávané a většinou neznámé sekvence, které nejsou bezprostředně srozumitelné. Složité interakce v systémech systémů mají za následek nejednoznačná rozhodnutí, nestabilní preference a konfliktní cíle. Těsná spojení jsou nutnou podmínkou k eskalaci nežádoucích jevů vedoucích až k selhání či havárii. Charakterizují se jako proces, který je časově závislý, má malé časové rezervy, je invariantní (v procesu je jediné pokračování – B musí následovat po A), a v důsledku předmětných charakteristik je u něho omezený prostor pro improvizaci.

Interaktivní složitost a těsná spojení mezi prvky v sociotechnickém systému mohou vést ke kritické situaci v důsledku systémového selhání. To znamená, že riziko se tak stává systémovou vlastností. Kvůli složitosti a vysoké propojenosti sledovaných objektů je systematická analýza zranitelností a robustností s ohledem na selhání obtížná, a proto se používají výsledky simulací. Bezpečnost je definována jako nefunkční požadavek a je spojena s vynořujícími se vlastnostmi systému. Zvažované nefunkční vlastnosti nemohou být přiřazeny k jednotlivým komponentám systému. Vynořují se jako integrující výsledek chování systému. Proto požadavky na bezpečnost jsou formulovány na úrovni celého socio-kyber-technologického systému a poté sestupným procesem na dílčí systémy. Výsledek působení pohromy o jisté velikosti závisí na okamžitém stavu systému.

3.1. Charakteristiky složitých socio-kyber-technologických systémů

Technologické objekty a infrastruktury jsou nutné pro životy lidí v dnešním světě. Je však pravdou, že na jedné straně usnadňují život lidí, ale na straně druhé ho ohrožují, když dojde k haváriím. Největší rizika jsou spojená s objekty a infrastrukturami, které jsou složité a obsahují nebezpečné chemické látky, anebo nahromadění velkých energií. Velké technologické provozy a technické systémy jsou víc než jen množinou technických částí zařízení a součástek. Jsou odrazem organizační struktury, managementu, provozních předpisů a kultury konstrukčních organizací, které je vytvořily a také jsou zpravidla i odrazem společnosti, ve které byly vytvořené [1,10,11].

Nehody a havárie v technologických objektech a infrastrukturách jsou často svalované na chyby operátorů nebo provozovatelů zařízení, bez rozlišení průmyslových, organizačních a manažerských faktorů, které způsobily, že se předmětné chyby a nedostatky staly nevyhnutelnými. Příčiny havárií mají často, ne-li skoro vždy, kořeny v organizaci, tj. v její kultuře, managementu a struktuře a platí, že všechny faktory jsou kritické pro bezpečnost technických systémů.

Pro popis složitých objektů v systémovém pojetí používáme následující charakteristiky [1,10]:

1. Interoperabilita složitého objektu je schopnost objektu, která zajišťuje, že jeho dílčí systémy pracují společně efektivním způsobem podle konceptu projektu, který je zaměřen na určitý cíl. Dělí se na technickou a organizační. Technická interoperabilita se vztahuje k fyzickým

a komunikačním spojením mezi zařízeními a systémy. Organizační interoperabilita se zabývá vztahy mezi organizacemi a jejich částmi včetně podnikatelských a právních vztahů.

2. Integrita bezpečnosti složitého objektu (SIL) označuje schopnost složitého objektu dosáhnout požadovaných bezpečnostních funkcí. Je definována jako „pravděpodobnost systému souvisejícího s bezpečností uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu“. Sleduje se většinou ve spojení s lidskými chybami v různých etapách životního cyklu systému. Patří sem např. chyby specifikace, chyby návrhu, chyby instalace, chyby údržby, chyby modifikace.
3. Kritičnost složitého objektu (C) je míra, s jakou může dojít v souvislosti s činností sledovaného objektu k úrazu osob, zničení materiálu, škodě či jiným velkým ztrátám. Platí vztah:

   $$C = S * O * B$$

   ve kterém S je závažn*ost největšího dopadu dané pohromy;* O pravděpodobnost výskytu pohromy; a B je podmíněná pravděpodobnost, že se při dané pohromě vyskytne nejzávažnější dopad. Kritičnost označuje určitou prahovou hodnotu pro sledovaný objekt. Jsou-li její hodnoty pod tímto prahem, tak je stav žádoucí a opačně.
   Spolehlivost ve smyslu reliability není samotná schopná zajistit SIL. Proto je třeba použít specifické techniky, které zajistí, že systém se vyhne chybám a omylům. Z předmětného důvodu se provádí řízení rizik zacílené na bezpečnost a provozní spolehlivost (dependability). Z hlediska bezpečnosti lidského systému (tj. bezpečí a udržitelného rozvoje lidské společnosti) je nutné zajistit kvalitní obslužnost území, která je rovněž podmíněna provozní spolehlivostí.
4. Provozní spolehlivost systému (dependability) znamená, že systém (objekt, zařízení) plní stanovené požadavky a že jeho provoz vyhovuje stanoveným podmínkám. Tato souhrnná vlastnost je pro analytické účely nepraktická, a proto se rozkládá do dvou základních vlastností, kterými jsou zranitelnost a odolnost. Provozní spolehlivost je důležitá u složitých objektů, jejichž systémy hrají klíčovou roli v obslužnosti společnosti, protože ovlivňují rozhodovací cyklus veřejné správy a politickou a sociální soudržnost a napomáhají v odstraňování fyzických a psychických škod, jsou nejen velmi složité, ale i zranitelné [1]. Proto se v jejich hodnocení vždy charakterizují a popisují tři základní vlastnosti: pružná odolnost (resilience); zranitelnost; a schopnost adaptace.
5. Odolnost je třeba chápat jako jistou funkční schopnost složitého objektu plnit úkoly i za jiných podmínek než jsou podmínky normální, pro které byl zkonstruován. Pro zajištění předmětné schopnosti je nutné, aby objekt měl určitou adaptační kapacitu. Proto dle [1] jsou v projektování, výstavbě a provozování technických děl zvažovány intervaly očekávaných podmínek a jim odpovídající mezní (kritické) stavy, tj. předvídatelné situace, jejichž dopady jsou vysoce nepřijatelné. Pro jejich odvrácení se uplatňuje princip předběžné opatrnosti a speciálně se vytváří zařízení a systémy pro podporu bezpečnosti při výskytu těchto mezních podmínek. Nicméně mohou nastat kritické stavy, které jsou nepředvídatelné nebo jsou důsledkem závažné chyby obsluhy, anebo vnější pohromy, se kterou se v projektu objektu nepočítalo, a ty mohou přejít do nežádoucích / nepřijatelných, tj. i vysoce kritických (krizových) stavů. Pro jejich zvládnutí je třeba vytvářet specifické nástroje odezvy. Pružná odolnost systému je schopnost systému absorbovat a využít odchylky a změny vyvolané pohromou tak, že systém není poškozen a přetrvá ve své funkčnosti.
6. Zranitelnost systému je náchylnost systému při výskytu pohromy ke vzniku škody.
7. Adaptace systému je schopnost systému přizpůsobit se změnám bez škod nebo za přijatelných škod.

Z hlediska současného poznání před námi dnes stojí minimálně dva následující úkoly:

1. Řešit problém funkčnosti souboru vzájemně propojených (tj. závislých) objektů a infrastruktur (tj. systému systémů) za normálních, abnormálních a kritických podmínek.
2. Vyhledat kritické stavy systému systémů, které jsou nepředvídatelné a za jistých podmínek mohou přejít do vysoce nežádoucích, tj. vysoce nepřijatelných stavů, ve kterých je ohrožena samotná existence lidí a které obvykle označujeme jako krizové.

Jelikož kritické objekty jsou často vybaveny drahou technologií, dochází při odezvě na nouzové situace často ke konfliktu mezi provozními inženýry a bezpečnostními složkami zacílenými na ochranu lidí, protože inženýři jsou vzdělávání i cvičení ke zvládání normálních, abnormálních i kritických podmínek a k respektování ochrany technologií, protože provoz technologií jim poskytuje práci, tj. i obživu. Na základě pro-aktivního přístupu, který je vlastní projektovému a procesnímu řízení, se řešení konfliktů předem připravuje, a to sestavením plánu pro řízení rizik, který je odsouhlasen předpokládanými zúčastněnými stranami [12,16],

3.2. Rizika složitých systémů a zásady pro jejich řízení

Nejprve shrneme základní pojmy a souvislosti, o které se opíráme:

1. Bezpečí je stav systému, při kterém vznik újmy na chráněných aktivech má přijatelnou pravděpodobnost (tj. je téměř jisté, že újma nevznikne). Do předmětné charakteristiky systému patří i jistá stabilita systému v čase a prostoru, tj. udržitelný rozvoj v čase a prostoru. Antonymum je nebezpečí.
2. Bezpečnost je uspořádaný soubor antropogenních opatření a činností, kterými člověk zajišťuje bezpečí systému. Pro zajištění současných potřeb jde o integrální bezpečnost, tj. o bezpečnost, která sleduje několik chráněných zájmů (aktiv) najednou. Antonymum je nebezpečnost, anebo častěji v technické oblasti kritičnost.
3. Bezpečnost souboru vzájemně závislých systémů je předurčená nejen bezpečností jednotlivých systémů, ale také charakterem vzájemných propojení.
4. Řízení bezpečnosti systému je pak disciplína aplikující metody, nástroje a techniky založené na inženýrských a manažerských přístupech tak, aby systém byl bezpečný. Opírá se o řízení rizik, ve kterém je zapracován princip předběžné opatrnosti. V případě komplexního řízení bezpečnosti jde o řízení komplexního (integrálního) rizika.
5. Riziko je chápáno jako pravděpodobná velikost ztrát, škod a újmy na chráněných aktivech v konkrétním objektu rozpočtená na jednotku plochy a času. Je závislé na velikosti konkrétní pohromy a místní zranitelnosti. Pro potřeby strategického řízení je normativně stanoveno, jak bylo uvedeno v předchozí kapitole.
6. Komplexní (integrální) řízení bezpečnosti je specifická disciplína pro řízení bezpečnosti složitých systémů (SoS), jejíž koncept ukazuje obrázek 11.
7. Zabezpečený systém je systém, který plní kvalitně uložené úkoly po celou dobu životnosti a je ochráněn proti vnitřním i vnějším pohromám (škodlivým jevům všeho druhu).
8. Bezpečný systém je zabezpečený systém, který kvalitně plní uložené úkoly po celou dobu životnosti, je ochráněn proti vnitřním i vnějším pohromám (škodlivým jevům všeho druhu) a navíc ani při svých kritických podmínkách neohrožuje sebe a své okolí.

Vzhledem k lidským schopnostem a možnostem je rozdíl mezi zabezpečeným a bezpečným systémem v tom, že bezpečný systém má v sobě zabudované mechanismy na zvládnutí kritických a extrémních podmínek tak, aby škody na veřejných aktivech a na něm samotném byly přijatelné.

Bezpečnost a riziko spolu jistým způsobem souvisí, ale nejsou komplementární veličiny. Snížení rizika znamená zvýšení bezpečnosti, ale obráceně to neplatí!!! Rizika spojená se sledovanými objekty jsou: bezpečnostní rizika; stavebně-technologická a projekční rizika; kreditní rizika; tržní rizika; vnější rizika; provozní rizika a rizika spojená s řízením a

rozhodováním [5]. Je si třeba uvědomit, že významné zdroje rizik jsou: poruchy dodavatelsko-odběratelských vztahů; nejistota v oblasti pracovních sil; neurčitost finančních zdrojů; havárie a velké poruchy na provozovaném zařízení; průmyslové havárie u jiných subjektů; živelní pohromy; a politická nebo hospodářská nestabilita v regionu, kde je objekt umístěn.

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 [1].

Celkové (integrální) riziko je rovno součtu přímých a nepřímých ztrát na aktivech, přičemž nepřímé ztráty zvyšují:

- prodlevy nebo chyby v odezvě,
- kaskády selhání způsobené synergickými a kumulativními jevy, které jsou způsobené vazbami a spřaženími mezi aktivy,
- domino efekty

[1]. Je vyjádřeno vztahem

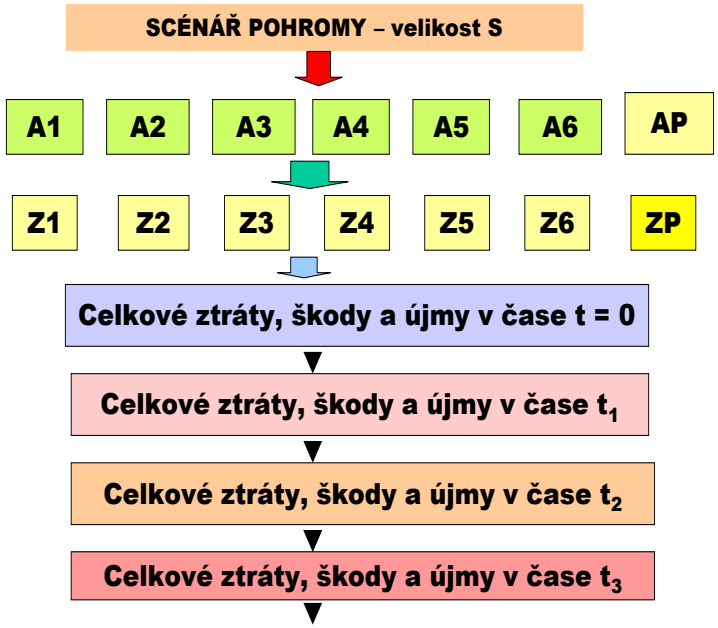
$$R(H) = \left[\sum_{i=1}^{n} A_i(H)Z_i(H) + \sum_{i=1}^{n}\int_0^T \int_S F(H, A_i, P_i, O, t)\mathrm{d}S\mathrm{d}t\right] \cdot \tau^{-1} \quad ,$$

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

Na základě současných znalostí přímé škody, ztráty a újmy na aktivech umíme určit, když vybereme správný scénář pohromy. Neumíme správně určovat škody, ztráty a újmy spojené s vazbami a toky ve složitých systémech [1]. Proto v případě potřeby zajistit bezpečnost závažných objektů stanovíme expertním způsobem řadu relevantních scénářů prioritních pohrom. Jejich rizika určíme způsobem zobrazeným na obrázku 12 a expertním způsobem stanovíme ochranná opatření [1] s tím, že největší váhu budou mít údaje pro scénáře s největší pravděpodobností výskytu, která bude stanovena na základě posouzení případových studií sestavených pro možné situace na základě reálných dat.

Úkolem řízení rizika je najít optimální způsob, jak vyhodnocená rizika snížit na požadovanou společensky přijatelnou úroveň, případně je na této úrovni udržet. Proto je třeba se dohodnout na tom, jaké požadavky bude výstup z hodnocení rizika splňovat a při vypořádávání rizik je nutné se snažit tyto požadavky dodržovat a případné nedodržení odůvodnit. Na základě poznání moderní způsob práce s riziky požaduje:

- riziko stanovovat během celého cyklu životnosti objektu (umísťování, projektování, výstavba, provoz,
- stanovení rizika zaměřovat na požadavky uživatelů a úroveň poskytovaných služeb,
- stanovovat rizika podle kritičnosti dopadů na procesy, poskytované služby a na aktiva, která stanovuje veřejný zájem,
- nepřijatelná rizika zmírňovat prostřednictvím nástrojů řízení rizik, tj. pomocí technických a organizačních návrhů, standardizací operačních postupů nebo automatizovanou kontrolou [1].



Obr. 12. Vývojový diagram pro stanovení rizik pro potřeby strategického řízení bezpečnosti; A – aktiva a Z ztráty, škody a újmy na aktivech; označení: 1- životy a zdraví lidí, 2- bezpečí lidí, 3 – majetek, 4 – veřejné blaho, 5 – životní prostředí, 6 – infrastruktury a technologie, P – privátní.

Postup v případě, že riziko není přijatelné, spočívá v: 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; či retence rizika [5]. Podle Mezinárodní organizace pro standardizaci [5] kvalifikované řízení rizik musí respektovat:

1. Řízení rizik musí být nedílnou součástí systému řízení sledované entity.
2. Řízení rizik musí být obsaženo v každém procesu rozhodování sledované entity.
3. Řízení rizik se musí explicitně zabývat nejistou a neurčitostí v procesech a podmínkách sledované entity a jejího okolí.
4. Řízení rizik musí být systematické a strukturované.
5. Řízení rizik musí vycházet z nejlepších dostupných informací.
6. Řízení rizik musí být dynamické a vhodně reagovat na různé změny.
7. Řízení rizik musí být uzpůsobeno každé instituci.
8. Řízení rizik musí mít na zřeteli vliv člověka (lidský faktor).
9. Řízení rizik musí mít schopnost neustálého zlepšování.

Rizika se ovládají 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),

- 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 [1,2].

Znovu si je třeba připomenout, že 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.

Protože jak již bylo několikrát uvedeno, se ve sledované oblasti při řízení rizik orientujeme na bezpečnost [1,5], tak nástroj pro řízení bezpečnosti se zabývá také připravenosti, která určuje:

1. Co se může vyskytnout?
2. Jak to bude veliké?
3. Čím se zmírňuje to, co je nepřijatelné?
4. Co je důležité pro varování a zásah inženýrů, výkonných složek, pro akce veřejné správy a pro chování občanů?

V dané souvislosti mluvíme o řízení bezpečnosti sledovaných objektů. Jeho problémy z hlediska současného poznání [1,5] jsou:

1. Je třeba sledovat několik různorodých chráněných aktiv, mezi nimiž existují různé vnitřní vazby a toky.
2. Je třeba sledovat odolnost, zranitelnost a adaptabilitu jednotlivých prvků, komponent, systémů a znát, kdy (při jaké kombinaci vlastností) je systém bezpečný.
3. Je třeba sledovat integrální riziko a zvažovat zdroje rizik uvnitř i vně systému, jelikož dílčí nebo integrovaná rizika zanedbávají závažné skutečnosti spojené s tím, že sledovaná entita má více rozmanitých chráněných aktiv, které jsou propojené vnitřními vazbami a toky.
4. Legislativa pro podporu řízení bezpečnosti nesmí mít charakter všeobecných proklamací.
5. Kontrolní mechanismy pro monitorování úrovně bezpečnosti musí být místně specifické a mít dostatečnou vypovídací hodnotu.

Řešením uvedených problémů je: komplexní chápání rizik; vyjednávání s riziky dle priorit; a zavedením strategického a koncepčního řízení entity, ve které problémy v oblasti investiční, technické, technicko - organizační, správní a řídící, vědeckovýzkumné, výchovy a dalších se řeší pro-aktivně, systémově a strategicky s ohledem na znalosti a zkušenosti projektovým způsobem [1].

Právě uvedená skutečnost znamená zásadní obrat v řízení organizací s ohledem na žádoucí cíle, a to o uvědomění, že integrální / komplexní bezpečnost nelze dosáhnout jednotlivými dílčími opatřeními, ale pouze komplexním přístupem s ohledem na místní podmínky. V dané souvislosti 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 zájmů a jejich obnově a k nastartování jejich dalšího rozvoje (viz zlatá pravidla shrnutá v práci [28]).

Systémová bezpečnost je nástroj používaný lidmi, který využívá teorii systémů a systémové inženýrství pro prevenci předpověditelných havárií a pro minimalizování následků nepředvídatelných havárií. V moderním pojetí se zajímá všeobecně o ztráty a škody a ne jen o smrtelné úrazy, anebo o zranění, např. o poškození majetku, nesplnění poslání (mise, účelu), anebo environmentální škody. Klíčovým bodem je považovat ztráty za dostatečně vážné na to, aby na jejich prevenci byl věnovaný dostatek času, úsilí a prostředků. Velikost investic

věnovaných na předcházení haváriím, anebo jejich dopadům je podstatně závislá na sociálních, politických a ekonomických faktorech.

Prvotním zájmem systémové bezpečnosti je řízení rizik: identifikace možných ohrožení; stanovení a vyhodnocení rizik; eliminace anebo řízení pomocí analýzy designu, anebo organizačních procedur. V r. 1968 vzniká nová disciplína „inženýrství systémové bezpečnosti" jako „organizované veřejné mínění". Jedná se o plánovaný, osvojený a systematický přístup k identifikování, analyzování a kontrolování rizik během celého životního cyklu systému za účelem snížení pravděpodobnosti výskytu nehod a minimalizace jejich dopadů.

Program systémové bezpečnosti musí zabezpečovat přesně stanovený postup metodické kontroly bezpečnostních aspektů a hodnotit projekt zařízení ve smyslu identifikování možných zdrojů rizik a předepsání časově i nákladně efektivních nápravných zásahů. Cíle programu systémové bezpečnosti mají zajistit:

- bezpečnost zařízení odpovídající jeho poslání, která je zabudovaná inherentně,
- identifikaci, vyhodnocení, eliminaci anebo řízení rizik na akceptovatelné úrovni ohrožení, a to u všech rizik přidružených k systému, podsystému a jednotlivým částem,
- řízení rizik od ohrožení, která nemohou být eliminována; tj. rizika musí být zajištěná tak, aby chránila personál, zařízení a majetek,
- minimální riziko při použití nových materiálů, anebo výrobků a testovacích technik,
- realizaci nápravných opatření požadovaných pro zlepšení bezpečnosti dočasným včleněním bezpečnostních faktorů, které byly vytvořeny již během vzniku systému,
- zvážení historických údajů o bezpečnosti generované podobnými programy bezpečnosti všude tam, kde je to vhodné.

Průmyslová odvětví si buď adaptovala programy systémové bezpečnosti z vojenství anebo NASA, anebo samostatně vyvinula své vlastní programy podle zkušeností, které byly získány z výstavby jaderných elektráren, z výroby složitých nebezpečných a drahých zařízení. Čekání na výskyt havárií a následné eliminování příčin se stalo neekonomickým a někdy až neakceptovatelným způsobem úprav a zdokonalování systémů [1].

Budování mnohých dnešních komplexních systémů si vyžaduje integraci částí (podsystémů a komponentů) zhotovených různými samostatnými dodavateli a organizacemi. I když každý z dodavatelů dodrží požadovanou kvalitu svých částí, kombinování podsystémů do systémů vnáší nové chyby a nebezpečí, které nejsou vidět, pokud se na uvedené části díváme jako na oddělené části nebo systémy. V mnohých průmyslových odvětvích se potvrdilo, že zabudování inherentní bezpečnosti do zařízení nebo výrobků může zredukovat celkové náklady na jejich životní cyklus, a že dosažení akceptovatelné úrovně bezpečnosti vyžaduje pokrokové recentní přístupy systémové bezpečnosti [1].

Aktivity související se systémovou bezpečností začínají hned v nejranějších stádiích vývoje koncepce systému a pokračují přes všechny projekční činnosti, výrobu, testování, provoz a odstavení. Podstatný aspekt, který odlišuje přístup systémové bezpečnosti od ostatních přístupů bezpečnosti je prvořadý důraz na včasnou identifikaci a klasifikaci nebezpečí tak, aby mohly být přijaté nápravy pro jejich eliminování, anebo minimalizování ještě před konečným projektovým rozhodnutím.

I navzdory tomu, že je systémová bezpečnost relativně novou a ještě stále se vyvíjející disciplínou, má své základní ideje, které jsou zachovány ve všech jejich projevech a odlišují ji od ostatních přístupů bezpečnosti a řízení rizika. Jsou to zásady, že systémová bezpečnost v recentním pojetí:

- zdůrazňuje budování bezpečnosti a ne její přidávání do vytvořeného systému,
- zabývá se systémem jako celkem a ne jen podsystémy a komponentami,
- pojímá ohrožení a s ním spojená nebezpečí poněkud šířeji než jen jako chyby personálu,
- klade důraz raději na analýzu, než na později získanou zkušenost a dodatečně vytvořené standardy,

- upřednostňuje kvalitativní přístupy před kvantitativními,
- rozpoznává důležitost změn a konfliktů cílů v projektu systému a je více, než jen systémové inženýrství.

Nejdůležitějším aspektem systémové bezpečnosti v termínech prevence havárií jsou procedury řízení bezpečnosti. Účinné řízení bezpečnosti spočívá ve stanovení politiky a v definování cílů bezpečnosti, tj. v plánování úloh a procedur; v definování odpovědnosti a určení kompetencí; v dokumentování a průběžném sledování ohrožení a z nich plynoucích nebezpečí včetně kontrol; v udržování bezpečnostního informačního systému včetně zpětné vazby a forem hlášení poruch/havárií apod.

Systémová bezpečnost je odpovědná za zajištění bezpečnosti systému jako celku včetně analýzy rozhraní mezi komponentami. Aktivity na úrovni bezpečnosti komponent, jako např. bezpečnost raketové odpalovací rampy, mohou být součástí všeobecné odpovědnosti za systémovou bezpečnost, anebo mohou být částí inženýrství komponent ve velkých a komplexních projektech. Pro vymezené druhy nebezpečí, jakými mohou být požáry, jaderná bezpečnost anebo výbušné prostředí, může být požadované další členění odpovědnosti za bezpečnost. Při jakémkoli odstupňování rozčlenění úsilí o systémovou bezpečnost mají odpovědnost za integraci jednotlivých bezpečnostních aktivit a informací inženýři systémové bezpečnosti. Systémová bezpečnost je obyčejně provázaná s odpovídajícími inženýrskými, anebo vědeckými disciplínami jako např. inženýrství spolehlivosti, zajištění kvality, lidský faktor apod.

Jaké procesy a úlohy systémové bezpečnosti budou prováděny v konkrétním projektu, závisí na jeho velikosti a úrovni rizika projektovaného systému.

Vždy, když pracujeme s rizikem, ať ho řídíme nebo s ním vyjednáváme, a to v klasickém pojetí nebo v moderním pojetí zaměřeném na bezpečí a udržitelný rozvoj, tak musíme respektovat, že hlavními znaky každého rizika jsou nejistota a neurčitost. Jejich příčiny dělíme na odchylky vznikající při průběhu děje, který je:

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

Nejistota souvisí s rozptylem pozorování a měření. Lze ji do hodnocení a predikce zapracovat pomocí aparátu matematické statistiky. Neurčitost souvisí jak s nedostatkem znalostí a informací o procesu, tak s přirozenou variabilitou procesů a dějů, které vyvolávají pohromy nebo dokonce hrubými chybami. Pro zapracování a zvážení neurčitostí je aparát matematické statistiky nedostatečný a je třeba používat jiný, modernější matematický aparát, který poskytují např. teorie extrémních hodnot, teorie mlhavých množin, teorie fraktálů, teorie dynamického chaosu, vybrané expertní metody a vhodné heuristiky [15].

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

V praxi dnes sledujeme několik typů zranitelnosti. Nejčastěji se jedná o:

1. Zranitelnost systémovou. Ta zohledňuje zranitelnost jako funkci četnosti a závažnosti ohrožení (popř. pravděpodobnosti výskytu) a dopadů pohrom všeho druhu. V konceptu studované zranitelnosti systémů se řeší úkoly v oblasti věd přírodních a technických včetně

věd biofyzikálních (např. zranitelnost v důsledku extrémního počasí a klimatické změny), věd tzv. environmentálních, aplikované ekologie apod.
2. Zranitelnost společenskou. Ta vnímá zranitelnost systému v rovině sociálně-ekonomických ukazatelů např. typu politické svobody a sociální soudržností, prohloubení chudoby a ohrožení lidských práv, napětí mezi blahobytem a bídou, podvýživy a dětské úmrtnosti, zvládání stresu, zdravotních dopadů apod. Její hodnocení je kvalitativní, verbální, opřené o statistické údaje.
3. Zranitelnost kybernetickou. Ta se týká převážně virtuální oblasti rozvoje a propojení nových informačních a komunikačních technologií a především vytvoření infosféry a kyberprostoru jako základny informační společnosti.

3.3. Úvahy o bezpečnosti a nástrojích pro zajištění bezpečnosti technických děl

Inženýrství pružné odolnosti (houževnatosti) je považováno za vynořující se inženýrskou disciplínu, která je spojená s bezpečností [1]. Podle současných znalostí existují pružně odolné systémy, které nejsou bezpečné a bezpečné systémy, které nejsou pružně odolné. Řízení bezpečnosti se stále více orientuje na pružnou odolnost kvůli rostoucím složitostem a propojitelnostem reálných technologických objektů a infrastruktur. Vychází se z konceptu, že je stále obtížnější identifikovat všechna ohrožení a nechtěné nehody, a proto pro zabránění a snížení následků různých poruch je důležitá pružná odolnost.

Šetření selhání a havárií složitých technologických systémů ukazují, že havárie jsou často způsobeny kombinací několika nepravděpodobných nehod a získat schopnost jejich předpovědi znamená najít kombinace nehod, které mají potenciál způsobit havárie doprovázené velkými škodami. Odvrácení výskytu těchto kombinací pak povede ke zvýšení bezpečnosti. Aplikovaný výzkum se proto soustřeďuje na proaktivní indikátory nebo bezpečnostní funkce, s jejichž pomocí lze řídit bezpečnost za hraničních podmínek, a tím snížit možnost výskytu málo pravděpodobné kruté havárie. Používá se sedm principů pružné odolnosti, a to: zálohování; schopnost uhlazené a řízené degradace; schopnost návratu z degradovaného stavu; flexibilita v systému i organizaci; schopnost řídit mezní stavy blízko výkonnostního rozhraní; ustavení a výzkum obvyklých mentálních modelů řízení; redukce složitosti; a redukce vzniku možných nežádoucích spřažení.

Bezpečnost technických systémů není proto jen záležitost technická, je směsicí aspektů bezpečí a spolehlivosti a vysoce souvisí s provozní spolehlivostí technického systému, která se popisuje zkratkami RAMS (Reliability, Availability, Mantainability, Security) nebo ARSS (Availability, Reliability, Safety, Security), přičemž platí:
1. Availability (dostupnost) je schopnost systému poskytovat služby, když se požadují.
2. Reliability (spolehlivost) je schopnost systému fungovat tak, je zamýšleno, tj. plnit úkoly tak, jak mu byly předepsány.
3. Safety (bezpečnost) je schopnost systému fungovat tak, že nepůsobí škodlivě na sebe a na okolí.
4. Security (bezpečí) je schopnost systému ochránit se před nežádoucími vnějšími a vnitřními vlivy.

Zajištění bezpečného systému je výsledkem fungování procesu řízení bezpečnosti (uspořádaného souboru opatření a činností), který je souborem procesů, jež mají pod kontrolou všechny faktory, které by mohly vést ke vzniku škody, ztráty či újmy na systému a jeho okolí. Ze systémového hlediska se bezpečnost skládá z následujících komponent:
1. Informační činnost pro podporu rozhodování, protože stav bezpečí je výsledkem racionálního rozhodování a dobrých informací. Je však třeba počítat s vlivy na rozhodování

o bezpečí jako jsou různá omezení (institucionální, právní, organizační), vlivy medií a veřejného mínění a dimenze politické (zájmové skupiny, ideologie) a technologické.
2. Struktura technického systému, což jsou zařízení, technologie a organizační složky.
3. Lidé jako subjekty bezpečnosti (experti a manažeři bezpečnosti), lidé jako objekty bezpečnosti (ochrana a prevence).
4. Procedury spojující lidi a strukturu.

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

1. Neuvažovat bezpečnost v „kulturní izolaci“, protože tak se bezpečnost stává sebe referenční. Bezpečnost se musí formovat pod vlivem apriorně definovaných rizik.
2. V bezpečnostních studiích je třeba oprostit koncept bezpečnosti od ideologického a politického klišé.
3. V metodice řízení bezpečnosti je třeba dát důraz na rozhodování o řešení problémů a na zvažování přínosů a dopadů konkrétních rozhodnutí, a to z pohledu veřejného zájmu.
4. Stále mít na paměti vztah mezi rizikem a bezpečnosti; obecně nejde o komplementární veličiny [1,10]. Podstata problému je v odpovědích na otázky: Jak se identifikují rizika a jejich škodlivé dopady? Odpověď: Stanovují se věrohodnými scénáři. Ale jak se takový scénář tvoří? Obvykle se scénář odkazuje na minulé události a jevy, a nebere v úvahu porušování pravidel a pátrání po možných překvapeních.

Moderní stát hraje roli, která se dá popsat v termínech řízení rizik, protože přerozděluje určité typy rizik prostřednictvím systému blahobytu / veřejného blaha a zdravotní péče. Rostoucí debaty o riziku na úrovni veřejné správy je možné vysvětlit jako důsledek uvědomění rizik, kvůli nimž může selhat poskytování veřejných služeb. Nadto veřejnost se může při špatně zvládaných krizových a nouzových situacích domnívat, že veřejná správa je zdrojem rizik.

Rizika vstupují do veřejné oblasti, naplňují-li některý z dále uvedených atributů:

1. Jde o externality, které nemohou řešit tržní mechanizmy.
2. V souvislosti s individuálními právy jsou občanům vnucovány škodlivé dopady.
3. Je ohrožena značná část veřejnosti.
4. Politické rozhodnutí vyvolá událost, při které dojde k realizaci rizika.
5. Nežádoucí události, tj. jevy, při kterých se realizují nepřijatelná rizika, jsou rozloženy tak, že neberou ohled na politickou spravedlivost.

Veřejná správa musí zajistit, že rizika jsou analyzována nejen z hlediska společenských dopadů, nýbrž také z hlediska dopadů na systém řízení veřejné správy. Může se totiž stát, že rozhodování veřejné správy může dopady nouzové situace ještě zhoršit. Kroky postupu řízení rizik veřejné správy se liší od běžného postupu řízení jen tím, že se musí věnovat značná pozornost formulaci kontextu a musí se sledovat rizika ze strategických a procesních hledisek, tj.:

1. Ve strategickém kontextu, který se zabývá vztahy mezi institucí veřejné správy a prostředím sledovaným systémově se posuzuje schopnost veřejné správy a ostatních zúčastněných při dosažení strategických cílů v oblasti bezpečnosti, ochrany, mobility a stavu prostředí (zdravotní a environmentální rizika).
2. V organizačním kontextu se posuzuje schopnost instituce, tj. veřejné správy, řešit problémy.
3. V kontextu řízení rizik se posuzuje prahová úroveň rizika, maximální úroveň dopadů a řeší se priority rozhodování.

Řízení území i každého technického či jiného subjektu musí kvůli zajištění udržitelného rozvoje respektovat tzv. strategická rizika a logickým způsobem je řídit. S ohledem na výše uvedené skutečnosti předložená práce zakládá způsob řízení rizik založený na současném

poznání s cílem problémy řešit ve prospěch bezpečí a udržitelného rozvoje lidského systému a jeho chráněných aktiv.

Pro řízení bezpečnosti každého systému mají zásadní důležitost vlastnosti systému jako zranitelnost, pružná odolnost a adaptabilita ke změnám vyvolaným vnitřními i vnějšími pohromami. Zranitelnost je integrální vlastnost systému, která je příčinou toho, že systém se za určitých podmínek nechová žádoucím způsobem, protože je pozměněna, ve smyslu lidského vnímání narušena, jedna nebo více složek z následného seznamu:

- struktura a forma složení prvků systému,
- forma, směr a intenzita vazeb systému,
- forma, směr a intenzita toků systému,
- vytvoření nových či ztráta nebo závažná změna starých interdependences, tj. vazeb napříč systémem a jeho okolím.

Jedná se o dynamickou vlastnost, která se mění v prostoru a čase a jistým způsobem také územně specificky, protože závisí na systému samotném a na podmínkách, do kterých je systém zasazen.

Nejedná se o zcela novou věc, ale o vyšší stupeň poznání reality, protože všem, kteří prováděli nebo provádí při všech druzích hodnocení bezpečnosti (spojených s umísťováním, projektováním, navrhováním, výstavbou a provozem objektů a infrastruktur) syntézy s cílem dosáhnout dlouhodobě funkční a bezpečné objekty a infrastruktury, vždy šlo, jde a i půjde o nalezení přijatelného řešení pro daný případ v podmínkách, které existují v daném místě. Tj. nejdříve hrály roli dílčí zranitelnosti, poté jejich agregace (integrovaná zranitelnost) a dnes kvůli existenci interdependences vycházíme ze systémového hodnocení a snažíme se určit integrální zranitelnost.

Protože dané útvary mají mnoho komponent (často též systémů), které spolu interagují a jsou uspořádané v několika úrovních, což způsobuje, že pozorujeme:

- náhle vynořené rysy chování, které nelze získat ze znalostí o chování komponent, jde o tzv. emergenci (náhlé vynoření),
- hierarchičnost,
- samo organizovanost,
- rozmanité řídící struktury, což vše dohromady připomíná chaos.

Vzájemná provázanost systémů pochopitelně působí závislosti (tzv. interdependences). Proto pochopitelně neplatí, že bezpečnost SoS je agregací bezpečností dílčích systémů; musí se totiž respektovat i průřezová rizika způsobená vazbami a toky napříč SoS a s okolím. Uvedená skutečnost znamená, že dnes používaná integrovaná bezpečnost, která je založená na řízení integrovaného rizika není zcela na místě u daných objektů. Proto musí být postupně nahrazována integrální bezpečností, při které se spoléhá i na řízení průřezových rizik.

3.4. Způsob zajištění bezpečnosti složitých socio-kyber-technických systémů

Nejdříve si je třeba uvědomit, o co jde. Dle [1] požadujeme, aby technická díla a zařízení: fungovala co nejdéle, a to bez závad nebo s jen malým počtem závad; co nejlépe plnila požadované funkce; byla co nejlevnější; spotřebovala co nejméně energie a surovin; neohrožovala ani sebe ani své okolí; a neprodukovala velké množství odpadu, hlavně nebezpečného. Každý systém má strukturu a mechanismus řízení svého chování. Jeho obecné vlastnosti [1,108]:

- koherentnost (změna prvku vyvolá změnu ve všech ostatních prvcích),
- samostatnost (opak koherentnosti, změna prvku nevyvolá změnu ve všech ostatních prvcích),

- kompatibilita (soubor podmínek, za kterých se dva a více systémů mohou podílet na společných činnostech),
- centralizace (dominance jednoho prvku nad ostatními),
- ekvifinalita (schopnost systému dosáhnout cíle z různých výchozích stavů),
- operabilita (soubor podmínek, za kterých je systém bezpečný, spolehlivý a funkční).

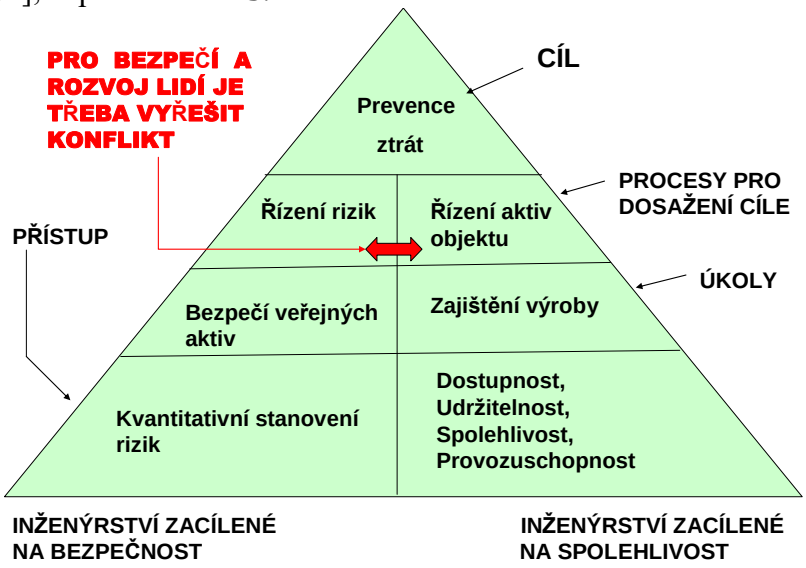
Je skutečností, že sice existuje řada přístupů, norem a standardů, jejichž aplikací se zajišťuje bezpečnost objektů, ale havárie se vyskytují stále, a proto se hledají další účinnější přístupy. Základní požadavky jsou, aby se v technologických objektech a infrastrukturách: používaly systémy inherentní bezpečnosti; řídila průřezová rizika v dynamicky proměnném světě; a aplikoval proces řízení bezpečnosti, který dominuje nad všemi procesy organizačními i technickými, které probíhají v technologickém objektu či infrastruktuře. Poslední požadavek je v souladu s dnešním stylem řízení, kterým je projektové a procesní řízení [1].

3.4.1. Položky řízení bezpečnosti

Řízení bezpečnosti technických děl řeší otázky týkající se materiálu, technologií, konstrukce, výstavby, provozu, personálu, organizace, vzdělávání, financí a práva tak, aby zajistilo žádoucí procesy, které mu přinášejí zisk, zajišťují soulad se státem a konkurenceschopnost, a zároveň potlačilo procesy, které mu přinášejí škody a ztráty.

Ze současného poznání i z výše uvedených faktů vyplývá, že bezpečnost složitých technologických systémů, které představují soubory otevřených a vzájemně se prolínajících systémů uspořádaných tak, aby plnily určité úkoly v oblasti součinnosti (interoperability), závisí především na řízení integrálního rizika, a to hlavně dílčích rizik spojených s vazbami a toky v systému.

Výběr vhodné strategie na zmírňování rizika je tudíž velmi komplexní a kritický úkol. Nejde jen o snížení pravděpodobnosti výskytu selhání, ale také o zlepšení podmínek provozních aktiv, jejichž selhání může vést k velkým provozním nákladům. Nesprávná strategie snižuje produktivitu a výnosnost technologického systému. Výběr strategie zmírňování rizika je proto typický multikriteriální rozhodovací problém. Nejlepší strategie pro řízení rizika se musí vybrat z možných alternativ. Musí být vzato v úvahu množství kritérií, z nichž některá jsou konfliktní [1,5,10,32], např. obrázek 13.



Obr. 13. Příklad základního konfliktu při řízení kritických objektů – sestaveno s uvážením představy v [32].

Aby se zabránilo iniciaci velkých rizik, která při realizaci působí velké ztráty a škody lidem a dalším veřejným i privátním aktivům, tak základním cílem řízení technologických celků není dosáhnout velkého množství výrobků, ale i prevence ztrát na svých i veřejných aktivech, a proto se hledá konsensus mezi řízením rizik a řízením aktiv objektu. Jde o nalezení způsobu, kterým se nevyvolají rizika, která způsobí ztráty a škody na veřejných i privátních aktivech, které budou de facto vyšší než užitky ze zvýšené výroby.

Protože při orientaci na prevenci ztrát dle [32] nejde jen o snížení pravděpodobnosti výskytu selhání, technologického systému, ale také o zlepšení podmínek provozních aktiv, tak SMS (systém řízení bezpečnosti) technologických objektů musí být flexibilní a musí být zacílen na interoperabilitu veřejných a privátních aktiv.

Jak již bylo řečeno, heterogenita a těsná propojení systémů v technologických objektech a infrastrukturách jsou příčinou obtížného popisu a emergentního chování předmětných systémů [1,6,7]. Klasické analytické metody nemají schopnost poskytnout dostatečný pohled kvůli složitosti systémů. K tomu je třeba hluboké porozumění a holistický přístup [1,10,11].

Kromě inherentní složitosti předmětných systémů jsou důležitá jejich propojení, označovaná jako interdependences. Zvláštní význam mají emergentní propojení, která vzniknou jen za specifických podmínek. Právě tyto nepředvídatelné závislosti jsou příčinou kaskádovitých selhání, anebo nežádoucích domino efektů a jiných nežádoucích jevů, které jsou důsledkem různých synergií a kumulací, a které jsou největší hrozbou pro dnešní společnosti.

Modely řízení bezpečnosti složitých technologických objektů a infrastruktur jsou teprve v počátku. Musí mít inherentní charakteristiky jako dynamické nelineární chování, spletitá pravidla interakcí, která jsou výsledkem jejich otevřenosti a vysoké propojitelnosti. Dále musí respektovat mnohaúrovňové vnitřní závislosti a nedostatek rozhraní v požadované: diverzitě podstaty poskytovaných služeb; koexistenci více časových stupnic; a úrovni vyřešení úkolu.

Interoperabilita (vzájemná schopnost spolupráce) dílčích systémů znamená, že dílčí systémy plní zadané úkoly tak, aby systém systémů plnil cíl v požadovaný čas, v požadovaném rozsahu a v požadované kvalitě, a to za normálních, abnormálních i kritických podmínek. To znamená, že chování prvků musí být koordinované a zacílené na určitý cíl, tj. vzájemným sdílením inherentních instrukcí (know-how systému) jsou v prostoro-časové oblasti zajištěny takové součinnosti prvků, kterými se dosáhne cílů. Jde o implicitní schopnost procesního systému (technologie), zajistit nejúčinnější, kvalitní, bezpečný, environmentálně šetrný, ekonomicky efektivní, automatizovaný a integrovaný průběh procesů přes rozhraní různých vnitřních entit a jejich okolí. Cílem je operabilní poskytování vzájemných služeb operačních objektů v souladu s požadavky jeho subjektů ve standardizovaném prostředí. Interoperabilita v kontextu rozsáhlé aplikace je schopnost systému spolupracovat s jinými systémy bez zvláštního úsilí zákazníka / uživatele. Je to schopnost interakce a výměny informací mezi technologickými objekty a jejich informačními systémy jak uvnitř, tak vně objektu. Musí být řešena minimálně ve třech oblastech / úrovních: DATA, APLIKACE, ORGANIZACE [33]. Nejde tedy pouze o problém software a IT, ale i o komunikace, technické a organizační záležitosti.

Omezování rizik v rámci řízení bezpečnosti pokrývá několik okruhů: 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 [34]. Příčiny organizační havárie se hledají ve třech základních aspektech: organizační procesy; podmínky, které působí vznik chyb nebo porušení předpisů; a neřešené problémy, které dovolují chyby a/nebo porušení předpisů. Organizační procesy zahrnují čtyři procesy, které jsou součástí každé technické či technologické organizace: projekce a konstrukce, výstavba, provoz a údržba. Uvedené procesy jsou zabudovány ve třech provázaných činnostech: stanovení cílů v rámci hospodářské a sociální situace podniku; organizace podniku pro splnění stanovených dlouhodobých strategických cílů; a řízení provozních činností.

Podmínky, které působí vznik chyb, jsou: neseznámení s úkolem; nedostatek času; špatný odstup signálu od šumu; neporozumění mezi konstruktérem a uživatelem; nevratnost chyb; zahlcení informacemi; záporný převod mezi úkoly (špatné předání úkolů); špatné vnímání (podcenění) rizika; špatná zpětná vazba ze systému; nezkušenost; špatné pokyny a postupy; nedostatečná kontrola; nevhodné vzdělání osoby s daným úkolem; nepřátelské prostředí; a monotónnost a nuda.

Podmínky, které působí porušení předpisů a pravidel jsou: nedostatek kultury bezpečnosti v organizaci; rozpory mezi řídícími pracovníky a zaměstnanci; špatná morálka; špatný dohled a kontrola; normy tolerující porušování předpisů; špatné vnímání zdrojů rizik; postřehnutelný nedostatek péče a zájmu vedoucích pracovníků; malá hrdost na vlastní práci; machrovský přístup k práci, který povzbuzuje podstupování rizik; víra, že se nemůže nic špatného stát; nízká sebeúcta; poznaná bezmocnost; postřehnutelné povolení pro porušování pravidel; obojaká, dvojsmyslná nebo zjevně nesmyslná pravidla; a věk a pohlaví: mladí muži se dopouštějí porušování pravidel.

Neřešené problémy, které dovolují chyby a porušení předpisů / pravidel jsou:

1. Chyby se dějí jako důsledek problémů v informačních procesech a dají se pochopit ve vztahu k poznávacím funkcím jednotlivce. Dají se minimalizovat školením, zlepšením pracovišť, definicí rozhraní, lepším informováním atd.
2. Porušení předpisů / pravidel jsou založeny na motivaci. Jsou společenským jevem a dají se pochopit jen v souvislostech dané organizace. Porušení se musí odstranit změnou přístupů, přesvědčení, norem, morálky a kultury bezpečnosti.

Na základě šetření velkých havárií [1,12] lze konstatovat, že řada primárních (kauzálních) a sekundárních příčin se u nehod opakuje, ačkoliv existuje poměrně dost znalostí potřebných k prevenci nejen skoro nehod, ale i závažných havárií, ke zmírnění jejich dopadů, a tím ke zmenšení ztrát a škod s nimi spojených. Příčinou daného stavu, kromě lidského činitele, jsou nedostatky jak v zavedení funkčního systému řízení bezpečnosti, tak i neznalost závěrů z již vyšetřovaných nehod a havárií.

Je skutečností, že i v organizacích, v kterých se vyskytly havárie, jsou s postupem času a změnami personálu původní opatření provedená po proběhlé havárii zapomenuta nebo nejsou předána všem pracovníkům v dané organizace. Proto je třeba zavést následující opatření ke zlepšení společné paměti organizace:

1. Připojení poznámky ke každému pokynu, předpisu nebo normě, proč je právě takový.
2. Popis staré i nedávné havárie v podnikovém tisku s poučeními z nich vyplývající, a projednání na školeních o bezpečnosti pro všechny složky podniku.
3. Pravidelná kontrola dodržování vydaných opatření.
4. Odstranění existujících zařízení teprve po poznání, proč bylo instalováno. Zrušení původního postupu po zjištění, proč byl přijat. Je to nutné, aby se neodstranilo něco, co má zabránit havárii nebo má zmírnit její dopady.
5. Zavedení lepšího informačního systému pro nalezení podrobností o haváriích a vydaných doporučeních po havárii.

Po každé nouzové situaci nebo skoro nehodě se proto dělá situační hodnocení:

1. Co se stalo?
2. Byla příčinou pohroma vnitřní vnější nebo lidský faktor? Proč?
3. Jaké zranitelnosti se projevily při nouzové nebo situaci?
4. Jakým způsobem lze zabránit opakování a snížit zranitelnosti (opatření sociální, technická, administrativní, politická, právní, ekonomická)?
5. Mohou opatření sociální, technická, administrativní, politická, právní, ekonomická zvýšit odolnost zařízení vůči pohromě, která vyvolala nouzovou nebo kritickou situaci)? Která z nich to mohou udělat?
6. Jaká jsou doporučení pro implementaci poučení?

Přitom se u předmětného systému dle [1] sleduje robustnost (tj. schopnost systému snést vnější zátěž, aniž by ztratil funkčnost), redundance (tj. míra funkčnosti systému během poruchy), vynalézavost (tj. schopnost systému identifikovat problém a mobilizovat zdroje k jeho odstranění) a rychlost (tj. schopnost systému zabránit budoucím škodám).

Pro bezpečný a spolehlivý provoz složitých socio-kyber-technologických objektů se kodifikují pravidla pro umístění, projektování, výstavbu a provoz. Z inženýrského hlediska se stanovují podmínky a limity provozu, instalují se bezpečnostní systémy (aktivní, pasivní i hybridní) a zajišťuje se jejich vhodné zálohování - řeší se:

- jaké bezpečnostní systémy jsou vhodné a jaké musí být jejich zálohování?
- kde / ve kterých místech bezpečnostní systémy působí nejúčinněji?
- proč jsou použity právě tam a ne jinde?
- v jakých limitech spolehlivě pracují?

přičemž základní strategický přístup pro řízení bezpečnosti je: nic není absolutně bezpečné; i prvky, objekty i sítě mohou selhat dříve nebo později.

Na základě současného pojetí bezpečnosti formulovaného OSN v r. 1994 [20] bezpečnost zahrnuje spolehlivost, tj. bezpečný systém je systém spolehlivý. Přesto do dnešního dne není zodpovězena otázka, kterou položil Scott Sagan [35] v r. 1993, a to „Jsou nehody normální a nevyhnutelné, anebo mohou být bezpečně řízeny kombinací interaktivní složitosti a těsným spřažením?“. Ukázal rozpor mezi koncepty:

- u složitých technologických systémů jsou havárie nevyhnutelné, neodvratitelné, tj. normální [36,37],
- haváriím může být zabráněno dobrým organizačním projektem a řízením, tj. přístup založený na vysoké spolehlivosti, kterou lze stále zvyšovat. Předpokládá se: bezpečnost je primárně organizační cíl; zálohování zvyšuje bezpečnost; decentralizované rozhodování dovoluje promptní a flexibilní odezvy na překvapení; kultura spolehlivosti zvyšuje bezpečnost podpořením jednotné aktivity obsluhy, přičemž se vyžaduje striktní organizace činností; kontinuální akce, výcvik a simulace vytváří a udržují vysokou úroveň spolehlivosti sytému a test a poučení z havárií může být efektivní a může být doplňováno předtuchami a simulacemi

Na základě analýzy havárií [1] je zřejmé, že teorie spolehlivosti nezvažuje fakt, že duplikace a překrytí mohou způsobit, že spolehlivý systém má nespolehlivé části).

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

- řízení a inženýrství spolehlivosti,
- řízení a inženýrství zabezpečení (bezpečnostní),
- řízení a inženýrství bezpečnosti.

Všechny tři uvedené koncepty používají stejné postupy, metody, nástroje i techniky. Praxe ukazuje, že mezi nimi jsou občas konflikty – např. při požáru objektu, který je dobře zabezpečený, lidé v objektu uhořeli; dobře zabezpečená pilotní kabina umožnila Andreasovi navést letadlo plné lidí do svahu Alp a usmrtit je; spolehlivý systém (gilotina) je spolehlivý a z pohledu současného chápaní bezpečnosti [20] není bezpečný, jelikož způsobuje ztrátu života člověka apod.

Konflikty lze řešit reaktivně nebo proaktivně. Koncept integrální bezpečnosti řeší konflikty proaktivně, od počátku projektu, a proto je výhodný pro složitá technologická zařízení a proto se používá u významných zařízení: raketoplány; satelity; ponorky; moderní vojenská letadla apod. [1,12]

Zásady pro integrální bezpečnost sledovaných složitých technologických objektů: v systému řízení bezpečnosti (SMS) skloubit aspekty technické, organizační, právní, finanční, manažerské, sociální, znalostní, vzdělávací, mezinárodní apod.; a v hlavních procesech mít proces pro řízení bezpečnosti – PSM (Proces Safety Management). SMS zahrnuje: organizační

strukturu; odpovědnosti; praktiky; předpisy; a postupy a zdroje pro určování a uplatňování prevence pohrom, včetně lidských chyb, či alespoň zmírnění jejich nepřijatelných dopadů. Používá k tomu tzv. zlatá pravidla, kulturu bezpečnosti a plán řízení prioritních rizik [1,28].

Tvorba a provoz bezpečného systému jsou podstatně náročnější na znalosti, zdroje, síly a prostředky, a proto v běžné praxi jsou používány zabezpečené systémy, které jsou v případě potřeby doplněny organizačními opatřeními, která zajišťují ochranu veřejných aktiv, když předmětné systémy ohrožují sebe a své okolí [1,10].

Zabezpečený systém je chápán jako systém, který je zabezpečen vůči všem vnitřním a vnějším pohromám včetně lidského faktoru, tj. všem škodlivým jevům. Ve srovnání s bezpečným systémem může za svých kritických podmínek ohrozit sebe a své okolí, a proto s ohledem na lidskou bezpečnost může být provozován jen za jistých podmínek [2,20].

3.4.2. Řízení bezpečnosti zabezpečených systémů

Vzhledem k omezeným znalostem a možnostem člověka, jsou běžné objekty vytvořené člověkem zabezpečené v určitém intervalu podmínek; některé z nich jsou bezpečné v určitém (zpravidla užším) intervalu podmínek, když se provedou další (zpravidla nadstandardní) opatření.

Jak bylo výše řečeno, zabezpečené systémy zahrnují běžně používané technologické systémy, které za jistých podmínek mohou poškodit sebe i své okolí. Proto se u nich sleduje vlastnost kritičnost. Stanovení kritičnosti se důsledně vztahuje k velikosti dopadů ztráty funkčnosti každého systému či systému systémů zaměřeném na plnění určitých cílů na společnost [10]. Dle citované práce stanovení kritičnosti v obslužnosti území vychází z analýz ohrožení od pohrom možných v daném území, ze zvážení zranitelností dílčích systémů v území, ze zvážení vzájemných propojení dílčích systémů v území, tj. zranitelnosti celého systému systémů. Při stanovení kritičnosti se zvažují aktiva veřejná, aktiva technologického systému, aktiva území i aktiva státu a používají se otázky:

1. Jak objekt či infrastruktura reaguje na určité typy pohrom?
2. Jak je objekt či infrastruktura masivní, odolná a pružná?
3. Jak se chování objektu či infrastruktury může zlepšit?
4. Jaké jsou vhodné mechanizmy řízení ve smyslu ovládání?
5. Jaká pravidla se mohou využít pro samoregulaci nebo pro přípustné odchylky?
6. Které části objektu či infrastruktury jsou kritické?

Pro zajištění bezpečnosti zahrnující funkčnost, provozní spolehlivost a stabilitu objektu či infrastruktury se pak vyžaduje znalost prahové hodnoty – kritičnosti, která určuje stav, při kterém systém systémů zaměřený na plnění určitých cílů nezajišťuje očekávané funkce v požadovaném čase, místě a v požadované kvalitě. Na základě analýzy významných a nebezpečných poruch a selhání, ztrát a škod způsobených neprovozuschopností funkce, vnějších pohrom, zmírňujících opatření, reakcí a látek v daném zařízení, úniků či vytékání látek (produktovody) apod. se určují pro provoz limity a podmínky [10].

Limity a podmínky jsou pak nástroje pro řízení bezpečnosti těchto technologických zařízení. Jejich dodržování zaručuje bezpečný provoz technologického zařízení. Jsou souborem jednoznačně definovaných podmínek, pro které je prokázáno, že provoz technologického zařízení je bezpečný. Předmětný soubor tvoří údaje o přípustných parametrech, požadavcích na provozuschopnost zařízení, nastavení ochranných systémů, požadavcích na činnost pracovníků a na organizační opatření ke splnění všech definovaných podmínek pro projektované provozní stavy [10].

Pro zajištění bezpečnosti, tj. i spolehlivosti a funkčnosti řídicí systém sledovaného technologického objektu či infrastruktury musí udržovat určené fyzikální veličiny (parametry dílčích systémů) na předem určených hodnotách. V procesu regulace mění řídicí systém

působením na akční veličiny stavy jednotlivých řízených systémů tak, aby bylo dosaženo žádaného stavu celého systému. U řídicího systému se dle pojetí integrální bezpečnosti [10] sledují v prioritním pořadí vlastnosti jako:

- úroveň dodržování stanovených podmínek provozu a nevytváření škodlivých (nepřijatelných) dopadů na samotný systém a na jeho okolí,
- funkčnost (úroveň plnění požadovaných úkonů),
- provozuschopnost, tj. úroveň plnění požadovaných úkonů v závislosti na podmínkách normálních, abnormálních a kritických,
- provozní stálost, tj. úroveň dodržování stanovených podmínek provozu v čase,
- inherentně zabudovaná odolnost vůči možným pohromám.

Z výše uvedeného vyplývá, že řídicí systémy určují kvalitu a výkon (výkonnost) systémů. Mají rozhodující vliv na bezpečnost, a proto se u řídicích systémů 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 [10].

3.5. Způsob zajištění bezpečnosti složitých socio-kyber-technických systémů i jejich okolí

Základem pokrokového řízení bezpečnosti technického díla je vytvoření bezpečného technického díla a programu na zvyšování jeho bezpečnosti pomocí systému řízení bezpečnosti. Předmětný systém řízení bezpečnosti musí zabezpečovat přesně stanovený postup metodické kontroly bezpečnostních aspektů a hodnotit technické dílo ve smyslu identifikování možných zdrojů rizik a předepsání časově i nákladně efektivních nápravných zásahů. Cíle programu technického díla na zvyšování bezpečnosti zajišťují:

- bezpečí a funkce zařízení, které odpovídají jeho poslání,
- identifikaci, vyhodnocení, eliminaci anebo regulování možných rizik na akceptovatelné úrovni u všech zařízení přidružených k systému, podsystému a k jednotlivým částem,
- řízení dopadů od ohrožení, která představují všechny možné pohromy se zdroji uvnitř i vně systému, která nemohou být eliminována, přičemž musí být zajištěna ochrana personálu, lidí v okolí, zařízení a majetku,
- použití nových materiálů, anebo výrobků a testovacích technik jen způsobem, který je spojen jenom s minimálním rizikem,
- včlenění bezpečnostních faktorů již během vzniku systému, tj. minimalizace dočasných, nápravných opatření, která vedou ke zlepšení,
- zvážení všech vhodných historických údajů o zajištění bezpečí, které byly generované podobnými programy na zvyšování bezpečnosti.

Jaké procesy a úlohy systému řízení bezpečnosti se provedou v konkrétním projektu, závisí na jeho velikosti a úrovni rizika projektovaného systému. Všeobecně platí, že bezpečnost a spolehlivost spolu úzce souvisí. Přitom platí, že bezpečné zařízení nebo bezpečný systém musí být spolehlivý, ale spolehlivý systém ještě nemusí být bezpečný. Spolehlivostní inženýrství se přednostně zabývá chybami a redukováním četnosti jejich výskytu. Spolehlivost je definovaná jako charakteristika daného objektu, která je vyjádřená pomocí pravděpodobnosti, že sledovaný

objekt bude vykonávat specifikovaným způsobem funkce, které jsou na něm požadovány během stanoveného časového intervalu a za stanovených resp. předpokládaných podmínek.

Reprezentativními technikami spolehlivostního inženýrství zaměřeného na minimalizaci chyb komponentů (součástek) a tím i chyb komplexních systémů, které byly zapříčiněné chybami komponentů, jsou:

1. Paralelní redundance.
2. Zálohování zařízení.
3. Koeficient a rezerva bezpečnosti.
4. Snižování počtu přetížení.
5. Limitování doby použití.

Uvedené techniky jsou prokazatelně efektivní pro zvýšení spolehlivosti, ale dle výše uvedených fakt bezpečnost nevyhnutelně nezvyšují, ba dokonce za jistých okolností ji mohou redukovat (např. vložení mnoha záloh vytvoří zdroje vnitřních vazeb, tzv. interdependences, přes která se šíří kaskádovitá selhání systémů [10]). Analýzy rizik prováděné u systému řízení bezpečnosti se dívají na interakce a nezaměřují se jen na chyby anebo jistoty inženýrského řešení. Spolehlivostní inženýři často považují spolehlivost a bezpečnost za synonyma. To je pravda jen v některých speciálních případech. Všeobecně má bezpečnost širší / vyšší význam. Běžně mají spolehlivost a bezpečnost mnoho společných vlastností.

Mnohé havárie však nastanou bez toho, že by selhala nějaká komponenta. Právě naopak, častokrát všechny komponenty při haváriích fungovaly podle očekávání a bezchybně [10]. Taktéž se může stát, že komponenty mohou selhat (mít poruchu) bez toho, aby došlo k havárii. Havárie a nehody mohou být zapříčiněny provozem zařízení mimo povolené rozsahy hodnot parametrů nebo časových limitů, z kterých vycházely analýzy bezpečnosti či analýzy spolehlivosti. To znamená, že systém může mít vysokou spolehlivost a přece může dojít k havárii. Navíc, generalizované pravděpodobnosti a analýzy spolehlivosti se nemohou přímo aplikovat na specifické, anebo lokální podmínky. Nejdůležitější je, že havárie a nehody mnohdy nejsou výsledkem jednoduchých kombinací chyb (selhání) komponentů [10].

Orientace na bezpečnost musí být součástí systému řízení podniku při respektování omezení reálného světa. V praxi to znamená zvažovat:

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

Bezpečnost jako vlastnost vystupuje na úrovni systému, když jsou komponenty provozovány společně. Události vedoucí k havárii mohou být složitou kombinací chyby zařízení, nesprávné údržby, problémů informačního a řídicího systému, zásahů člověka a konstrukčních chyb. Analýzy spolehlivosti se zaobírají jen pravděpodobnostmi havárií a nehod souvisejících s chybami. To znamená, že nevyšetřují potenciální škody, které může způsobit správná činnost (provoz) jednotlivých komponentů.

Není tudíž možné, aby spolehlivostní inženýrství nahrazovalo systém řízení bezpečnosti, může ji ale doplnit. Musí to však být provedeno s jasným vědomím, že konečným cílem je zvýšení odolnosti systému vůči nebezpečím spojeným s výskytem náhodných chyb. Je vždy lepší, když se zařízení (systém) navrhuje tak, že individuálně náhodné chyby nemohou způsobit havárii, i kdyby se vyskytly; je si však třeba uvědomit, že to není vždy možné.

Velké opatrnosti je třeba při aplikování technik odhadování spolehlivosti pro posuzování bezpečnosti. Pokud nejsou havárie nevyhnutelně zapříčiněné událostmi, které se dají vyjádřit pravděpodobnostmi, nelze pro ně všeobecně používat míry pravděpodobnosti rizika. Odhady

pravděpodobnosti měří pravděpodobnost náhodných chyb a ne rizik a nehod anebo havárií. Když se při analýzách systému řízení bezpečnosti najde projektová chyba, je daleko účinnější ji odstranit, než někoho přesvědčovat pomocí vypočítaných pravděpodobností, že tato chyba nikdy nezpůsobí havárii. Nízké hodnoty pravděpodobnosti výskytu havárie nezaručují bezpečnost a bezpečnost nevyžaduje mnohdy ultra vysokou spolehlivost zařízení.

Hlavním nedostatkem pravděpodobnostních modelů nejčastěji není to, co zahrnují, ale to, co nezahrnují. Nízké hodnoty pravděpodobnosti jednoduše hovoří o tom, že systém neselže uvažovaným způsobem, ale naopak, selže s daleko vyšší pravděpodobností způsobem, o kterém uvažováno nebylo. Odlišování rizika nehody od chyb je podstatné pro to, abychom porozuměli rozdílu mezi bezpečností a spolehlivostí.

Z praktických důvodů musí být přístupy systému řízení bezpečnosti efektivní a cenově dostupné. Návratnosti nákladů na program systému řízení bezpečnosti se dosáhne tehdy, když se zabrání haváriím. Efektivnost programu na zvyšování bezpečnosti pomocí systému řízení bezpečnosti se prokazuje velmi těžko, protože měřit něco, co se nestalo, je těžké.

Jeden z nepřímých způsobů měření efektivnosti programu na zvyšování bezpečnosti pomocí systému řízení bezpečnosti, byť i ne celkem uspokojivý pro nedostatek porovnávaných faktorů, je porovnávání systémů, které měly program na zvyšování bezpečnosti pomocí systému řízení bezpečnosti s těmi, které ho neměly. Jinou cestou zjišťování efektivnosti programu na zvyšování bezpečnosti pomocí systému řízení bezpečnosti je vykazování nebezpečí, které bylo personálem systému řízení bezpečnosti korigováno ještě předtím, než došlo k havárii, anebo bylo jinak zjištěno.

Třetí cestou odhadování efektivnosti programů na zvyšování bezpečnosti pomocí systému řízení bezpečnosti je zkoumání případů, při kterých nebylo respektované doporučení pro zvyšování bezpečnosti a došlo k haváriím.

Zvýšený tlak na efektivnost a ekonomičnost podnikání se promítá i do systémů řízení bezpečnosti a ochrany zdraví při práci (BOZP). Souhrnně lze vztah bezpečnost (nebo riziko) versus ekonomika vidět ve třech rovinách:

1. Podnikové náklady vynaložené na eliminaci ztrát a škod převyšují náklady na snížení rizika. Úkolem řídících pracovníků (managementu) podniku je nalézt a podpořit prostředky směřující k jejich snížení.
2. Snižování rizik je nákladné z hlediska výsledků analýzy nákladů a ztrát, ale je vyžadováno okolím (veřejností). V daném případě vliv veřejnosti může výrazně ovlivnit výši nákladů do řízení bezpečnosti s cílem zvýšit bezpečí a zajistit udržitelný rozvoj základních veřejných chráněných aktiv.
3. Jedná se o čistě ekonomické náklady na zlepšení pracovních podmínek, které jsou vyžadovány právními předpisy. V daném případě je velmi obtížné nalézt ekonomické stimuly.

Dnes však lidé vyžadují mnohem více než v minulosti, dnes chtějí, aby riziko bylo známé a kontrolované v takové míře, jak jen je to prakticky možné. V podnicích jsou stanovená práva zaměstnanců a spotřebitelů a veřejnost se dozví, s jakými riziky se setkává a kdo je za ně odpovědný.

Posun od čistě osobní odpovědnosti k veřejné, nebo podnikové odpovědnosti za rizika, je převládajícím fenoménem dneška. Na začátku minulého století se od dělníků očekávalo, že: si zabezpečí svoje vlastní nástroje; znají rizika spojená se svou prací; a přejímají odpovědnost za svoje vlastní bezpečí. Zmíněný postoj byl částečně odůvodnitelný skutečností, že pracující věnovali celou svou kariéru výrobě jednoho, nebo dvou produktů. Svoji práci důkladně znali a měli pod kontrolou vše, co souviselo s jejím vykonáváním.

V oblasti bezpečnosti jsou dnes dělníci daleko více závislí na svých zaměstnavatelích, což přirozeně vyvolává přesun odpovědnosti za bezpečnost od pracovníků k zaměstnavatelům. Ve většině průmyslových zemí se od zaměstnavatelů požaduje, aby zabezpečili bezpečné pracovní

prostředí a nutné vybavení a zařízení pro jeho udržování. Navíc, změny zákonů a odpovědnost za jejich plnění vedou k programům bezpečných produktů, které chrání jak pracující při jejich výrobě, tak i spotřebitele.

Je jasné, že pokud jde o riziko, dnešní složitá, technologicky orientovaná společnost požaduje, aby důvěra veřejnosti byla založená na znalostech expertů. V uvedeném smyslu je odpovědnost za detekci a ochranu před nebezpečím přenesená z obyvatelstva na stát, management podniků, inženýry, bezpečnostní experty a na jiné odborníky. Není ale rozumné úplně se vzdát osobní odpovědnosti. V některých případech, jako např. při havárii v chemickém provozu nadnárodní firmy Union Carbide (USA) v Bhópálu (Indie, 1984) se obyvatelstvo při nouzovém plánování a účinném chování při havárii zcela spolehlo na instituce, což mělo tragické následky. Chemická továrna Bhópal Union Carbide byla provozována tak, že bylo jisté, že v ní musí dojít k vážné havárii. Také nouzové plánování, evakuační plán, trénink a pomůcky byly neadekvátní možnému nebezpečí. Okolní obyvatelstvo nebylo varované před možným i vzniklým nebezpečím a nikdo mu neoznámil ani jednoduchá opatření (např. dát si na obličej vlhký šátek), která mohla tehdy zachránit lidem život. Katastrofické havárie předmětného druhu vyburcovaly veřejnost k větší zainteresovanosti v otázkách rizika.

Naopak, zájem veřejnosti u problémů, které minulé generace považovaly za zajištěné, jako např. nebezpečí související se zdravotnictvím, dopravou a průmyslem, vede ke státní regulaci a k vytváření veřejných sdružení pro kontrolu nebezpečí, která byla kdysi tolerovaná.

Na základě současného poznání byl sestaven přehledný model systému řízení bezpečnosti (SMS), obr. 12. Je si třeba uvědomit, že uvedený model SMS platí pro systémy s nepříliš složitou strukturou a s jasně definovanými vztahy a toky mezi elementy systému. I zde však platí, že vzhledem k rozmanitosti systémů, které jsou objektem řízení je nutné každý konkrétní SMS rozpracovat podle konceptu, který respektuje konkrétní strukturu a specifika systému, jímž nahrazujeme objekt, který chceme řídit. Uvedeným konceptem určujeme též, jaká rizika sledujeme a jakým způsobem je zvažujeme, tj. zda rozhodování při řízení provádíme podle výsledků hodnocení rizik dílčích, integrovaných nebo integrálních. Je třeba opět zdůraznit, že pouze integrální rizika zahrnují průřezová rizika, která jsou spojená s vnitřními závislostmi mezi vzájemně propojenými aktivy systémů nebo mezi vzájemně propojenými jednotlivými systémy v případě tzv. systémů systémů (SoS).

Protože svět se dynamicky vyvíjí, je třeba použít pokrokové zásady řízení procesů [38]. Proto byly v citované publikaci navrženy 2 provázané super procesy, které vedou k budování bezpečného světa. Jde o další rozpracování konceptu vyjádřeného modelem zobrazeným na obrázku 6. Obrázek 14 ukazuje soubor provázaných procesů pro vytváření bezpečného území v čase a obrázek 15 ukazuje soubor provázaných procesů pro vytváření bezpečného technického díla v čase.

Pro zajištění bezpečného území a bezpečných veřejných aktiv je třeba použít super proces, který se skládá z pěti procesů (obrázek 14):

1. Proces pro získání dostatečných znalostí o území zahrnuje: stanovení aktiv v území; stanovení parametrů území a charakteristik aktiv v rozsahu územní plánovací dokumentace; a stanovení seznamu pohrom, které mají dopady na území (při jejich identifikaci je třeba vyjít ze seznamu pohrom, uvedeném v [2,5-7], aby nedošlo k zanedbání nějakého významného zdroje rizik).
2. Proces hodnocení rizik a následného řízení rizik zahrnuje: stanovení velikostí ohrožení pro všechny pohromy, které mohou mít dopady v daném území a také period jejich opakování (návratu); stanovení zranitelných míst v území a zranitelnost veřejných aktiv s ohledem na stanovené velikosti ohrožení (způsoby stanovení ohrožení jsou například v [1,5]); stanovení velikostí projektových pohrom (normativně určené velikosti pohrom); stanovení dopadů pohrom na území a jeho sledovaná aktiva (je vhodné určit normativní scénáře dopadů pro projektové pohromy); určení integrálních rizik pro všechny důležité pohromy (tj. zvažovat

jak přímé dopady pohrom, tak nepřímé dopady pohrom na aktiva způsobené prostřednictvím vazeb a spřažení mezi aktivy); práce s riziky.

Obr. 14. Hierarchický soubor provázaných procesů pro zajištění bezpečného území v čase.

Obr. 15. Hierarchický soubor provázaných procesů pro zajištění bezpečného technického díla v čase.

3. Proces hodnocení kvality řízení a vypořádání rizik zahrnuje: posouzení úrovně účinnosti prevence, připravenosti, odezvy a obnovy s ohledem na integrální rizika spojená s důležitými pohromami; stanovení kritických bodů v oblasti řízení a vypořádání rizik a určení jejich kritičností s ohledem na integritu a účinnost aplikovaných opatření a činností a způsob jejich řízení (tj. jde o odhalení zdrojů možných organizačních havárií); návrh korekcí pro vysoce kritické body.

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

Z důvodu dynamického vývoje světa je nutné sledovat území a připravovat postupy pro korekce nepříznivých situací. Z ekonomických důvodů je třeba nejprve použít nejlevnější postup, který naznačuje zpětná vazba 1 na obrázku 14; v případě jeho selhání použít postup naznačený zpětnou vazbou 2 atd.; v případě obrovských škod a ztrát ihned použít postup naznačený zpětnou vazbou 4, což znamená změnu koncepce bezpečnosti území. V každém případě označeném zpětnou vazbou se provádí dále uvedené úpravy procesů:

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

Pro zajištění bezpečného technologického objektu nebo zařízení, které se nachází v reálném území, je nutné aplikovat super proces, který se skládá ze čtyř procesů (obr. 15):

1. Proces umístění stavby, projektování stavby, výstavby a konstrukce technického díla (budovy, zařízení, sítě) zahrnuje: sběr dat o území a jeho aktivech v rozsahu územně plánovací dokumentace; shromáždění dat o pohromách a jejich dopadech, ohroženích a specifikách v daném území (při identifikaci pohrom je třeba vyjít ze seznamu pohrom, uvedeném v [2,5-7], aby nedošlo k zanedbání nějakého významného zdroje rizik; způsoby stanovení ohrožení jsou například v [1,5]; stanovení a posouzení integrálních rizik a stanovení zranitelnosti technického díla nebo zařízení s ohledem na možné pohromy všeho druhu, a to i těch, kterými v případě kritických podmínek technické dílo může poškodit území, ve kterém je umístěn; umístění entity, projektování, výstavba a konstrukce objektů a zařízení s ohledem na odhalená rizika s respektováním principu ochrany do hloubky (Defence-In-Depth) [1]) a vypořádání rizik spojených s vazbami a spřaženími mezi

technickým dílem nebo zařízením a jeho okolím; a stanovení způsobu řízení bezpečnosti technologického celku v průběhu jeho životního cyklu (dokumentace: předběžná bezpečnostní zpráva [1]).

2. Proces přípravy a zahájení trvalého provozu technologického celku (budovy, zařízení, sítě) zahrnuje: zkoušky funkčních schopností jednotlivých budov, vybavení a zařízení a odstranění odhalených zdrojů rizik v oblastech technické a organizační; poloprovoz, během kterého se zjišťují a vypořádávají rizika spojená s vazbami a spřaženími (realizovanými různými toky při provozu), a to uvnitř i vně technického díla; zkušební provoz, během něhož se dále zjišťují a vypořádávají rizika spojená s vazbami a spřaženími (realizovanými různými toky při provozu), a to uvnitř i vně technického díla; realizace návrhu řízení bezpečnosti technického díla (zpracování předprovozní bezpečnostní zpráva a návrh zprávy provozní bezpečnosti [1]); a zahájení trvalého provozu.
3. Proces bezpečného provozu technického díla (budovy, zařízení, sítě během životního cyklu zahrnuje: zavedení provozních postupů pro normální, abnormální a kritické podmínky, kultury bezpečnosti a monitoringu rizik; program pro zvyšování bezpečnosti technického díla v čase a postupy plánu kontinuity pro překonání kritických podmínek (provozní bezpečnostní zpráva [1]); plán optimální údržby budov, vybavení a zařízení a jeho zabezpečení (odpovědnosti, prostředky); plán pro pravidelné prohlídky budov, vybavení a zařízení a pravidel pro provádění včasných oprav zjištěných závad na budovách, vybavení a zařízení, zejména těch, které důležité z bezpečnostních důvodů a jejich zabezpečení (odpovědnosti, prostředky); plán modernizace budov, vybavení a zařízení a plán pravidelných auditů bezpečnosti technického díla a jeho dopadů na okolí (odpovědnosti, prostředky), a to včetně posuzování: úrovně kultury bezpečnosti, úrovně realizace opatření pro zvládnutí zjištěných významných rizik, úrovně odstranění zdrojů organizační havárií; a včasné reakce na kritické situace a zajištění kontinuity provozu technického díla po opravě.
4. Proces ukončení činnosti technického díla (budovy, zařízení, sítě) zahrnuje vyřazení z provozu, odstranění budov a zařízení a předání území pro nové použití zahrnuje: stanovení zdrojů a odpovědnosti za opatření a aktivity, které jsou nezbytné pro odstranění technického díla vyřazeného z provozu (budovy, zařízení a sítě) a sanační práce; odstranění budov, zařízení a sítí z území; provedení dekontaminace území. Jde o proces, na který se často zapomíná v praxi, jak ukazuje spousta brownfields show, a proto, je třeba nezapomínat na předmětný úsek během životního cyklu technického díla.

Z důvodu dynamického vývoje světa je nutné sledovat technologický celek a připravovat postupy pro korekci nepříznivých situací. Je také nutné zvažovat, že každý technologický celek má omezenou životnost, a proto, pro zachování podmínek pro bezpečí a rozvoj lidí je nezbytné předcházet znehodnocení území. Z toho důvodů je třeba připravit postupy a korekce u každého technického díla pro odvrácení nepříznivých situací. Z ekonomických důvodů je třeba nejprve použít nejlevnější postup, který je vyznačený zpětnou vazbou 1 na obrázku 15; v případě jeho selhání použít postup vyznačený zpětnou vazbou 2 atd.; v případě obrovských škod ihned použít zpětnou vazbu 3, která znamená úplnou změnu konceptu bezpečnosti. V každém případě označeném zpětnou vazbou se provádí dále uvedené úpravy procesů:

- v případě použití zpětné vazby 1, se provádí změny v procesu řízení bezpečnosti technického díla jako: změní se požadavky státní správy na provoz technického díla, pravidla pro řízení bezpečnosti technického díla, priority v řízení bezpečnosti technického díla – obrázek 13 ukazuje, že často je nutné vyřešit konflikty mezi bezpečností veřejných aktiv a počet výrobků technického díla atd.),
- v případě použití zpětné vazby 2, se provádí změna procesu přípravy a zahájení trvalého provozu technického díla, např. změní se způsoby řízení a vypořádání rizik a jejich ověření během zkušebního provozu, změní se alokace vypořádaní rizik mezi zaměstnanci, změní se priority v oblasti řízení a vypořádání rizik, změní se systém přidělování prostředků pro

opatření vedoucí ke snížení rizika – např. přestane se spoléhat jen na odezvu a provedou se i preventivní opatření atd.,

- v případě použití zpětné vazby 3, se provádí možné změny v umístění stavby, projektování, výstavbě a konstrukci technického díla, např. jsou zváženy další zdroje rizik, použita další kritéria pro hodnocení rizik, změněny hodnotové stupnice, zváženy další příspěvky k integrálnímu riziku spojené s vazbami a spřaženími mezi aktivy, které byly odhaleny jako zdroje velkých ztrát, škody a újmy na veřejných aktivech atd. Pochopitelně v souladu s pravidly uvedenými v [5] se v daném případě nejprve přehodnotí potřebnost technického díla. Je-li předmětné dílo pro území potřebné, tak se provedou korekční opatření a zavede se monitoring s častějším hodnocením a korigováním rizik.

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

Cílem komplexního řízení je za každé situace zajistit ochranu životů, zdraví a bezpečí lidí, majetku, životního prostředí, infrastruktury a technologií, které jsou nezbytné pro přežití lidí, tj. vždy zajistit mobilizaci a koordinaci využití národních zdrojů (energie, pracovní síly, výrobní schopnost, jídlo a zemědělství, suroviny, telekomunikace aj.), koordinaci činností takových, jako je systém vyrozumění, systém záchrany a zdravotnické služby, které snižují dopady pohrom a také kontinuitu činnosti státní správy a dodržování zákonů. Typy plánování tvořící základní metodické nástroje jednotlivých vzájemně provázaných typů řízení musí vytvářet základnu, ve které jsou výše uvedené cíle zakotvené [2,5].

Pro cíle lidské společnosti, tj. především pro její udržitelný rozvoj se musí vzájemně kombinovat opatření a činnosti na snižování zranitelnosti a na zvyšování pružné odolnosti (resilience) a schopnosti adaptace, které respektují všechny základní chráněné zájmy v jednotlivostech i celku. Současným nástrojem založeným na znalostech a zkušenostech je na všech úrovních řízení implementovat proaktivní systém řízení bezpečnosti, ve kterém se upraví práce s riziky do takové formy, která respektuje všechny chráněné zájmy a bere v úvahu existující a prokázané vnitřní závislosti. S ohledem na současné poznání je třeba provádět a sledovat výzkum vnitřních závislostí, které zprostředkovávají sekundární a další dopady pohrom na životy, zdraví a bezpečí lidí [1,2,5].

Na základě současného poznání a zkušeností musí být svět chápán systémově a pro zajištění bezpečí a rozvoje lidí musí lidská uskupení, tj. obce, kraje, státy a společenství států dobře pracovat s riziky. ***Výhody orientace na řízení rizik procesů*** vedou k:

- lepšímu pochopení a větší integraci,
- nepřetržitému řízení vazeb mezi jednotlivými procesy,
- důrazu: pochopení požadavků a jejich plnění, potřeby zvažovat procesy z hlediska přidané hodnoty, dosahování zvýšení výkonosti a efektivnosti, a na neustálé zlepšování procesů na základě jejich výkonosti.

Veřejná správa určuje úroveň bezpečnosti i v případě privátních subjektů [1,2], protože odpovídá za právní a správní předpisy, politické koncepce a praktická opatření a za jejich vynucení od občanů, vlastníků apod. K danému cíli musí: pravidelně přezkoumávat a aktualizovat předpisy; monitorovat právnické a fyzické osoby i občany v komunitě s cílem zajistit, aby jejich přístup k rizikům byl správný; zajistit účinnou spolupráci a koordinaci všech zúčastněných v komunitě a pro tento cíl jejich otevřenou a účinnou komunikaci; znát rizika v komunitě a zajistit vhodné nouzové plánování; a připravit a být schopna realizovat účinnou odezvu a obnovu. Z uvedeného je zřejmé, že veřejná správa: vytyčuje obecné cíle bezpečnosti

v komunitě; stanovuje jasný a promyšlený systém dozoru, vhodný systém inspekcí i systém pro vynucení požadavků.

Pro zajištění bezpečnosti sledovaných objektů a zařízení je dle [1,10,11] třeba: 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; aplikovat opatření pro ochranu; periodicky kontrolovat stav; udržovat ochranu na odpovídající úrovni; a revidovat opatření v závislosti na vývoji. Úkoly má: vlastník; veřejná správa; bezpečnostní složky; i občané dle [10].

3.6. Rizika technických děl spojená s automatizací

Řízení každé entity dělíme dle rozsahu odpovědnosti, rozhodování a délky plánovacího horizontu. Každá entita plánuje a řídí své aktivity a procesy celkem na třech úrovních: strategická (vrcholová, dlouhodobá), taktická (střednědobá) a provozní (operativní, krátkodobá), přičemž hranice mezi jednotlivými vrstvami nejsou pevné a ostré. V současné době se používá procesní a projektové řízení. V obecném smyslu rozumíme řízením usměrňování procesů nebo činností, které probíhají v určitém dynamickém systému. 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 praxi se odlišují ovládání, regulace a vyšší formy řízení (optimální a adaptivní řízení, učení a umělá inteligence).

3.6.1. Informační technologie

Informace, informační systémy a technologie zahrnují velmi širokou oblast, která vytváří vazby mezi systémy. Informace dnes řadíme vedle materiálových, energetických a finančních zdrojů k hlavním faktorům podmiňujícím pokrok nejen v technice, ale ve všech oborech lidské činnosti [39]. Informační toky v systémech vytváří důležitá propojení a spřažení prvků i celých systémů v komplexních technologických objektech [1,11]. Bez jisté míry informace totiž není možné vytvářet a řídit procesy jakékoliv povahy.

Pro účely předložené práce se v oblasti informačních systémů a technologií zaměříme především na informační systémy procesního typu [39] a tzv. kyber-fyzické systémy [40,41], které jsou v současnosti neoddělitelnou částí pro řízení technologických celků, tak jako je například předmětný systém řízení metra. Informační systémy procesního typu jsou dle [40] určeny k řízení technologických procesů. Uvedeme příklad procesů pro řízení městské kolejové dopravy. Kyber-fyzické systémy představují množinu technologií a jejich vazeb s fyzickými vlastnostmi ovlivnitelnými vnějším fyzikálním prostředím, které jsou určené pro práci s informacemi v kybernetickém (informačním) prostředí [40,41].

Informační systém vyobrazuje pozorované vlastnosti objektu prostřednictvím jazyka a může sloužit k tvorbě informace o pozorovaném objektu. Proces vzniku informace, informačního systému, nového objektu či modifikace originálního objektu je dle [39] složen z následujících podprocesů respektive množin a jejich vazeb popsaných v tabulce 1.

Tabulka 1. Proces vzniku informace dle [39].

	Proces / množina	**Dotčené abstraktní uzly**	**Použité informační technologie**	**Vstupy procesu**	**Výstupy procesu**
1	Identifikace objektu	objekt, pozorovatel	fyzikální receptory (senzory, čidla)	pozorované stavové (fyzikální) veličiny na objektu	signály
2	Vyjádření pozorování	pozorovatel, jazyk (syntaxe)	vzorkování, kvantování, kódování	signály	data
3	Komunikace mezi zdrojem a příjemcem zprávy	jazyk (pozorovatele resp. systému sběru dat), příjemce zprávy	telekomunikační, přenosové a sdělovací systémy	data	data
4	Interpretační množina, vznik informace.	jazyk (pozorovatele resp. Systému sběru dat, příjemce zprávy), množina informací	ontologie, jazyk	data	informace
5	Relace funkcí a strukturální uspořádanosti objektu, verifikace integrity	Informace, objekt	akční člen systému, akční informační systém	objekt, informace	správnost informace, změna objektu
6	Množina informací v množině informačních systémů	informační systémy	informační systémy	informace	informace
7	Interpretační proces	Onformace, objekt 2	signalizační a zobrazovací technologie, umělá inteligence	informace	obraz objektu, nový objekt

Proces vzniku informačního obrazu lze také vyjádřit pomocí Freggeho funkcionálního konceptu vzniku informačního obrazu [39], který je složen z množin: $\boldsymbol{O_i}$ – množina stavových veličin na objektu; $\boldsymbol{P_i}$ – množina stavů (pozorovatelů); $\boldsymbol{\Phi_i}$ – množina syntaktických řetězců (tok dat); $\boldsymbol{I_i}$ – množiny informačních obrazů stavových veličin, a jejich vztahů, které zahrnují: ***aOP*** – identifikace, ***aPO*** – invazivita (schopnost pronikat do systému), ***aPΦ*** – projekce v množině symbolů a syntaktických řetězců, ***aΦP*** – korekce a identifikace neurčitelnosti, ***aΦI*** – interpretace, vznik informace, ***aIΦ*** – reflexe jazykových konstruktů, ***aIO*** – relace funkčních a strukturální uspořádání, ***aOI*** – verifikace integrity.

Mezi Freggeho funkcionálním konceptem a údaji v tabulce 1 lze rozpoznat shodné prvky a dle zdroje [39] lze odvodit vztah mezi daty a informacemi. Data jsou získané údaje o stavu objektu a informace jsou poznatky získané jistým způsobem z dat.

Pro praxi je důležité ocenit velikost či míru informace. Míru informace dle [39] charakterizujeme nejčastěji Hartleyovou mírou informace pro binární systém symbolů (tj. pro většinu současných kyber-fyzických systémů). Vyjadřujeme ji vztahem:

$$\boldsymbol{I = \frac{1}{ln(2)} \cdot ln(N)}$$

ve kterém N reprezentuje počet možných dat:

$$\boldsymbol{N = S^n}$$

ve kterém $\boldsymbol{S}$ je počet znaků v abecedě $\boldsymbol{A\ (A_1,A_2,\ldots\ A_S)}$ a $\boldsymbol{n}$ je počet prvků v množině znaků. Znalost dle [39] je interpretovaná informace, interpretace kauzálních řetězců a citlivostí na množinách neurčitostí, informačních obrazů stavů a přechodů v systémových vazbách objektů reálného světa.

Procesní informační systémy charakterizujeme dle [37] grafy přiřazenými relacím:

$$\boldsymbol{I_i \sim F[P(t), \Phi(t)]},$$

ve kterém $\boldsymbol{t}$ je čas a $\boldsymbol{i = 1,2,\ldots, n}$.

Předmětné přiřazení umožňuje strukturální interpretaci složitých informačních systémů, hodnocení zpětných vazeb a kvalitu převozu a zpracování informace v dílčích informačních systémech [39] a jeho informační segment vychází z maticového vyjádření:

$$\underbrace{\begin{pmatrix} \boldsymbol{I_2} \\ \boldsymbol{\Phi_2} \end{pmatrix} \approx \begin{pmatrix} \boldsymbol{t_a t_b} \\ \boldsymbol{t_c t_d} \end{pmatrix} \approx \begin{pmatrix} \boldsymbol{I_1} \\ \boldsymbol{\Phi_1} \end{pmatrix}}_{[\boldsymbol{T_i}]}$$

ve kterém $\boldsymbol{T_i}$ je přenosová matice i-tého informačního segmentu (tj. segmentu informačního výkonu).

Informační výkon, tj. míra pro hodnocení efektivity informačního je vyjádřena vztahem

$$\boldsymbol{P_i(t) = I_i(t)\Phi_i(t),}$$

ve kterém $\boldsymbol{P_i\ (t)}$ je okamžitý informační výkon. Informační výkon $\boldsymbol{P}$ potom vyjadřuje přeložený-dekódovaná obsah zprávy $\boldsymbol{I}$ v informačním toku $\boldsymbol{\Phi}$. Informační výkon je také roven velikosti míry odstraněné neurčitosti $\boldsymbol{E}$ za jednotku času [39].

S informačním výkonem souvisí i pravděpodobnost správného výběru varianty řešení, pravděpodobnost správného rozhodnutí v provozu řízení systému $\boldsymbol{PCD}$ [39].

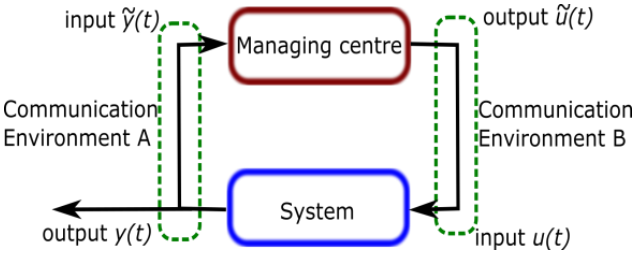
$$\boldsymbol{PCD = F[\Phi(t), k]}\ ,$$

kde $\boldsymbol{k}$ označuje úroveň znalostí ve funkci. Ze vztahu (6) plyne, že se řídicí systém s vyšší úrovní znalostí rozhoduje rychleji [39].

U složitějších systémů vzhledem k nehomogenitě typů informací (počet, obsah, správnost, validita) nelze informační výkon jednoznačně kvantifikovat. Je nutné jej zvyšovat tak, aby byla zajištěná co nejvyšší kvalita vykonávaných funkcí řízeného systému.

Pro zvyšování informačního výkonu a minimalizaci prostředků, které jsou zapotřebí pro jeho vytvoření, se používají různé metodiky. Jsou jimi, např. COBIT z hlediska vrcholového managementu a auditu informačních technologií [42,43], ITIL pro management informačních technologií [42] nebo refraktoring [43], tj. změny v softwarovém systému, které nemají vliv na vnější chování informačního systému, ale vylepšují jeho vnitřní strukturu.

Vzhledem k povaze řešeného úkolu v předložené práci, tj. distribuovaného dopravního systému s geograficky od sebe vzdálenými systémovými uzly, je vhodné uvést vztahy popisující kvalitu přenosu informace v přenosovém prostředí (3. proces dle tabulky 1). Uvažujme proto řídicí systém se zpětnou vazbou vyjádřený obrázkem 16 v souladu s [41,43].

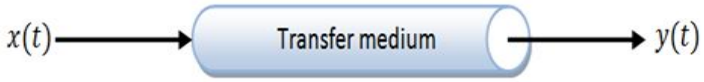


Obr. 16. Vazby v kybernetickém systému.

Kvalita funkcionality uvedeného kybernetického systému je tedy ovlivněna dvěma základními faktory [41]:

- správným chováním systému a řídicího centra,
- korektním přenosem dat mezi uzly kybernetického systému.

Pro exaktní matematický popis obou faktorů, tj. individuálního komunikačního kanálu a celého kybernetického systému, použijeme model Gaussova přenosového kanálu [43] a Bayesovu teorii (podmíněnou teorii pravděpodobnosti) [44], dle obrázku 17.



Obr. 17. Gaussův přenosový kanál [44].

Pro komunikační kanál bez paměti (bez ohledu na výstup v čase menším než je bod t) platí vztah:

$$\boldsymbol{p\big(y(t) \vee x(t)\big)}.$$

Pro komunikační kanál s pamětí (např. kanál se zpětnou vazbou), s daty do času $\boldsymbol{M}$, platí vztah:

$$\boldsymbol{p\big(y(t) \vee y(t-1), y(t-2), \ldots, y(t-M), x(t)\big)}$$

pro data v okolí bodu $\boldsymbol{M}$.

Pro kybernetický systém popsaný na obrázku 16 s parametry $\boldsymbol{\Theta = \{\theta, \theta_2, \ldots, \theta_N\}}$ je možné odvodit následující vztahy

- systém:

$$\boldsymbol{p(y(t) \vee y(t-1),\ldots,y(t-M),u(t),\ldots,u(t-M),\Theta)},$$

- řídicí centrum:

$$\boldsymbol{p\big(u(t) \vee y(t-1),\ldots,y(t-M),u(t-1),\ldots,u(t-M)\big)},$$

- komunikační prostředí A:

$$\boldsymbol{p\big(y(t) \vee y(t)\big),p\big(y(t) \vee y(t)\big)},$$

- komunikační prostředí B:

$$\boldsymbol{p\big(u(t) \vee u(t)\big),p\big(u(t) \vee u(t)\big)}.$$

Z pohledu praxe zvyšování informačního výkonu, a to zvláště v případě kritické infrastruktury se nesmí narušit zabezpečení systému a u zvlášť důležitých položek se musí zaručit bezpečný systém. Bezpečnost socio-kyber-technologických systémů je soubor opatření a činností, které zabezpečují všechny informace a informační toky v systému tak, aby mohl řízený systém vykonávat své funkce bezpečně, tj. aby ani při svých kritických stavech způsobených poruchami neohrozil sám sebe ani své okolí. Proces zabezpečení informací spočívá v ochraně důležitých aktiv kybernetického (informačního) systému tak, aby byla pro důležité informace zajištěna požadovaná úroveň dostupnosti, integrity a důvěrnosti [41,45].

- dostupnost znamená přístupnost a použitelnost informace na žádost oprávněné entity,
- integrita znamená přesnost a úplnost informace,
- důvěrnost znamená, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.

Předmětné požadavky jsou často konfliktní, např. zajištěním důvěrnosti snižujeme dostupnost a integritu a také časové nároky na kódování a dekódování, přenos, autentizaci apod. [41,45]. U procesních informačních systémů v dopravě převládají především požadavky na dostupnost a integritu, kdežto důvěrnost nemá tak velkou prioritu [41,45].

Pro zajištění vysoké bezpečnosti, tj. vysokého informačního výkonu a zabezpečení kybernetických systémů se aplikují přístupy procesního a projektového řízení typu TQM (Total Quality Management) [46], ze kterých vychází používané metody i mezinárodní a evropské standardy pro systémy řízení [45]. Účelem výstavby systémů řízení je najít ekonomicky efektivní procesy, které zajišťují jistou míru bezpečnosti a zabezpečení kyber-fyzických systémů, a to je sledováno ve všech fázích, tj. od návrhu, přes analýzu a vývoj, konstrukci, provoz, modernizaci až likvidaci [41].

3.6.2. Automatické řízení

Automatické řízení se obvykle dělí na logické, spojité, diskrétní a fuzzy řízení. Při jeho aplikaci se nejčastěji používají rozdělení pravděpodobnosti: normální, log-normální, Weibullovo a Gamma. Používá se teorie Markových procesů, Kolmogorovy rovnice a další [10]. V teorii automatického řízení je zdůrazněn význam systémového přístupu k řešení automatizačních úloh a praxe vyžaduje kvantum znalostí z oblasti informačních technologií [47]. Stále více je automatické řízení realizované pomocí kybernetických sítí propojených přes internet. Jelikož pro internet je charakteristická anonymita uživatelů, globální dostupnost a

souběžné používání mnoha různých technologií, je zabezpečení informačních systémů připojených k internetu dosti obtížné.

Na základě prací [48-52] 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.

Na základě představy o propojení řídicího a řízeného systému v [10] je zřejmé, že základní význam v automatickém řízení mají zpětné vazby, na jejichž základě řídicí systémy upravují činnost celého technického díla podle informací z řízených systémů. Kladné zpětné vazby podporují výsledky řízených procesů a záporné je naopak oslabují. Řídicí systémy mají algoritmy, které udělují příkazy a spouštějí některé operace. Řídicí systém zajišťuje, že určené fyzikální veličiny se udržují na předem určených hodnotách. V procesu regulace mění řídicí systém působením na akční veličiny stav řízeného systému tak, aby bylo dosaženo žádaného stavu.

U řídicího systému se dle recentních pojetí, které klade nejvyšší důraz na bezpečnost: V prioritním pořadí se sledují vlastnosti jako: bezpečnost (úroveň dodržování stanovených podmínek provozu a nevytváření škodlivých (nepřijatelných) dopadů na samotný systém a na jeho okolí); funkčnost (úroveň plnění požadovaných úkonů); provozuschopnost (úroveň plnění požadovaných úkonů v závislosti na podmínkách normálních, abnormálních a kritických); provozní stálost (úroveň dodržování stanovených podmínek provozu v čase); a inherentně zabudovaná odolnost vůči možným pohromám.

Řízeným systémem je většinou složitý nelineární systém, který: je tvořen konečným počtem prvků; každý z prvků je jednoznačně popsán konečným počtem měřitelných veličin; vzájemné vazby mezi prvky jsou jednoznačně formulovány. Dynamické vlastnosti řízeného systému můžeme popsat pomocí diferenciálních rovnic, jejichž řešením je stavový vektor. Stavový vektor umožňuje pomocí minimálního počtu veličin určit stav systému v libovolném časovém okamžiku [10].

Pokud není možné kompletně eliminovat zdroj rizika, což platí např. pro živelní pohromy, je dalším nejlepším výběrem ochrana před dopady spojenými s realizací rizika, a to minimalizováním vzniku realizace rizika způsobem, že se příslušná bezpečnostní ochranná opatření (bezpečnostní systémy – Safety Systems) přímo zabudují jak do projektu zařízení, tak i do podmínek provozu projektovaného zařízení, tj. zajišťují bezpečnost. Dalšími v akceptovatelném pořádku priorit jsou zařízení na zvládnutí nebezpečí a na zmírnění jejich dopadů (systémy spojené s bezpečností – Safety Related Systems), které mají jen ochranné funkce. Jsou to např. pojistné ventily, které chrání před nedovoleným přetlakem v případech, ve kterých se nedovolenému zvýšenému tlaku v zařízení nedá úplně zabránit [1,10].

Bezpečnostní systémy jsou konstruované jako pasivní anebo aktivní. Nejefektivnějšími bezpečnostními zařízeními jsou zařízení pasivní, která fungují na bázi fyzikálních principů (např. gravitace) a pro uvedení do činnosti nepotřebují žádný přidaný impuls. Příkladem pasivního bezpečnostního systému je železniční semafor, jehož rameno automaticky spadne do polohy „stop“ vždy, když se přeruší ovládací proud v přívodním kabelu.

Aktivní bezpečnostní zařízení / systémy jsou méně vhodné, protože pro jejich aktivaci pro zabránění havárie anebo zmírnění jejich dopadů jsou potřebné zvláštní iniciační impulsy. Jejich vytvoření zahrnuje detekci nebezpečí a rozpoznání odpovídající bezpečnostní procedury. Příkladem aktivního bezpečnostního systému může být detektor kouře propojený se sprchovým systémem.

Současné technické poznání dovoluje používat hybridní bezpečnostní systémy, které se samostatně vypínají, když podmínky nejsou v rozsahu podmínek stanovených pro provoz aktivních systémů; příkladem jsou ochrany důležitých objektů před velkými zemětřeseními známé z Japonska, Nového Zélandu a z dalších seismicky aktivních oblastí [1,10].

Systém řízení bezpečnosti musí být vždy vybaven opatřeními pro minimalizování škod v případech, že bezpečnostní opatření a bezpečnostní 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 [2].

Správné porozumění určité problémové oblasti vyžaduje pochopení její historie, vědeckého základu, kulturního a sociálního prostředí, ve kterém byla vyvinutá a ve kterém se využívá. Systém řízení bezpečnosti má svoje kořeny v inženýrství průmyslové bezpečnosti, která se krok za krokem rozvíjí už od 19. století. Relativně nová disciplína zabývající se systémem řízení bezpečnosti (nebo v českém inženýrském slangu systémovou bezpečností) je odpovědí na podmínky, které vznikly po 2. světové válce, když se vyvinuly její "rodičovské" disciplíny, a to systémové inženýrství a systémová analýza, které se vyvinuly pro řešení nových a komplexních inženýrských problémů. Vědecká báze všech těchto nových proudů inženýrství spočívá v teorii systémů, jejíž vývoj začal v třicátých letech minulého století [11].

3.6.3. Chyby při řízení technických zařízení

U každého řízení technického procesu je důležité provést včas správné rozhodnutí. Lacko v práci [53] ukazuje, že k tomu je potřeba, aby osoba, která rozhoduje, měla dovednost, kterou označuje situační povědomí (situation awareness). Endsley ve svém příspěvku [54] vymezuje situační povědomí pro oblast lidských faktorů v letecké dopravě a zároveň uvádí vlastnosti dobrého situačního povědomí: správnost – podrobnost – předvídatelnost. Pro získání předmětné dovednosti je třeba umět:

- pozorovat aktuální stav významných prvků a procesů,
- sestavit kompletní obraz systému na příslušné odborné úrovni,
- vytvořit předpověď budoucího chování systému.

Předmětné umění vyžaduje kreativní systémové myšlení a jistou předvídavost. Řidiči osobních aut, piloti v klasických stíhacích letounech, vojenští velitelé ve válce, hasiči v běžných zásazích při požáru, apod. získávají předmětnou dovednost zkušenostmi na základě svého intelektu. Pochopitelně při automatickém řízení předmětná dovednost musí být inherentní pro automat, tj. řídicí systém.

Je si třeba uvědomit, že při rozhodování složitých problémů, osoba, která rozhoduje, nemá možnost získat samostatně odborný přehled a je odkázaná na informace z přístrojů. Má k dispozici záznamy z automatických technických prostředků (sonary, radary, termokamery, infradalekohledy či jiná speciální čidla; čidla jsou napojená na obrazovkové displeje, které zobrazují momentální situaci přehledovým způsobem, a na počítače, které mají programy pro mapování přehledové situace). Příkladem jsou automatizované systémy řízení rozsáhlých různých výrobních systémů (rafinerie, různé druhy chemický výrob, elektrárny, výrobní nebo montážní linky ve strojírenském nebo elektrotechnickém průmyslu, pivovary, cukrovary, papírny, systémy řízení dopravy velkých měst, monitorování provozu v dlouhých dálničních tunelech, řízení leteckého provozu v určitých regionech nebo na velkých letištích, apod.).

V uvedených případech si pracovníci vytvářejí přehled o situaci ve velínech prostřednictvím obrazovek automatizovaných počítačových systémů. Proto je důležité, aby informace získané tímto způsobem byly věrohodné a uspořádané tak, aby navedly osobu, která rozhoduje ke

správnému řešení, tj. vytvořily její správné situační povědomí. Zde vysokou roli hraje vzdělání, zkušenosti a odpovědnost za kvalitně provedenou práci. Převádíme-li rozhodování složitých problémů na automaty, tak jim musíme vložit inherentní algoritmy, které mají schopnost i zde nahradit člověka. Jelikož důvěra v současné schopnosti automatů není bezmezná, tak kritické rozhodnutí se nechává na týmu lidí, jak ukazují např. provozní předpisy v jaderných elektrárnách, převzetí ručního řízení letadla za kritických podmínek apod. [12].

Autor práce [53] shrnuje požadavky pro:

- prostředky, které zajistí pohotové reakce operátorů v provozu,
- účelové uspořádání prostředků,
- a způsob výchovy operátorů.

Uvádí též chyby, které přispívají k vytváření nedostatečného, anebo špatného situačního povědomí. Jejich doplnění podle poznatků shromážděných v [12 ukazuje, že jde o:

1. Chyby v analýze zainteresovaných stran, tj. stran, které jsou dotčeny činností daného subjektu; předmětná analýza je chybná nebo chybí. Např. se zvažují jen nebezpečí, která hrozí z různých technickoorganizačních, materiálových a konstrukčních příčin, ale ignorují se nebezpečí, které hrozí ze strany konkurenčních firem, dotčených výstupem firemního projektu nebo jeho realizací. Pro každé rozhodnutí je třeba si uvědomit celé řetězce vzniklých nebezpečí a následné škody, a přitom se nelze omezit jen na primární škody při různých haváriích, ale i na následné dopady na lidi, životní prostředí, ekonomické zázemí území apod..
2. Neodstranění tzv. „tunelové vidění“. Tunelové vidění znamená, že osoba, provádějící rozhodnutí se soustředí jen na jednu věc a ignoruje ostatní důležité souvislosti. Slavný německý stíhač 1. světové války Oswald Boelcke (jeden z průkopníků letecké taktiky) zpozoroval, že útočící pilot je velmi zranitelný, neboť vlivem koncentrace na protivníka a složitosti prováděných manévrů ztrácí přehled o dění kolem sebe. Doporučil proto systém navzájem se kryjících dvojic, který se praktikuje ve stíhacím letectvu na celém světě dodnes [55]. Tunelové vidění ve firemní praxi lze přirovnat k situaci, kdy se vrcholové vedení zaměří na dodržení co nejkratšího termínu uvedení nového výrobku na trh, aby eliminovalo riziko, že firmu konkurence předběhne, ale ignoruje kontrolu dodržování nákladů a kvalitu řešení. Výrobek je sice na trh dodán, ale se spoustou chyb, takže se obtížně prodává a v minimálním množství, přičemž překročené náklady jsou enormně vysoké [53], což může vést až k zániku firmy.
3. Nezabrání se rozhodování ve stresu. Tj. nevyžaduje se příprava řešení možných situací předem. Časová tíseň je situace, v níž je člověk nucen aplikovat rychlé rozhodování a jednání v závažných věcech, aniž by měl dostatek času si své jednání promyslet a připravit. Dovoluje se rozhodovat bez dostatečné přípravy a časových rezerv (vykrývajících případná dílčí selhání v synchronizaci jednotlivých kroků) zásadní akce, často i s nedostatečnými zdroji (neboť není dost času zmobilizovat dostupné rezervy) a pouze s dílčími a s neověřenými informacemi. Časová tíseň z tohoto důvodu prudce zvyšuje pravděpodobnost drobných i závažných chyb a selhání. Problematika časové tísně je velmi dobře známá všem šachistům - ti, co vynikají v rychlém rozhodování, si mohou dovolit hrát bleskový šach, ale obecně kvalita bleskových partií je podstatně nižší než klasicky hraných šachových partií, kde je na tah zaručen pravidly přijatelný časový limit [53].
4. Podceňování zajištění informovanosti týmu. Ignorance vypracování situačního povědomí týmu vede ke ztrátě systémového a interdisciplinárního pohledu. Ve firemních akcích a firemních projektech komplexního charakteru je třeba vždy využít týmové práce (platí rčení: „Více hlav, více ví!“). Interdisciplinárně složený tým různých odborníků a profesí snadněji realizuje systémový pohled na reprezentativní množinu nebezpečí. Týmová práce podporuje kreativitu, která je velmi důležitá zejména v případě práce projektových týmů. Zkušený odborník navíc upozorní na nebezpečí, které ostatním nemusí přijít vůbec na mysl.

Ve firemní praxi se vyskytuje mnoho všelijakých úskalí finančních, právnických, sociálních, interkulturních apod., kterým je nutno věnovat náležitou pozornost, aby se nevyskytly jevy vedoucí ke ztrátám (viz kultura bezpečnosti).

5. Nedocenění a přehlížení poučení z chyb. Vyhodnocení chyb plynoucích z nedostatečného situačního povědomí, které bylo příčinou špatného rozhodnutí, které způsobilo ztráty a škody, není děláno z různých důvodů (nedostatek času, opomenutí, podcenění situace, ignorování potřeby udělat vyhodnocení situačního povědomí apod.), což se následně ukáže jako zásadní, fatální chyba. Dle [53] platí, že považovat vyhodnocení situace za zbytečnost se prostě nevyplácí!
6. Ignoranci známých skutečností, tj. vytváří se tzv. "slepý prostor" [53]. Skoro každý uchazeč o řidičský průkaz byl již v autoškole seznámen s úskalím, spoléhat se výhradně na letmý pohled do levého zpětného zrcátka, a byl mu demonstrován „slepý úhel“, který se na něm projevuje. Dle [53] jde v podnikové praxi např. o necitlivosti měřidel v určitých rozsazích, kterými se zjišťuje stav řízeného procesu, vůle v ovládacích mechanizmech, nesledování některých účetních položek, časové zpožďování důležitých hlášení apod.
7. Netřídí se informace, což vede k přehlcení informacemi; tzv. přetížení vstupu. Jde o opačný problém, než je nedostatek informací, ale brání také kvalitnímu rozhodnutí. Množství informací není možno rozumně zpracovat tak, aby rozhodnutí bylo kvalitní v požadované době. K řešení problému je potřeba zorganizovat racionální „předzpracování“ a filtraci dat, nebo jejich racionální zobrazení tak, aby byla možná rychlá a správná orientace v problému. Zde pomáhá velmi účinně efektivní využívání automatizace s využitím počítačů.
8. Zanedbává se doplňování znalostí a provádění korekcí situačního povědomí, aby situační povědomí stále odpovídalo aktuálním podmínkám. Dle [53] stejně jako se mění aktuální situace, musíme pružně přehodnocovat případná nebezpečí podle aktuální situace. Proto je důležité v rámci firmy správně nastavit monitorování rizik, které vede např. k tomu, že jsou včas prováděny opravy, údržba a výměny, aby nedošlo k zastarání technologie [56].
9. Dovoluje se aplikace chybného modelu rozhodování. Jde např. o podporu řešení úkolu, založenou na software, které je založeno na modelu, který nezohledňuje možné reálné podmínky (např. software pro vydávání registračních značek aut zavedené v r. 2014 [12].
10. Nezvažuje se přetěžování klíčových zaměstnanců.
11. Nedbá se na pracovní podmínky zaměstnanců.
12. Nepřipravují se postupy na zvládání nouzových situací a povědomí o nich u všech zaměstnanců.

Výčet pochybení není úplný a v konkrétních situacích se mohou objevit další. Často se také vyskytuje i několik pochybení současně, což se často odhaluje při inspekcích po haváriích [12].

3.6.4. Rostoucí role vzdělávání ve světě smart technologií

Rozšíření chytrých mobilů a smart technologií zvyšuje dostupnost informací, a tím usnadňuje na jedné straně rozhodování. Na druhé straně však vede k hloupnutí populace, protože snižuje u lidí jejich schopnosti provádět správné hodnocení pomocí kombinace znalostí a odvozovat znalosti nové. Bohužel předmětný trend se projevuje i u lidí provozujících (tj. ovládajících) technická díla. Z důvodu bezpečnosti technických děl a lidského systému samotného, jde o zcela nežádoucí jev. Proto je zdrojem nových rizik a je třeba se s ním v zájmu bezpečí a rozvoje lidí inteligentně vypořádat.

Průmyslová revoluce reprodukovala dělbu práce ve společnosti tak, že všude dosadila úzkou specializaci celoživotních povolání. Oddělení výkonné funkce a řízení, fyzické a duševní práce je v tradiční průmyslové (mechanizované) produkci výrobním principem. Naproti tomu vědeckotechnická revoluce ve svém celku naznačuje možnosti překonání slabé dělby práce a její nahrazení vědomou organizací lidské součinnosti, v níž všichni tak či onak pracují na úrovni

tvůrčí činnosti (i když různé podoby), kde všeobecnou hlavní funkcí člověka se stává aplikace vědy, v níž mizí roztržka mezi intelektuálními silami výroby a prací, mezi fyzickou a duševní činností. S pokrokem techniky začíná počet pracovníků „duševní práce“ (jejíž obsah se mění) převyšovat počet ryze manuálně pracujících a nadto i ve zbylých funkcích na pokraji výroby (seřizovači, údržbáři) začínají zřetelně převládat duševní prvky.

Roste podíl tak zvaných průběžných povolání, jejichž představitelem je právě údržbář i opravář; dochází ke sdružování někdejších tisíců profesí a specializací v „široké profily“ a v jejich obsahu sílí inženýrsko-technická funkce. Schopnost specializace tu není zrušena, ale je spojena s univerzálním základem a je dynamizována. Stejná tendence je i u kvalifikace inženýrů, u kterých zrychlující se rozvoj techniky (během jedné generace dochází k radikálním převratům v technologii) vyžaduje osvojit si nejen široký základ teoretický a metodický (matematika, fyzika, chemie), ale i mnohé humanitní obory (ekonomie, psychologie atd.). Rostou nároky na propojování znalostí a zkušeností.

Je pravdou, že nároky na zvyšování kvalifikace inženýrů a techniků nerostou lineárně. V první etapě vědeckotechnické revoluce, ve které převládalo dokončování mechanizace (a ještě u částečné automatizace) nároky na kvalifikaci dočasně poklesly, což vedlo k přesunu pracovní síly do „nevýrobní“ sféry, tj. služeb, administrativy apod. V další etapě začalo docházet k obratu v souvislosti s použitím techniky i v terciální sféře (školství, kultura, zdravotnictví atd.), a vznikly vysoké požadavky na úroveň vzdělávání, protože nová technika se rychle mění a vyžaduje správné ovládání. Lze možná říci, že dochází k přesunu od specializace k univerzalizaci.

Předmětný trend proto vyžaduje průběžné vzdělávání. Dostupná technika vyžaduje udržovat po celý život znalosti na úrovni soudobého vývoje; z důvodu rychlého vývoje poznání, rychlého zastarávání techniky je člověk nucen učit se celý život. Proto v technických dílech je nutné kontinuální vzdělávání, aby díla byla bezpečná. Je si třeba uvědomit, že nejde o hromadění encyklopedických znalostí, ale o rozvíjení schopnosti samostatného logického myšlení a efektivní zvládání úkolů náročných na správné propojení znalostí.

Vědeckotechnická revoluce jako univerzální a permanentní proměna výrobních sil lidského života otevírá dva nové rozměry společenského vývoje:

- vědecké objevy, technologie a technická díla vytváří dynamické prostředí, ve kterém se člověk musí naučit žít,
- zároveň člověk má větší potenciál a více mění lidskou společnost.

V obou směrech se mezi člověkem a jeho dílem rozvíjí složitá dialektika, jejíž obraty dovádějí tradiční hranice života ad absurdum a zároveň se jim začínají vymykat.

Od roku 2011 se stále více mluví o čtvrté průmyslové revoluci. Její podstata byla představena na veletrhu v Hannoveru v roce 2013 [57]. Představují ji socio-kyber-technologické (kyberneticko-fyzikální) systémy. S nimi jsou spojené představy, že inteligentní systémy převezmou činnosti, které dosud vykonávali lidé. Jedná se o vnímání okolního dění s počítačovým spojením strojů a dílů. Mají k tomu pomáhat kamery, vysílače, čidla, čtečky kódů a jiná moderní zařízení. Automatické sklady včas odešlou zpracovanou zakázku a díly i polotovary budou obsahovat mikročipy, jež určí, jak mají být opracovány [57]. V nově vytvářeném prostředí je třeba:

- zajistit lidské hodnoty, které jsou uvedeny v Maslovově pyramidě [58],
- hledat způsob žití pro lidi, aby neztratili logické myšlení a zachovali si schopnost, která zabrání moderním kyber-technickým systémům zlikvidovat lidstvo a jeho hodnoty.

4. DATA A METODY POUŽITÉ PRO STANOVENÍ ZÁSAD PRO ŘÍZENÍ RIZIK SLOŽITÝCH TECHNOLOGICKÝCH ZAŘÍZENÍ

Z důvodu velké šíře problematiky nejprve stručně charakterizujeme oblasti zdrojů dat; zdroje konkrétních datových souborů použitých pro tvorbu jednotlivých databází a odkazy na databáze pak uvedeme u jednotlivých výsledků. Následně pak uvedeme přehled vybraných metod, které používá inženýrství rizika.

4.1. Zdroje, jejichž údaje byly použity při tvorbě databází, souboru poznatků pro výběr kritérií pro posuzování bezpečnosti složitých technologických děl

Pro odvození požadavků na zajištění bezpečnosti složitých socio-kyber-technologických systémů byly jako data použity poznatky uvedené v kapitolách 2 a 3 a dále uvedené zdroje:

1. Poznatky z odborné literatury a vlastního výzkumu o riziku a bezpečnosti.
2. Pokyny Mezinárodní organizace pro standardizaci kvalifikované řízení rizik.
3. Poznatky z aplikace ALARA, ALARP, RAM, RAMS aj. v průmyslu a stavebnictví.
4. Předpisy IAEA, OECD, NEA, WANO, OSN, FEMA, EMA, ISO, IRIS apod.
5. Poznatky z publikovaných výsledků hodnocení havárií, např.: Turner, Perow, Sagan, Lee, NASA, OECD, IAEA, WANO, NEA, OSN a další.
6. Poznatky z vlastních studií pro průmyslové a energetické objekty v ČR a zahraničí.
7. Vlastní výsledky získané z databáze havárií (sestavená z 258 světových zdrojů - 922 technologických havárií s přítomností nebezpečných látek od r. 1916; 168 světových zdrojů o 223 dopravních nehodách s přítomností nebezpečných látek od r. 1929; 281 světových zdrojů o 207 jaderných haváriích, aj.).
8. Vyhodnocení výpočtů rizik a veličin, které jsou ke stanovení rizik potřebné.
9. Zkušenosti ze sestavování nástrojů pro řízení bezpečnosti na základě řízení rizik pro průmyslové a dopravní systémy v ČR.
10. Zkušenosti z inspekcí a vyšetřování nehod a havárií v průmyslu a dopravě.
11. Zkušenosti z posuzování bezpečnostních zpráv složitých technologických objektů.
12. Výsledky výzkumných a aplikačních projektů EU, OECD, NEA a IAEA.

Výčet všech použitých zdrojů je rozsáhlý a velmi rozmanitý, a proto je zvolen postup, že u každého výsledku uvedeného v kapitole následující, jsou taxativně vždy uvedeny zdroje použitých dat. Všechna data jsou v archivu [12].

4.2. Přehled použitých metod

Při odvozování výsledků v dalších kapitolách jsou použity obecně známé metody (analogie, analýza, syntéza, dedukce, indukce, inženýrský úsudek, logický postup, komparace, klasifikace, strukturálně funkční analýza apod.), zásady logického myšlení a kritického hodnocení, výše uvedený koncept stanovení integrálního rizika a zavedené správní postupy (existující rozdíly v řízení při normálních, nouzových a kritických podmínkách; odlišení úrovní řízení – technická, funkční, taktická, strategická a politická).

Při analýze, hodnocení a posuzování složitých problémů jsou používány vybrané metody inženýrství rizika (aplikace axiomatické teorie kardinálního užitku MUT (Multiatribute Utility Theory), případové studie, What, If analýzy, diagramy rybí kost, stanovení kritických položek,

vícestupňová delfská metoda, expertní posouzení na základě přesně definovaných kritérií a hodnotových stupnic, metoda zpracování expertních odhadů, multikriteriální hodnocení, tvorba scénářů, metoda AHP (Analytical Hierarchy Process), multikriteriální hodnocení, hodnocení technik, metoda zpracování expertních odhadů, panelová diskuse, systémy pro podporu rozhodování aj.) [15].

Protože při řešení problémů složitých systémů je nutno používat kritéria z různých oblastí, která nejsou souměřitelná, tak se nejlépe hodí metody založené na skórování, např. metoda skórování míry zranitelnosti a míry důležitosti či obslužnosti [15]. Přitom je třeba zvažovat položky: doba trvání obnovy objektu / infrastruktury; dopad selhání objektu / infrastruktury na životy a bezpečí lidí; způsobené újmy a ztráty na veřejných aktivech; dopady na životní prostředí; a vyvolaný nepříznivý zájem [11]. Při zajištění bezpečnosti technického objektu / infrastruktury v území se musí zvažovat mnoho faktorů a mezi základní patří náklady na provoz a údržbu po dobu životnosti, náklady na preventivní údržbu a na nápravná opatření při odezvě a obnově. Pro každou z položek se musí stanovit kritéria pro posouzení fyzických podmínek (respektující vlastnosti objektu / infrastruktury i požadavky na fyzická a kybernetická aktiva), kapacity a poptávky po službách a pro posouzení funkčnosti. Na základě stanovených kritérií se stav položky kvalitativně hodnotí verbální stupnicí obsahující stupně 1 až 5 [10]. Vhodné je použít pětistupňovou stupnici, např.:

- stupeň 0: ztráty na objektu / infrastruktuře nemají dopad na bezpečí a rozvoj území a jeho veřejných aktiv.
- stupeň 1: ztráty na objektu / infrastruktuře mají malý dopad na bezpečí a rozvoj území a jeho veřejných aktiv.
- stupeň 2: ztráty na objektu / infrastruktuře mají střední dopad na bezpečí a rozvoj území a jeho veřejných aktiv.
- stupeň 3: ztráty na objektu / infrastruktuře mají významný dopad na bezpečí a rozvoj území a jeho veřejných aktiv.
- stupeň 4: ztráty na objektu / infrastruktuře mají závažný (velmi velký) dopad na bezpečí a rozvoj území a jeho veřejných aktiv.
- stupeň 5: ztráty na objektu / infrastruktuře mají podstatný dopad na bezpečí a rozvoj území a jeho veřejných aktiv.

Dle práce [10] je třeba ztráty ocenit kvantitativně, alespoň stupnicí: malý dopad – ztráty jsou menší než velikost pojištění; střední dopad – ztráty jsou menší než velikost pojištění za 3 roky; významný dopad – ztráty jsou menší než 25% hodnoty; závažný dopad – ztráty jsou mezi 25 a 45% hodnoty; podstatný dopad – ztráty jsou větší než 45% hodnoty. Při hodnocení rizik objektu / infrastruktury se používají otázky:

1. Jak objekt / infrastruktura reaguje na určité typy pohrom?
2. Jak je objekt / infrastruktura masivní, odolná a pružná?
3. Jak se chování objektu / infrastruktury může zlepšit?
4. Jaké jsou vhodné mechanizmy kontroly stavu objektu / infrastruktury?
5. Jaká pravidla se mohou využít pro samoregulaci nebo pro přípustné odchylky objektu / infrastruktury?
6. Které části objektu / infrastruktury jsou kritické?

Odpovědi na uvedené otázky se hledají v dále specifikovaných krocích:

1. Krok 1 - Modelování problémové situace. Správný popis problémové situace podmiňuje úspěšnost řešení. Je důležité znát souvislosti, vztahy a interakce mezi částmi, které se mají analyzovat a hodnotit. Popis objektu / infrastruktury má čtyři hierarchické úrovně, které mají dále uvedené funkce:
    - úroveň 1 představuje „systém systémů“, což je celé hospodářství, nebo mezinárodní společenství (jako EU) nebo soustava veřejné správy. Cílovou funkcí této úrovně je funkční schopnost složitého systému technologického objektu / infrastruktury,

- úroveň 2 představuje jednotlivé objekty / infrastruktury, s nimiž jsou spojeny různé zájmové skupiny (držitelé zájmů – stakeholders). Cílovou funkcí je minimalizace rizika nefunkčnosti jednotlivých objektů / infrastruktur,
- úroveň 3 je systémovou úrovní. Každý jednotlivý Objekt / infrastruktura se znázorňuje pomocí systému. Cílovou funkcí je hodnota pro akcionáře (shareholders),
- úroveň 4 je úrovní technických složek a prvků objektu / infrastruktury. Cílovou funkcí je technická funkčnost.

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

- aktivní činitel řídí a kontroluje řiditelné faktory,
- řiditelné faktory ovlivňují chování aktivního činitele,
- řiditelné faktory určují ukazatele,
- ukazatelé regulují řiditelné faktory.

Žádný konkrétní objekt / infrastruktura však není izolovaný (vzájemná závislost), a proto se specifikují neřiditelné faktory ovlivňující systémy předmětného objektu / infrastruktury, které působí na aktivního činitele a řiditelné faktory. Jedná se například o mezinárodní standardy. Na ukazatele však mají také vliv vnější a vnitřní faktory, které určují hodnotu cílové funkce, jež dovoluje aktivnímu činiteli měnit řiditelné faktory, když hodnota cílové funkce leží mimo normální hodnoty.

2. Krok 2 - Analýza příčinnosti. Analyzují se dále uvedené vrstvy předmětné infrastruktury: fyzická vrstva, vrstva regulace a řízení, vrstva organizace a managementu a vrstva strategického řízení správce objektu / infrastruktury. Analyzuje se také vzájemné působení prvků, a prvky se dělí na aktivní (řídící), pasivní (řízené), kritické a vyrovnávací prvky takto:
   - aktivní prvky silně působí na jiné, samy však nejsou ovlivňovány,
   - pasivní prvky působí slabě na jiné prvky, kdežto samy jsou silně ovlivňovány,
   - kritické prvky působí na jiné a reagují velmi intenzivně,
   - prvky, které neovlivňují jiné a ani nereagují s jinými, jsou prvky vyrovnávací.
3. Krok 3 - Návrh scénářů. Scénář se navrhuje následujícím postupem:
   - stanovení časového rámce,
   - identifikace faktorů ovlivňujících chování předmětného objektu / infrastruktury,
   - volba relevantní oblasti předmětného objektu / infrastruktury pro scénář,
   - návrh základního / výchozího scénáře selhání objektu / infrastruktury,
   - návrh alternativních scénářů selhání,
   - interpretace scénářů.
4. Krok 4 - Analýza dopadů. Cílem analýzy dopadů je zvýšení funkční schopnosti předmětného objektu / infrastruktury, přičemž se vychází z faktu, že funkční schopnost sice závisí na systémové udržitelnosti a technické provozuschopnosti, avšak zmíněné ukazatelé nejsou přímo řiditelné.
5. Krok 5 - Plánování opatření.
6. Krok 6 - Realizace robustního a adaptabilního řešení.

Pro řízení bezpečnosti entity, tj. pro řízení rizik zacílené na bezpečí a rozvoj entity však potřebujeme hodnoty, které mají zcela určitý význam. Protože velikost integrálního rizika spojeného se systémem závisí na celé řadě aspektů (dopady na jednotlivé komponenty, vazby a toky), je třeba mít sestavené hodnotové stupnice, aby se zajistila objektivita hodnocení. To znamená, že výsledky musí být správné (tj. opakovatelné, srovnatelné, ověřitelné a nezávislé na zpracovateli) a validované, tj. mít vypovídací schopnost k cíli řešeného úkolu. Proto pro měření rizika se používají standardní stupnice; uvedeme tři základní stupnice.

Vycházíme ze skutečnosti, že splnění požadavků, které zajišťují bezpečnost entity, oceníme buď jednoduchou stupnicí „ano, ne“ nebo klasifikační stupnicí (0 = požadavky na bezpečnost nejsou splněny až 5= požadavky na bezpečnost jsou splněny) a výsledek měříme procenty (u první stupnice je nízká bezpečnost, vysoká kritičnost nebo vysoké riziko, když odpověď ne je u téměř 100% případů, u druhé stupnice je nízká bezpečnost, vysoká kritičnost nebo vysoké riziko, když odpověď 0 je téměř u všech případů; je však skutečností, že v řadě případů v praxi se používá obrácená logika, tj. 5 znamená nesplnění požadavků na bezpečnost a vice versa).

Používané stupnice dle [10] jsou:

- FEMA - výsledek: 0 – 10% znamená riziko velmi velké; 11 – 40% znamená riziko velké; 41 – 60% znamená riziko střední; 61 – 90% znamená riziko malé; 91 – 100% znamená riziko velmi malé,
- ČSN - výsledek: méně než 5% znamená riziko katastrofálně vysoké; 5 – 25% znamená riziko velmi vysoké; 25 – 45% znamená riziko vysoké; 45 – 70% znamená riziko střední; 70 – 95% znamená riziko velmi malé; nad 95% znamená riziko zanedbatelné,
- OECD a Světová banka - výsledek: 0 – 4% znamená riziko téměř jisté; 5 – 10% znamená riziko vysoce pravděpodobné; 11 – 25% znamená riziko pravděpodobné; 26 – 74% znamená riziko je málo pravděpodobné; 75 – 95% znamená riziko velmi nepravděpodobné; nad 95% znamená riziko zanedbatelné.

Z hlediska úrovně poznání je třeba uvést, že výběr hodnotové stupnice je buď dán konceptem nebo požadavkem na aplikaci jisté normy nebo standardu, které hodnotovou stupnici stanoví. Nejčastěji používané koncepty jsou: ALARP, ALARA a výsledky založené na CBA (Cost-Benefit Analysis) či SCBA (Social Cost-benefit Analysis) [10]. V posledně citované práci jsou další postupy pro ocenění rizika s cílem určit kvalifikovaná opatření a činnosti vedoucí ke snížení zranitelnosti a zvýšení pružné odolnosti dopravní infrastruktury.

Pro posuzování kritičnosti aktiv, objektů a infrastruktur jsou použita multikriteriální hodnocení se soubory kritérií. V práci jsou uvedeny konkrétní výsledky pro několik souborů kritérií:

1. SK1: Pro kritičnost aktiv, objektů a infrastruktur je v souladu s postupy používajícími v USA, Austrálii, Kanadě [59-64] v praxi s dobrým výsledkem otestováno 14 kritérií:
    - míra schopnosti ochrany aktiva, objektu, infrastruktury,
    - míra zranitelnosti aktiva, objektu, infrastruktury vůči útoku,
    - míra ohrožení zdraví a životů lidí při selhání aktiva, objektu, infrastruktury,
    - míra dopadu selhání aktiva, objektu, infrastruktury na životní prostředí,
    - míra nákladů na výměnu či opravu aktiva, objektu, infrastruktury,
    - míra doby výměny či opravy aktiva, objektu, infrastruktury,
    - míra důležitosti aktiva, objektu, infrastruktury pro zajišťování záchranných a nouzových funkcí v území,
    - míra důležitosti aktiva, objektu, infrastruktury pro zajišťování funkcí správy a samosprávy území,
    - míra důležitosti aktiva, objektu, infrastruktury pro zajišťování funkcí armády a policie,
    - míra redundance nebo substituční služby za aktivum, objekt, infrastrukturu,
    - míra důležitosti infrastruktury pro zajišťování komunikačních funkcí v území,
    - míra dopadu selhání infrastruktury na obslužnost území a na ekonomiku území (regionu, státu),
    - míra důležitosti provozuschopnosti aktiva, objektu, infrastruktury pro území,
    - míra důležitosti aktiva, objektu, infrastruktury pro oblast symbolickou, kulturní apod. území.
2. SK2: Při zacílení na bezpečný lidský systém se pro kritičnost aktiv, objektů a infrastruktur dle [10] používá také 14 kritérií:

- míra schopnosti ochrany lidských životů, zdraví a bezpečí uvnitř systému,
- míra schopnosti ochrany lidských životů, zdraví a bezpečí vně systému,
- míra schopnosti ochrany majetku uvnitř systému,
- míra schopnosti ochrany majetku vně systému,
- míra schopnosti ochrany veřejného blaha uvnitř systému,
- míra schopnosti ochrany veřejného blaha vně systému,
- míra schopnosti ochrany životního prostředí uvnitř systému,
- míra schopnosti ochrany životního prostředí vně systému,
- míra schopnosti ochrany životně důležitých infrastruktur a technologií uvnitř systému,
- míra schopnosti ochrany životně důležitých infrastruktur a technologií vně systému,
- míra schopnosti ochrany lidských životů a zdraví před dopady pohrom způsobených vnitřními závislostmi,
- míra schopnosti ochrany životního prostředí před dopady pohrom způsobených vnitřními závislostmi,
- míra schopnosti ochrany lidské společnosti před dopady pohrom způsobených vnitřními závislostmi,
- míra schopnosti ochrany životně důležitých infrastruktur a technologií před dopady pohrom způsobených vnitřními závislostmi.

3. SK3: Pro určení míry zranitelnosti položky, tj. aktiva, objektu, infrastruktury se provádí skórování za pomoci kritérií:
   - úroveň společenského vnímání selhání položky,
   - množství postižených obyvatel při selhání položky,
   - dostupnost položky veřejnou komunikací,
   - zabezpečení vstupu do položky,
   - dopad nebezpečných látek na člověka a životní prostředí při selhání položky,
   - množství uvolněné nebezpečné látky při selhání položky.
4. SK4: Pro určení kritičnosti aktiv v technologickém celku se používá hodnocení zkrácené, tj. měří se jen výší škody.

Ve všech případech se údaje pro hodnocení získávají od expertů. V některých případech, které jsou dále prezentovány, jde o výsledky vzniklé dohodou 2 expertů, např. [65]. V jiných z oblasti dopravy jde o použití šesti expertů, vybraných podle kritérií používaných v EU [10] z oblastí: ochrana obyvatelstva; ochrana území; ochrana životního prostředí; veřejná správa zaměřená na ochranu obyvatelstva; ochrana technologických systémů; a Integrovaného záchranného systému.

V prvních dvou případech se používá stupnice pro posuzování kritičnosti: 0 bodu - faktor zajišťuje extrémně vysokou schopnost ochrany (očekávané škody jsou nižší než 5 %, aplikace konceptu znamená nevýznamné riziko pro aktiva, tj. zanedbatelnou kritičnost konceptu); 1 bod - faktor zajišťuje velmi vysokou schopnost ochrany (očekávané škody jsou v intervalu 5-25 %, aplikace konceptu znamená nízké riziko pro aktiva, tj. nízkou kritičnost konceptu); 2 body - faktor zajišťuje vysokou schopnost ochrany (očekávané škody jsou v intervalu 25-45 %, aplikace konceptu znamená střední riziko pro aktiva, tj. střední kritičnost konceptu); body - faktor zajišťuje střední schopnost ochrany (očekávané škody jsou v intervalu 45-70 %, aplikace konceptu znamená vysoké riziko pro aktiva, tj. vysokou kritičnost konceptu); 4 body - faktor zajišťuje nízkou schopnost ochrany (očekávané škody jsou v intervalu 70-95 %, aplikace konceptu znamená velmi vysoké riziko pro aktiva, tj. velmi vysokou kritičnost konceptu); a 5 bodů - faktor zajišťuje zanedbatelnou schopnost ochrany (očekávané škody jsou vyšší než 95 %, aplikace konceptu znamená extrémně vysoké riziko pro aktiva, tj. extrémně vysokou kritičnost konceptu). Výsledná hodnota pro každé kritérium je určena jako medián z údajů získaných od expertů. Celkové hodnocení kritičnosti je součtem hodnot získaných u

jednotlivých kritérií. Po normování, při kterém se se použije maximální možná hodnota, se provede klasifikace kritičnosti dle tabulky 2; např. v případě 14 kritérií je maximum 70 bodů.

Tabulka 2. Hodnotová stupnice.

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

Ve čtvrtém případu je používána zjednodušená stupnice: kritičnost = 0, když škoda je menší než 5% ceny aktiva a není narušena funkčnost aktiva; kritičnost = 1, když škoda je menší než 7% ceny aktiva a nedojde k přerušení funkčnosti systému, ve kterém je aktivum umístěno a aktivum lze opravit nebo vyměnit; kritičnost = 2, když škoda je menší než 10% ceny aktiva, dojde ke krátkému přerušení funkčnosti systému, ve kterém je aktivum umístěno; kritičnost = 3, když škoda je větší než 10% ceny aktiva, dojde k dlouhému přerušení funkčnosti systému, ve kterém je aktivum umístěno.

Uvedené příklady stupnic ukazují, že ještě nejde o ustálené pojetí a že u každého hodnocení daného druhu je třeba popsat použitou stupnici, což obvykle chybí, např. [66,67].

Další postupy multikriteriálního hodnocení jsou prováděny pomocí aplikace systémů pro podporu rozhodování, jež jsou naznačeny v tabulkách 3 - 5. Tabulka 3 se používá pro identifikaci kritičnosti aktiva nebo objektu z pohledu zajištění ochrany položky vůči možným pohromám. Tabulka 4 se používá pro identifikaci nedostatků řídicího systému technologického objektu z pohledu bezpečnosti (tj. posuzuje se SMS – safety management system). Tabulka 5 se používá pro identifikaci nedostatků při řízení bezpečnosti konkrétních míst s ohledem na kritické pohromy.

Ve všech dále studovaných případech jsou data kriticky posouzena a syntetizována podle principů sestavování modelů strategických procesů [1,2,5,10], tj. podle postupů, které jsou v souladu s postupem popsaným ve známých pracích [27,29,68-73].

Protože zajištění bezpečnosti technických děl a jejich okolí vyžaduje náklady, tak při návrhu opatření na řešení problémů se zvažují náklady spojené s:

- přímými ztrátami způsobenými pohromami,
- nepřímými ztrátami způsobenými pohromami, do kterých např. patří i ekonomické ztráty u průmyslových podniků, neschopnost obnovy podnikání, selhání veřejných služeb či nedostupnost objektů kvůli tomu, že některé z nich jsou nepojištěné nebo podpojištěné,
- ztrátami a újmami spojenými s lidmi (personál, kontraktoři, občané),
- náklady veřejné správy a bezpečnostních složek státních i privátních spojených se zvládnutím pohrom, které se dělí na náklady na odezvu, na obnovu a na náklady za jiné práce, které musí být vykonány ve veřejném zájmu,
- náklady na pojištění proti pohromám,
- náklady na prevenci u budov, zařízení, infrastruktur a v území,
- náklady na příslušný výzkum, vzdělání, výcvik a propagaci.

Tabulka 3. Identifikace nedostatků, tj. kritičnosti objektu z pohledu aplikace přístupu All-Hazard-Approach. Způsob vyplnění tabulky – zvažují se pouze pohromy, které mají přímé dopady, tj. políčka, vyžadující odpověď; ostatní políčka nemají hodnotu, začerní se a do celkového hodnocení se nezahrnují., tj. i=1,2,…, n.

Pohroma – název	**Je pohroma relevantní?**		**Patří-li pohroma do kategorie specifických pohrom, je to zohledněno v umístění, projekto-vání, výstavbě objektu účinnými preventiv-ními technickými opatřeními?**		**Patří-li pohroma do kategorie specifických pohrom, je to zohledněno v provozu objektu účinnými preventivní-mi organizač-ními opatřeními?**		**Patří-li pohroma do kategorie kritických pohrom, je to zohledněno v provozu objektu reaktivními opatřeními na ochranu zaměstnanců, technologie a životního prostředí uvnitř objektu?**		**Patří-li pohroma do kategorie kritických pohrom, je to zohledněno v provozu objektu reaktivními opatřeními zaměřenými na ochranu zaměstnanců, technologie, lidí a životního prostředí uvnitř i vně objektu?**	
	NE	**ANO**	**NE**	**ANO**	**NE**	**ANO**	**NE**	**ANO**	**NE**	**ANO**
1										
2										
3										
4										
.....										
n										
CELKEM										

Tabulka 4. Identifikace nedostatků pro specifické pohromy v daném území, tj. i=1,2,..., n. Jde o posouzení kritičnosti z pohledu aplikace přístupu Defence-In-Depth.

i	**Otázka**	**Odpověď**		**Poznámka**
		ANO	**NE**	
1	1. Má technologický systém zapracované principy inherentní bezpečnosti, tj. bezpečného designu?			
	2. Má řídicí systém technologického systému (SMS) nastaveny základní řídící funkce, alarmy a reakce operátora nastaveny tak, aby se technologický systém udržel v normálním (stabilním) stavu?			

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

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

Tabulka 5. Identifikace slabin, tj. konkrétních kritických míst pro kritické pohromy, i = 1,2,..., n – expertní šetření; ANO = 3; spíše ANO = 2; spíše NE = 1; NE = 0. Pojem „kritický“ je vysvětlen v [10].

Kritická pohroma	**Jsou zajištěna ochranná opatření a činnosti pro**	**Jsou zajištěny ochranné postupy pro špatnou odezvu?**		**Jsou zajištěny ochranné postupy pro špatné řízení provozu?**		**Jsou zajištěny ochranné postupy pro aplikaci špatných předpisů?**	
		ANO	**NE**	**ANO**	**NE**	**ANO**	**NE**

	zaměstnance a lidi v okolí přítomné v objektu	provoz technologie	životní prostředí v okolí	lidi v okolí objektu	obnovu provozu do 14 dní						
1											
2											
.....											
n											

Předmětné tabulky jsou používány v praxi s tím, že používají hodnotovou stupnici v tabulce 2.

5. VÝSLEDKY VÝZKUMU ZAMĚŘENÉHO NA BEZPEČNOST TECHNICKÝCH DĚL

Technologie jsou výsledkem lidského intelektu a jejich aplikace v praxi umožňuje lidem rozvoj a přežití nástrah přírody. Využití v praxi je spojeno s jejich rozšířením v území, což se mnohdy děje pomocí infrastruktur. Předmětem práce je přínos technologií, tj. nejsou řešeny otázky zneužití technologií. Technologické objekty a infrastruktury byly, jsou a budou veřejným aktivem, protože zajišťují dennodenní potřeby občanů, tj. energii, vodu, jídlo, informace apod. a právě na nich závisí přežití lidí při kritických situacích. Na základě současného poznání představují složité otevřené systémy v dynamicky proměnném světě, který je ovlivňován jak procesy, které probíhají nezávisle na člověku, tak procesy, které člověk vytváří vědomě či nevědomě svou činností a chováním.

U procesů, které se odehrávají nezávisle na vůli a chování člověka, má člověk pouze možnost zmírňovat nepřijatelné dopady na sebe a aktiva, na kterých je závislá jeho existence a kvalita života. Šanci má však jen tehdy, když předmětné procesy důkladně pozná a najde opatření a činnosti, kterými zmírní dopady procesů, které poškozují jeho nebo aktiva, na nichž je závislý. U procesů, které člověk vyvolává svým chováním a činnostmi, má člověk šance vyšší, protože může cíleným chováním a cílenými činnostmi vytvářet jen procesy, které zlepší kvalitu jeho života a zároveň významně nenaruší prostředí, na němž je existenčně závislý, tj. má možnost snižovat nebezpečnost objektů, infrastruktur i procesů. Šanci má ovšem jen tehdy, když bude mít znalosti a když znalosti a zkušenosti správně a cíleně využije [1,2,10,11].

V kapitole se zabýváme v současné době používanými koncepty bezpečnosti technických děl a na příkladech ukazujeme dopady pohrom a selhání technických děl. Dále uvádíme příklady nástrojů rizikového inženýrství, kterými lze rizika technických děl v dynamickém světě ovládat tak, aby technické dílo bylo bezpečné během své životnosti (tj. aby dílo během svého životního cyklu plnilo spolehlivě v požadované kvalitě funkce, ke kterým bylo zřízeno a aby při kritických podmínkách neohrožovalo ani sebe, ani své okolí). Uvádíme též návrhy možných aktivity a ochranných opatření ve sledovaných případech.

Protože lidský faktor je všudypřítomný, tak nakonec kapitoly uvádíme podkapitolu obsahující údaje o lidském faktoru a jeho hodnocení.

5.1. Výsledky porovnání používaných konceptů

Na základě poznatků uvedených v kapitolách 2 a 3 by technická díla měla být konstruována a provozována podle následujících zásad:

- každé technické dílo je systém systémů, který se v čase mění,
- v důsledku změn v technickém díle a okolí může dojít ke konfliktu, který nebyl očekáván,
- technické dílo i okolí jsou postihovány pohromami s tím, že velké pohromy se vyskytují zřídka a nepravidelně, a proto jejich možné velikosti nejsou odhalitelné metodami založenými na teorii pravděpodobnosti,
- pohromami pro technické dílo se stávají i vazby a spřažení, a to jak ty, které jsou úmyslně vytvořené z důvodu cíle, který dílo plní, tak i ty, které vzniknou neplánovaně tím, že v důsledku pohromy dojde k neočekávaným propojením, která pak vyvolají selhání díla.

V důsledku náhodných i znalostních nejistot je pro každé lidské společenství z pohledu veřejného zájmu, konkurenceschopnosti technického díla a udržitelného rozvoje lidského systému důležité, zda:

- bezpečnost (tj. úroveň opatření a činností ve prospěch bezpečí lidí, tj. i technického díla) v čase roste či klesá,

- ve stanovených časových úsecích je dosahováno plánované úrovně bezpečnosti,
- aplikovaná opatření vedou skutečně ke zvýšení bezpečnosti.

Protože jak technické dílo, tak jeho okolí jsou složité systémy, které se vyvíjí a tento vývoj nemusí byt nutně synergický, aplikace přesných matematických metod založených na teoriích, které počítají jen s náhodnými změnami, není schopna určit parametry a jejich proměnnost, jež zajistí bezpečnost technického díla po celou dobu životnosti. Rizikové inženýrství proto zavádí do praxe nástroje, kterými lze zvládnout podmínky, pro něž nebylo technické dílo konstruováno.

Dále zmíníme několik aspektů, které hrají závažnou roli. Prvním důležitým aspektem je volba samotného konceptu pro konstrukci a provoz technického díla. Velmi dlouho se za základ bezpečných technických děl považovala teorie spolehlivosti, jejím zakladatelem v r. 1816 byl Samuel T. Coleridge. Předmětná teorie je matematická disciplína, která se zabývá mírou selhávání prostředků nebo systémů, od kterých se očekává nějaká funkčnost nebo odolnost vůči vnějším vlivům, a rychlostí zotavení z jejich poruchových stavů. V hierarchii matematických odvětví patří pod aplikovanou statistiku. Pomocí nástrojů teorie spolehlivosti se vyčíslují parametry poruch, jako např. bezpečnost nebo spolehlivost, především těch zařízení, jejichž nečinnost nebo nesprávná činnost jsou z nějakého důvodu vysoce nežádoucí.

V r. 1978 Barry Turner [36] na základě analýz havárií technických děl vyslovil myšlenku, že složitost systému, kterým je technické dílo, zabraňuje stanovit všechna rizika, která mohou poškodit technické dílo a jeho okolí. Předmětný poznatek rozpracoval a potvrdil Charles Perrow na základě důkladné analýzy jaderné havárie Three Mile Island [37] a také závěry EU v r. 1981, které vedly k vydání direktivy SEVESO [74].

Předmětné poznání pochopitelně narušilo hegemonii teorie spolehlivosti a vzniklo soupeření mezi oběma směry, na které poukázal Scot Sagan [35]. Bohužel do dnešního dne dohady pokračují. Spolehlivostní inženýři věří, že haváriím může být zabráněno dobrým organizačním projektem a řízením (tj. jde o přístup založený na vysoké spolehlivosti). Předmětný přístup tvrdí:

- bezpečnost je primárně organizační cíl; zálohování zvyšuje bezpečnost, protože duplikace a překrytí zajistí, že spolehlivý systém nemá nespolehlivé části,
- decentralizované rozhodování dovoluje promptní a flexibilní odezvy na překvapení,
- kultura spolehlivosti zvyšuje bezpečnost podpořením jednotné aktivity obsluhy, protože vyžaduje striktní organizace činností;
- kontinuální akce, výcvik a simulace vytváří a udržují vysokou úroveň spolehlivosti sytému,
- testy a poučení z havárií jsou efektivní a mohou být doplňovány předtuchami a simulacemi.

Naproti tomu inženýři vycházející z disciplín o riziku tvrdí, že u složitých technických děl jsou havárie a selhání nevyhnutelné a že zálohování často zvyšuje složitost systému. Pro zajištění bezpečnosti složitých technických děl je proto třeba mít připraveny nástroje na zvládnutí jejich havárií a selhání. Diskuse a opatření po havárii jaderné elektrárny Fukushima uvedenou strategii potvrdily.

Komplikace v praxi působí skutečnost, že obě inženýrské disciplíny, používají stejné postupy, metody, nástroje a techniky. Protože koncepty obou disciplín jsou různé, tak často jsou i jejich návrhy opatření na zajištění bezpečnosti odlišné, až konfliktní (např. dojde k selhání provozu vlaku z důvodu námrazy na elektrickém vedení, vlak se zastaví v polích a přestane topit, tj. pro lidi vznikne kritická situace, ale provozovatel nemá povinnost, ani nástroje pro řešení, přestože životy a zdraví lidí jsou dle Ústavy ČR základním chráněným aktivem v ČR – situace nastala např. 1. 12. 2014).

Předmětnou situaci ještě zkomplikovalo rozdělení zdrojů rizik na dvě skupiny, a to: ty, které souvisí s chováním člověka (sabotáž, neoprávněný přístup, ilegální přesun nebo jiné zákeřné činy spojené s nebezpečnými látkami nebo na ně připojenými zařízeními; a ty ostatní. V prvním případě se začaly tvořit disciplíny zacílené na zabezpečení (security) a v druhém na bezpečnost

(safety), např. [75]. Je faktem, že opatření pro druhý případ jsou propracovanější, protože jejich vývoj začal v 30. letech minulého století. Další skutečností je, že obě disciplíny pracují s riziky, spoléhají na ochranu technického díla ve smyslu Defence-In-Depth (obrázek 8) a požadují řízení technického díla pomocí SMS (obrázek 11). Bohužel v praxi se často aplikují odděleně, a dochází ke konfliktům až haváriím (požár ve vojenské centrále v Seatlu 15. 7. 2008 – zabezpečení místnosti nedovolilo otevřít dveře a uhořelo 8 lidí). Z důvodu bezpečnosti je pak východiskem buď provedení optimalizace opatření před zavedením do praxe, anebo použití výše popisovaného přístupu All-Hazard-Approach, který neodděluje zdroje rizik. Základem je koncept integrální bezpečnosti, který je rozpracován v předchozích kapitolách, který řeší konflikty proaktivně, tj. od začátku projektu. Proto se dnes koncept používá u tvorby raketoplánů, satelitů, ponorek, moderních vojenských letadel apod. [12].

Další problém bezpečnosti technických děl během životního cyklu je spojen se zadávacími podmínkami, které předurčují schopnost technických děl zvládat různé podmínky, které mohou nastat během jeho životnosti. V daném případě hraje roli řada faktorů, a to: výběr přístupu; rozsah a kvalita datových souborů použitých pro výpočet parametrů; a výběr metody zpracování dat.

Nejstarší používaný přístup při stanovení parametrů pro konstrukci a provozování technických děl je deterministický přístup, který z důvodu bezpečnosti důležitých technických děl požaduje zvažovat nejméně příznivé podmínky [76]. Na základě nutnosti zvažovat náhodné odchylky byl požadován při hodnocení bezpečnosti technických děl od 90. let minulého století pravděpodobnostní přístup [77]. Problémy spojené s havárií Kashizawaki Kariva v roce 2008 [78] vedly k tomu, že od r. 2012 se požaduje používat heuristiky, protože se připustily náhlé (skokové) změny podmínek ve vývoji území [79].

Kvalita nebo lépe řečeno validita datových souborů použitých při stanovení zadávacích podmínek pro technické dílo je dalším důležitým aspektem, který předurčuje bezpečnost technického díla. Např. při zemětřesení dne 11. 3. 2011 byla vážně poškozena jaderná elektrárna Fukushima, zatímco jen 30 km vzdálená jaderná elektrárna Onagawa odstavila a byla bez problémů – důvod: v prvním případě byla v zadávacích podmínkách zvážena jen tsunami od r. 1890 a v druhém od r. 840 [80]. Nemusíme však chodit až do Japonska, ale máme příklad velkých rozdílů v parametrech pro zadávací podmínky i z naší republiky [81].

Nakonec zmíníme samotné metody stanovení parametrů zadávacích podmínek. Použití teoretických modelů dává přesné a krásné výsledky. Jejich věrohodnost však značně závisí na tom, jak přesně vystihují realitu. Příkladem použití nesprávných modelů jsou např. obětí a stovky poškozených budov postavených v posledních dvou desetiletích ve střední Itálii, které od r. 2010 postihlo několik středně silných zemětřesení. Předmětné budovy byly postaveny na základě vysoce teoretických třídimenzionálních modelů na základě přesných dat získaných měřením od 60. let minulého století [82].

Jestliže použijeme experimentální data z dlouhých časových údobí, kde lze předpokládat, že datové soubory obsahují velké jevy, jejichž výskyt je řídký a nepravidelný, je zase problém v tom, že přesnost historických dat není srovnatelná s přesností dnešních dat získaných měřením. Datové soubory tudíž vykazují velký rozptyl, což způsobuje, že aplikace několika výpočetních metod na jeden takový datový soubor dává výsledky, které jsou tak odlišné, že neleží v intervalech daných standardními odchylkami; a navíc lze najít několik odlišných datových souborů a aplikovat na ně soubor několika metod a dostanou se výsledky ležící v jednom intervalu daném standardní odchylkou [83].

Navíc vzhledem ke skutečnosti, že velikost rizika závisí na velkých jevech, které se vyskytují zřídka a nepravidelně, je zřejmé, že metody matematické statistiky nejsou vhodné. V rizikovém inženýrství se proto nahrazují metodami expertními a heuristickými [15]. Na příkladech, které prezentuji při přednáškách studentům, ukazují, že různé metody tohoto typu také nedávají stejné

výsledky; stačí při vyhodnocení kontrolního seznamu použít stupnice upřednostňované různými světovými organizacemi jako je OECD, WB, FEMA, Swiss Re atd. [15].

Další problém je neexistence jedné stupnice pro posouzení bezpečnosti, kritičnosti či rizika při multikriteriálních hodnoceních. Např.:

1. Stupnice pro posuzování kritičnosti aktiv definovaná způsobem: 0 – očekávané ztráty na aktivech mají zanedbatelný dopad na infrastrukturu / objekt / území / stát; 1- očekávané ztráty na aktivech mají malý dopad na infrastrukturu / objekt / území / stát; 2 - očekávané ztráty na aktivech mají střední dopad na infrastrukturu / objekt / území / stát; 3- očekávané ztráty na aktivech mají významný dopad na infrastrukturu / objekt / území / stát; 4- očekávané ztráty na aktivech mají velký dopad na infrastrukturu / objekt / území / stát; a 5- očekávané ztráty na aktivech mají velmi vysoký / extrémní dopad na infrastrukturu / objekt / území / stát - tj. nemohou být tolerovány [84]. Předmětná stupnice klasifikuje dopady selhání infrastruktury na plnění základních funkcí pouze slovně. Pro posouzení nákladů na obnovu a schopnosti vlastníka provést obnovu je nedostatečná.
2. Stupnice pro posuzování schopnosti náhrady / výměny poškozeného aktiva je více konkrétní, protože používá dobu, za níž lze provést opravu nebo výměnu: 0 doba náhrady je 1 – 5 dní; 1 doba náhrady je 6 – 30 dní; 2 doba náhrady je 31-90 dní; 3 doba náhrady je 91 – 180 dní; 4 doba náhrady je více než 180 dní; 5 nemůže být nahrazeno [84].
3. V souvislosti s teroristickými útoky se často oceňuje, jak veřejnost vnímá důležitost aktiva: 0 – veřejnost si potřebu aktiva neuvědomuje; 1 – veřejnost si potřebu aktiva velmi málo uvědomuje, útočník neví nic o důležitosti aktiva; 2 – veřejnost si potřebu aktiva málo uvědomuje, útočník ví málo o důležitosti aktiva; 3 – veřejnost si potřebu aktiva středně uvědomuje, útočník ví o důležitosti aktiva; 4 – veřejnost si potřebu aktiva vysoce uvědomuje, útočník ví hodně o důležitosti aktiva; 5 - veřejnost si potřebu aktiva vysoce uvědomuje, útočník ví o velké důležitosti aktiva [84].
4. V souvislosti s teroristickými útoky se oceňuje dostupnost aktiva, tj. jistého zařízení: 0 – zařízení je fyzicky, organizačně a kyberneticky dobře zabezpečené (plot, kamery..); 1 - zařízení je fyzicky a organizačně dobře zabezpečené; 3 - zařízení je fyzicky dobře zabezpečené; 4 – zařízení je fyzicky středně zabezpečené; a 5 – zařízení není fyzicky zabezpečené [84].

Aplikací všech čtyř stupnic na jisté zařízení se hlavně v USA určuje kritičnost zařízení a k tomu se používá prostá suma čísel ze všech čtyř stupnic takto: 0-6, tj. kritičnost je velmi malá až malá - 1; suma se rovná 7-12, tj. kritičnost je malá - 2; suma se rovná 13-18, tj. kritičnost je střední - 3; suma se rovná 19-24, tj. kritičnost je vysoká - 4; suma se rovná 25-30, tj. kritičnost je velmi vysoká – 5 [84].

Protože inženýři konstruující a provozující technická díla se z důvodu bezpečnosti technických děl nemohou spokojit s konstatováním, došlo k výskytu atypické havárie označované jako černá labuť nebo královský drak, např. [85], a proto dílo havarovalo nebo selhalo, používají nástroje k tomu, aby při haváriích a selháních technických děl z jakýchkoliv příčin nepřesáhly dopady na lidi i technické dílo kritické meze pro přežití lidí a existenci technického díla.

Proto inženýrství rizika předem připravuje nástroje pro zvládnutí havárií a selhání technických děl a po každé havárii a selhání požaduje provedení situačního hodnocení:

1. Co se stalo?
2. Byla příčinou pohroma vnitřní, vnější, anebo lidský faktor? Proč?
3. Jaké zranitelnosti technického díla nebo obslužného personálu se projevily při nouzové nebo kritické situaci?
4. Jakým způsobem lze zabránit opakování takové havárie nebo selhání a jek je možné snížit zranitelnosti (opatření, sociální, technické, administrativní, politické, právní, ekonomické)?

5. Která opatření sociální, technická, administrativní, politická, právní či ekonomická mohou zvýšit odolnost zařízení vůči pohromě, která vyvolala nouzovou nebo kritickou situaci? Která z nich jsou nejúčinnější a dostupná?
6. Jaké je poučení pro provoz a budoucí výstavbu technických děl a jak ho implementovat do praxe?

Na základě poučení se pak provádí úpravy. Kvůli složitosti světa se celý cyklus stále opakuje.

5.2. Výsledky recentních projektů EU spojených s ochranou technických děl

V oblasti sledované v práci se EU soustřeďuje především na kritickou infrastrukturu. Podle základního dokumentu [86] kritická infrastruktura (KI) může být poškozena, zničena a narušena úmyslnými teroristickými útoky, přírodními pohromami, nedbalostí, haváriemi nebo počítačovým hackerstvím, trestnou činností nebo nezákonným jednáním. Pro ochranu životů a majetků lidí v EU ohrožených terorismem, přírodními pohromami a haváriemi, je nezbytné, aby jakákoliv narušení nebo manipulace s kritickou infrastrukturou byla, v rámci možností, krátká, málo četná, zvladatelná, geograficky omezená a minimálně škodlivá pro dobré životní podmínky občanů členských států (ČS) a Evropské unie (EU). EU vytvořila Evropský program pro ochranu KI (EPCIP) [87], varovnou informační síť kritické infrastruktury (CIWIN) [88] a zadala řadu výzkumných projektů z předmětné oblasti.

EPCIP by měl co možná nejvíce minimalizovat jakýkoliv nepřijatelný dopad, při kterém by zvýšené investice do bezpečnosti mohly ovlivnit konkurenceschopnost příslušného průmyslového odvětví. Při kalkulaci proporcionality nákladů se nesmí ztratit ze zřetele potřeba udržovat stabilitu trhů, která je zásadní pro dlouhodobé investice, ani vliv předmětné ochrany na vývoj akciových trhů a na makroekonomické prostředí.

Kritická analýza vybrané dostupné dokumentace k příslušným projektům [86,89-123] ukazuje dále uvedené poznatky:

1. Z důvodu ochrany KI je třeba dělat rozdíl mezi závislostí (dependence) a vzájemnou závislostí (interdependence). Závislost znamená, že infrastruktura A ovlivní stav infrastruktury B. Závislost je přímá nebo nepřímá; nepřímá závislost je tehdy, když infrastruktura A ovlivní infrastrukturu B, prostřednictvím infrastruktury C. Vzájemná závislost infrastruktur označuje oboustranný vztah mezi infrastrukturou A a infrastrukturou B; tj. vytváří se smyčky vzájemného ovlivňování. Důsledkem je skutečnost, že důsledky jakéhokoliv narušení nemohou být popsány stromovou strukturou, ve které se předpokládá, že všechny události se dějí jedním směrem. Předmětný poznatek je v souladu s poznatky, které máme v ČR [10,11] a prosazujeme je v oblasti vzdělávání.
2. Je třeba rozlišovat 4 zdroje vzájemných závislostí, a to: fyzická vzájemná závislost – provoz jedné infrastruktury závisí na fyzickém výkonu infrastruktury jiné; kybernetická vzájemná závislost – provoz jedné infrastruktury závisí na informaci přenesené přes informační infrastrukturu; geografická / územní vzájemná závislost – infrastruktury jsou územně blízko sebe (tj. naruší je každá pohrom – exploze, požár,..); a logická vzájemná závislost; podrobnosti lze nalézt v práci [10], která se problematikou detailně zabývá. Jelikož stav každé infrastruktury je v území regulován manuálně, poloautomaticky či kyberneticky, tak lze přes předmětné vzájemné závislosti odstartovat organizační havárie, tj. selhání infrastruktur bez narušení technických prvků; dopady těchto selhání pak naruší nejen očekávané služby, ale mají potenciál poškodit i technické prvky, jejichž obnova může být časově, finančně i technicky náročná.
3. Rozdílné vzájemné závislosti působí selhání na rozdílných úrovních, např.: fyzická vzájemná závislost působí selhání distribučních sítí pro rozvod, elektřiny, vody, plynu a

dalších produktů; kybernetická vzájemná závislost působí selhání komponent hardware a software, jež jsou určeny k ovládání a řízení infrastruktur (SCADA, DSC); a organizační vzájemná závislost působí chyby v postupech a funkcích používaných pro stanovení lidských činností a pro podporu spolupráce infrastruktur.

4. V praxi je třeba odlišovat různé typy selhání. Kaskádovité selhání znamená, že narušení jedné infrastruktury způsobí, že další infrastruktury přestanou plnit své funkce. Eskalující selhání znamená, že narušení jedné infrastruktury zhorší podmínky pro provoz jiných infrastruktur, a to zvýšením nároků na jejich provoz, není doba na zotavení nebo obnovu, což vede časem k selhání. Porucha se stejnou příčinou znamená, že několik sítí (zpravidla těch, u kterých je velká geografická závislost) selže ve stejnou dobu, např. v důsledku výskytu silného zemětřesení.
5. Ochrana KI vyžaduje koordinovaný multidisciplinární přístup a není jen technologickým problémem.

Velké projekty EU z pohledu cílů i financí v předmětné oblasti jsou projekty CIPRNet a CASCADE, a proto se o nich zmíníme více. První jmenovaný projekt (grant agreement no 312450) s rozpočtem 7.6 M€ řeší od r. 2012 celkem 12 členských zemí a Kanada, koordinátorem je Fraunhofer IAIS [124].

Základním zjištěním projektu CIPRNet je, že porušení kritické infrastruktury způsobuje velké ekonomické a sociální dopady a možné kaskády v důsledku závislostí v kritické infrastruktuře. Proto je potřeba lépe rozumět těsným vazbám v kritické infrastruktuře a zlepšit analýzu rizik, a tím řízení i ochranu kritické infrastruktury, dále je třeba zlepšit odezvu na pohromy, jejichž pravděpodobnost výskytu je malá, realizovat cvičení, provádět analýzy What, If, znovu zvažovat správnost rozhodnutí s cílem najít poučení pro zlepšení projektování další generace kritické infrastruktury. To znamená, že je potvrzeno vše, co pro zajištění bezpečnosti technických děl uvádíme v kapitolách 2 a 3. Prezentované konkrétní výsledky projektu CIPRNet jsou:

- zotavení infrastruktur je velmi pomalé po kaskádovitých nebo paralelních selhání infrastruktur,
- průměrná doba trvání selhání je různá: elektřina - 73 minut až 5 hodin; železnice – 1 den; dodávky plynu – 8 hodin; letiště – 2 dny,
- původci selhání jsou: lidský faktor a technické příčiny - EU 45%, USA + Kanada 36%; vzájemné závislosti - EU 25%, USA + Kanada 13%; živelní pohromy - EU 17%, USA + Kanada 46%; úmyslné narušení - EU 9%, USA + Kanada 5%,
- úroveň ochrany všech infrastruktur nemusí být stejná, protože dopady pohromy na infrastruktury také závisí na zranitelnosti určité infrastruktury,
- původci selhání v jednotlivých zemích a možné způsoby odezvy jsou v členských zemích EU rozdílné, tj. nepomůže společný standard řízení v EU.

Projekt CASCADE (grant agreement no.: 283068) je řešen 14 členskými zeměmi EU pod vedením nizozemského ústavu Soil Science Centre ve Wageningenu. [125,126]. Jeho zjištěním je:

- příčin selhání infrastruktur je velmi mnoho,
- pro zajištění ochrany kritické infrastruktury je třeba: zvažovat přístup All-Hazard-Approach; a analyzovat historické události.

To znamená, že je opět potvrzeno vše, co pro zajištění bezpečnosti technických děl uvádíme v kapitolách 2 a 3.

Z výsledků obou projektů vyplývá, státy z EU dostanou v nejlepším případě obecná doporučení, která lze získat studiem odborné literatury i praxe z provozu technických děl. Konkrétní systémy ochrany, tj. i vlastní programy na zajištění ochrany a bezpečnosti objektů kritické infrastruktury, si musí vytvořit, realizovat a zaplatit každá země sama. Proto je třeba zajistit vzdělanost v oblasti rizikového inženýrství.

5.3. Struktury technických děl a jejich charakteristiky

Jak již bylo několikrát výše uvedeno a na obrázku 6 znázorněno, tak pro zajištění bezpečnosti technických děl je třeba znát jak území, ve kterém je technické dílo, tak vlastnosti, kterými bude technické dílo ovlivňovat území během výstavby a provozu. V případě prvním jde především o zranitelnosti území a charakteristiky pohrom, které dané území postihují. V případě druhém jde o dopady technického díla na území za podmínek normálních, abnormálních, kritických až extrémních, a to především při provozu.

V případě infrastruktur je velmi důležitá topologie technického díla, tj. uspořádání technického díla v prostoru. U síťových technických děl, kterými jsou právě infrastruktury, jde o propojení různých prvků uvnitř a vně technického objektu. Topologie sítě výrazně definuje vlastnosti a možnosti provozu sítě. V praxi rozdělujeme fyzickou a logickou topologii. Fyzická topologie popisuje reálnou konstrukci sítě, jednotlivé uzly a fyzicky zapojená zařízení a jejich umístění včetně instalovaných kabelů, přesného umístění uzlů a přípojek mezi nimi. Logická topologie se vztahuje k tomu, jak jsou:

- u kybernetických sítí data v síti přenášena a kudy protékají z jednoho zařízení do druhého,
- jak se přesunují polotovary z jednoho výrobního zařízení na druhé,
- jak se přesunují energie, materiály, výrobky či služby z jednoho místa na druhé.

Je však skutečností, že logická topologie nemusí nutně kopírovat fyzické schéma sítě. Nejdůležitější a nejvíce používané topologie sítí jsou okružní a stromové. Okružní či smyčková síť je provedena jako uzavřený okruh. Stromová či větvená síť má tvar stromu.

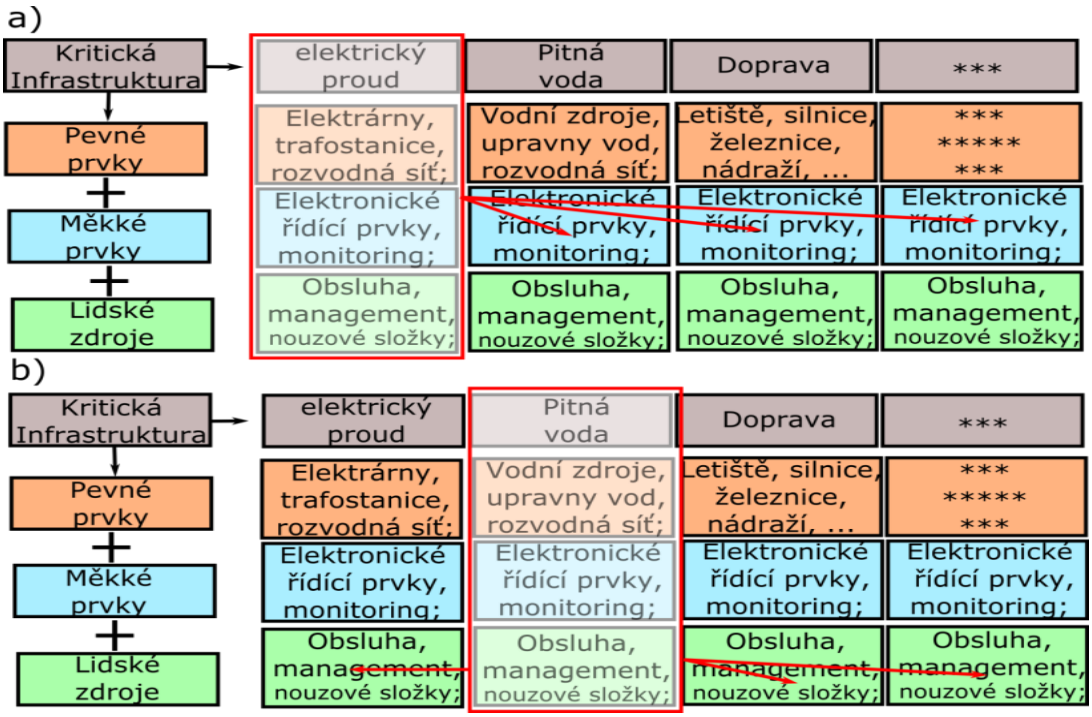
Právě sítím se budeme dále věnovat především, protože již více než 10 let je předmětem velké pozornosti odborníků i vedení států kritická infrastruktura. Předmětné položce budeme sice dále věnovat samostatný odstavec, ale na tomto místě považujeme za důležité ukázat jisté skutečnosti, které zaslouží pozornost a značně ovlivňují interoperabilitu a integritu sítí. Vlastnosti každé infrastruktury je nutno zkoumat z pohledu jak vnitřního uspořádání, tak vnějších vazeb na ostatní chráněná aktiva lidského systému i na ostatní infrastruktury.

Rozdíly, které působí vnitřní topologie sítí a procesů, ukážeme na obrázku 18. Předmětný obrázek porovnává selhání dodávek pitné vody a selhání dodávek elektrické energie na chráněná aktiva, které je v práci [127]. Sledovaný obrázek člení části infrastruktur na pevné prvky (hardware), měkké prvky (software) a lidské zdroje.

Pod pevné prvky patří fyzické stavby, liniové i bodové, nezbytné pro fungování poskytované služby od zdroje, přes transport po distribuci. Pevné prvky jsou v praxi ohroženy především živelními pohromami, technologickými haváriemi, či útoky. Pevné prvky by teoreticky mohly samy o sobě poskytovat službu. Nikoliv však v požadované podobě a rychle by vybočily ze svých funkčních rozsahů. Aby infrastruktura pracovala v požadovaném rozsahu a kvalitě, jsou nezbytné měkké prvky, které se skládají z nastavených procesů řízení a monitoringu. Procesy jsou prováděny buď kybernetickou podporou, nebo lidským personálem. Narušení měkkých prvků může být způsobeno selháním jiné infrastruktury (elektrická, kybernetická) nebo lidskou chybou, (rutina při vykonávání procesu, řízení - špatné nastavení procesů). I v případě, že bychom byli technologicky schopni sestavit autonomní infrastrukturu jenom z pevných a měkkých (kybernetických) prvků, tak ta by nemohla bez lidského faktoru dlouhodobě splňovat požadavky na ní kladené. Poslední část infrastruktur, lidské zdroje, má vliv při definování struktury sítě (fyzické i procesní). Lidské zdroje jsou nezbytné pro reagování na vývoj lidského systému, nové požadavky, nové hrozby. V neposlední řadě ještě mnoho rutinních procesů nejsme schopni adekvátně automatizovat. Lidské zdroje jsou zranitelné všemi pohromami [5].

Srovnání dopadů selhání dodávek elektrického proudu a selhání dodávek pitné vody ukazuje dopady na všechna chráněná aktiva, a tedy i na všechny typy infrastruktur. V případě selhání dodávek elektrického proudu jde o vyřazení měkkých prvků všech ostatních infrastruktur, které

tak přestanou také fungovat buď hned, nebo během několika hodin. Selhání dodávek pitné vody má o něco pomalejší vliv, působí však přímo na lidi a ostatní infrastruktury vyřazuje právě skrze lidské zdroje během několika dnů.



Obr. 18. Diagram vlivů selháni kritických infrastruktur na prvky ostatních kritických infrastruktur, a) selhání dodávek elektrického proudu, b) selhání dodávek pitné vody [127].

Na základě výše uvedených zřejmých rozdílů sledujeme nejprve odděleně infrastruktury a jejich technická díla, a teprve potom se věnujeme otázkám důsledků propojitelnosti, a tudíž vzájemné závislosti technických děl.

5.4. Specifická rizika technických děl

Z dříve uvedené teorie vyplývá, že správný postup pro vypořádání rizik začíná určením zvažovaných aktiv technického díla a jejich kontextu. Jelikož v praxi aktiva mají různou podstatu (prvky, vazby, spřažení vytvořená toky různého druhu), tj. náleží do oblasti fyzické, logické, organizační, kybernetické a sociální, tak nestačí sledovat jen technická aktiva, tj. zařízení, objekty a sítě, ale je třeba zvláště sledovat kybernetická aktiva a lidský faktor. Pro uvedení do problematiky uvedeme přehled velikosti rizik vztažených na lidské životy při různých lidských činnostech dle [128], tabulka 6. Z předmětné tabulky vyplývá, že riziko úmrtí je největší ve stavebnictví, těžbě uhlí a dopravě na silnicích.

Tabulka 6. Velikost specifických rizik v různých sektorech lidských činností dle [128].

Lidská činnost	**Typické riziko úmrtí x 10-6 za rok**
Stavebnictví	150 – 400
Průmysl	40
Těžba uhlí	300
Požáry objektů	8-24
Letectví	24

Silniční doprava	200
Železniční doprava	15
Selhání staveb	0.1

V souladu s údaji v kapitole 3 je třeba v sektorech s vysokým rizikem aplikovat systematický přístup a logiku řízení jednotlivých objektů a infrastruktur takto:

- 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 na opatření,
- aplikovat ochranná opatření,
- periodicky kontrolovat stav,
- udržovat ochranu na odpovídající úrovni,
- revidovat opatření v závislosti na vývoji.

Rozdělení kompetencí a odpovědností je zásadní a důležité v každé složitější činnosti lidské společnosti.

Další oblastí, kterou je třeba zvažovat, jsou současné způsoby využívání území vynucené sociálními a ekonomickými požadavky. Práce [2] uvádí, že ve vyspělých zemích z důvodu lepšího využití území, potřeb ochrany životního prostředí a splnění sociálních a ekonomických cílů lidí a lidské společnosti je dnes již běžné prostorové plánování. Jeho úkolem je řešit problematiku nejen území, ale také prostoru, protože výškové a podpovrchové objekty se stále více v praxi používají. Předmětné objekty, tj. jak technická díla, ale i výškové administrativní a obytné budovy se vyznačují specifickými zranitelnostmi (které působí velké obtíže např. při evakuaci lidí z budov při kritických podmínkách – příkladem jsou skutečnosti, které se objevily při požáru výškového domu v Londýně 14. 6. 2017 a při rychlých evakuacích následně nařízených v Londýně u podobných 5 budov z důvodu ochrany obyvatelstva). Z hlediska komplexní bezpečnosti je třeba zavést pravidla, aby nové zdroje rizik nepřevýšily únosnou míru rizik. Na tomto místě lze jen konstatovat, že předmětná problematika se v české praxi dosud neřeší.

Pro efektivní ochranu kritických objektů a infrastruktur, tj. významných technických děl, v ČR je nutné, aby byl určen nebo zřízen centrální úřad, který bude koordinovat záležitosti s mezinárodními institucemi, i na národní úrovni. Jasně by měla být vymezena odpovědnost parlamentu i vlády za zajištění ochrany jednotlivých sektorů, životně důležitých složitých technických děl a spoluodpovědnost jednotlivých vlastníků a provozovatelů důležitých složitých technických děl.

5.5. Výsledky studia rizik informačních systémů a návrh ochranných opatření

Informační technologie (IT) změnily svět, dochází k propojování různých sektorů mezi sebou, a tím i různých států navzájem. Produktovody a komunikace překračují hranice, elektrické soustavy jsou propojeny, finanční a telekomunikační systémy jsou vzájemně provázané. Dálková řízení technologických celků, přenos dat a internetová spojení mají pro lidskou společnost bezesporu velký přínos na jedné straně, ale na druhé straně jejich nesprávné funkce spojené s provozním nebo organizačním selháním či lidským úmyslem jsou pohromami, protože iniciují nouzové situace s rozsáhlými dopady. Je prokázané, že vážná porucha některého sektoru v jednom státě může mít vážné dopady na jiný stát a na celá společenství států. Proto jsou předmětem výzkumu.

5.5.1. Problémy informačních technologií

Zatímco fyzické a organizační technologie mají za sebou určitý historický vývoj a pro zajištění jejich bezpečnosti existují postupy, standardy a normy, informační (kybernetická) technologie a její infrastruktura jsou vcelku nové, a proto v současné době má jejich problematika zvláštní postavení. Důvodem tohoto stavu je skutečnost, že doposud nejsou kvalifikované standardy pro snížení zranitelnosti kybernetických systémů (tj. IT). Ke specifickému postavení kybernetické infrastruktury přispěla také analýza teroristických útoků spočívající v ocenění schopnosti teroristů použít nástroje IT k poškození veřejných aktiv, a to i důležitých technických děl, která jsou součástí kritické infrastruktury [129-133].

Předmětné problémy se systematicky řeší v USA od počátku devadesátých let minulého století, v EU od r. 2002, řeší se v rámci G8 atd. [129,130,134,135]. Ochrana kritické informační infrastruktury je předmětem projektů EU (CI2RCO, MERCI atd.), které se zaměřují na zabezpečení její ochrany proti pohromám všeho druhu [130].

Je faktem, že kybernetická infrastruktura je zásadní pro sběr, analýzu a šíření informací napříč podnikem, organizací a ve veřejném sektoru. Informační systém představuje soubor všech prvků, vazeb a toků, které se podílejí na distribuci a zpracování informací v čase a prostoru. Komunikační systém je pak podmnožina, která je zaměřená na distribuci informací.

Na základě současného poznání shrnutého v pracích [130,131] lze kybernetický systém popsat následovně:

1. Struktura celého kybernetického systému, tj. informačních a komunikačních systémů dohromady má tři základní části, a to: procesní strukturu; technickou strukturu (hardware); a programovou strukturu (software). Jednotlivé prvky a části jsou vzájemně provázané, tj. vzájemně závislé.
2. Procesní struktura popisuje logiku systému, tj. popisuje, jaká data se mají kam a kdy distribuovat, jak se data získávají, zpracovávají, uchovávají atd., a zahrnuje řídící procesy, produkční procesy a servisní procesy. Řídící procesy jsou procesy, které organizují jednotlivé prvky a činnosti systému a zajišťují komunikaci s okolím. Produkční procesy jsou procesy zaměřené na produkci, tj. na vytváření užitné hodnoty. Servisní procesy jsou procesy, které řeší podpůrné činnosti efektivního a bezpečného fungování, které zajišťuje obsluhu společnosti. Při výpadku procesní struktury ztrácí technická i programová struktura svůj význam, a to vše dohromady způsobuje kritičnost systému.
3. Technická struktura popisuje technické prostředky a prostředí realizace systému. Skládá se z výpočetní techniky, periferní a podpůrné techniky, komunikační techniky a z transportních médií. Výpočetní technika představuje vlastní místo zpracování dat, tj. servery, PC, notebooky atd. Periferní a podpůrná technika zahrnuje prostředky, které zvyšují efektivitu a bezpečnost systému, tj. tiskárny, scannery, zálohovací zařízení apod. Komunikační technika zahrnuje komponenty, které vstupují do komunikace, tj. modemy, routery, switche, firewally atd. Transportní média jsou média, která umožňují přenos dat, tj. datové kabely (metal / optika), mikrovlnné spojení, diskety, CD apod.
4. Programová struktura představuje vytvořené programy a aplikace, tj. realizující část procesní struktury na technické struktuře. Skládá se z řídicích systémů, z produkčních a servisních systémů. Řídicí systémy jsou systémy podporující řídící procesy, které jsou orientovány na řízení úkolů, sledování a vyhodnocování efektivity provozu a na řešení vztahů k zaměstnancům, okolním společnostem a státu. Dělí se následovně: ekonomické a účetní systémy; systémy na podporu rozhodování; plánovací systémy atd. Produkční systémy jsou zaměřené na vytváření vlastních výrobků. Servisní systémy jsou systémy a aplikace, které zajišťují bezpečnost a efektivní činnost společnosti. Dělí se takto: operační, bezpečnostní a zálohovací, a komunikační systémy.

5. Provedená inventarizace systému ukazuje, že pro zajištění bezpečnosti kybernetické infrastruktury se musí sledovat následující prvky systému a jejich vzájemné vazby: procesy; datové množiny; software; hardware; lidi; a dokumentace.

5.5.2. Příklady selhání kybernetických systémů

V souvislostech, které v práci sledujeme, selhání kybernetických systémů znamená selhání technických děl; uvedeme několik příkladů z praxe:

1. Dne 12. prosince 2014 došlo v centru pro řízení letového provozu (NATS) ve městě Swanwick k selhání řídícího počítače a jeho záloh v důsledku špatně nakonfigurovaného maximálního počtu uživatelských rolí. Proto bylo zrušeno přibližně 150 letů, 20 dalších přesměrováno mimo vzdušný prostor Velké Británie a 353 letů bylo zpožděno. Náprava pomocí automatizovaných nástrojů a auditu logů byla provedena pracovníky odborné jednotky ETIC a systém byl po několika hodinách restartován jako plně funkční [136].
2. Pravděpodobný kybernetický útok na ropovod BTC (Baku-Tbilisi-Ceyhan) byl příčinou vzniku trhliny v ropovodu a následného požáru v srpnu roku 2008 v Turecku. Ropovod byl v důsledku uvedeného požáru mimo provoz 19 dní. Podle autorů práce [137] útočníci pronikli do IP kamerového systému a následně buď skrze něj, nebo pomocí fyzického přístupu, pronikli k řídícím (a dalším) systémům, pomocí nichž provedli změnu tlaku v ropovodu; tj. ke zvýšení tlaku nad povolenou hodnotu, což vedlo ke vzniku trhliny a k následným jevům.
3. V práci [138] je popsáno 15 kybernetických útoků na průmyslové řídicí systémy (používající software SCADA) v letech 1982 - 2012, a to konkrétně:
   - výbuch sibiřského plynovodu (1982),
   - vyřazení poplachového systému v rafinerii firmy Chevron v Kalifornii (1992),
   - neoprávněný přístup do systému Salt River Project v Arizoně (1994),
   - vyřazení počítače telefonní společnosti, který řídil spojení s letištěm Worchester v Massachusetts (1997),
   - útok na systémy ruské společnosti Gazprom (1999),
   - únik a následný požár benzínu z produktovodu v Bellinghamu ve Washingtonu (1999),
   - útok vedoucí k vypuštění odpadní vody do řeky v Qeenslandu v Austrálii (2000),
   - průnik do systému Cal-ISO v Kalifornii (2001),
   - vyřazení některých systémů jaderné elektrárny Davis-Besse v Ohiu v důsledku infekce červem SQL Slammer (2003),
   - vyřazení systému pro řízení vlakové dopravy ve státě Florida v důsledku infekce červem Sobig (2003),
   - zavedení neautorizovaného programu do systému Tehama Colusa Canal Authority v Kalifornii (2007),
   - destrukce odstředivek v zařízení v Natanz v Iránu (2010),
   - útoky na nadnárodní společnosti energetického sektoru nazvané Night Dragon (2011),
   - objevení špionážního programu Duqu (2011),
   - objevení špionážního programu Flame (2012).
4. V roce 2014 došlo k útoku na německou ocelárnu společnosti ThyssenKrupp, při kterém byly vyřazeny komponenty řídicího systému z provozu. V důsledku toho nebylo možné provést vypnutí tavící pece a došlo fyzickému poškození tohoto technického zařízení. Popisovaný útok byl realizován pomocí spear-phishingu zaměřeného na operátory průmyslových systémů [139]. Pomocí spear-phishingu získali útočníci přístup do vnitřní sítě ocelárny a k ní připojeným řídicím systémům technických zařízení.

5. Studie [140] popisuje průběh kybernetických útoků na bezdrátově komunikující SCADA systémy řídící tok odpadních vod v oblasti Maroochy Shire (Queensland, Austrálie) realizovaných v období od ledna do dubna 2000. Podvržením specifických identifikátorů v rámci bezdrátového komunikačního protokolu užívaného infrastrukturou získal útočník možnost zasahovat do funkce pump odpadních vod. V důsledku útočníkem vložených zpráv nebyly vybrané pumpy zapínány v době, kdy měly dle nastavení systému běžet, a komunikace dalších pump s centrálním počítačem byla přerušena. Výsledkem útoků byl mimo jiné únik 800 000 litrů odpadních vod a následné zamoření několika parků, řek a pozemku blízkého hotelu. Útoky byly zastaveny pomocí detekce rádiového signálu útočníka vyšetřovateli incidentu a jeho následným zadržením. V citované práci je popis výše uvedených útoků následován popisem v době útoků realizovaných bezpečnostních opatření a jejich konfrontací se standardem NIST SP 800-53. Na základě uvedeného standardu jsou následně také popsána opatření, která mohla daným útokům zamezit (např. monitorování/omezení vzdáleného přístupu, management uživatelských účtů apod.).
6. V Bellingtonu ve státě Washington (USA) došlo 10. června 1999 k prasknutí produktovodu a úniku benzínu do dvou blízkých potoků. Následné vznícení uniklé tekutiny způsobilo výbuch, v jehož důsledku byly usmrceny 3 osoby a došlo k úniku dalších téměř 950 000 litrů benzínu. K prasknutí produktovodu došlo v důsledku zvýšeného vnitřního tlaku kombinovaného s fyzickým porušením produktovodu, nefunkčností ventilů pro vyrovnávání tlaků a současnou nefunkčností SCADA systému užívaného pro ovládání produktovodu [141].

5.5.3. Příčiny a dopady selhání kybernetických infrastruktur

Analýzy situací odstartovanými selháními IT v databázi [12] a ve světové databázi EM-DAT [142] odhalily příčiny selhání kybernetické infrastruktury a jejich dopady na veřejná aktiva. Jejich shrnutí ukazuje, že jde o:

1. Překročení (přetížení) přenosové kapacity vlastní telekomunikační sítě.
2. Havárie technologických celků.
3. Cílené poškození informační a komunikační infrastruktury (sabotáž, hackerství, terorismus, kriminální činnost apod.).
4. Ztrátu integrity dat v informačním systému.
5. Živelní pohromy velkého rozsahu jako rozsáhlé požáry, vichřice, sesuvy půdy, povodně apod. s následným poškozením nebo výpadkem informačních a komunikačních systémů (IKS).
6. Radiační havárie s následným poškozením nebo výpadkem řídicího systému objektu.
7. Havárie velkého rozsahu způsobené vybranými nebezpečnými chemickými látkami a chemickými přípravky s následným poškozením nebo výpadkem řídicího systému objektu.
8. Jiné technické a technologické havárie velkého rozsahu – požáry, exploze, destrukce nadzemních a pozemních částí staveb s následným poškozením nebo výpadkem IKS.
9. Destrukce hrází vodohospodářských děl se vznikem povodňové vlny s následným poškozením nebo výpadkem řídicího systému objektu.
10. Narušení dodávek elektrické energie velkého rozsahu.
11. Narušení zákonnosti velkého rozsahu s následným poškozením nebo výpadkem řídicího systému objektu.
12. Výpadky veřejných telekomunikačních sítí.
13. Disfunkční chování řídících a informačních systémů při zabezpečování základních funkcí státu.
14. Výpadek kritických informačních systémů nebo procesů.

Z výše uvedených poznatků, analýz a simulací v pracích [11,12,130-133,136-141] vyplývá:

1. Pohromy, tj. jevy, které působí škody na kybernetickém systému a jeho infrastruktuře, mají původ:
   - v samotné technologii a infrastruktuře systému (konstrukce, spolehlivost, materiál, provoz, organizace apod.),
   - ve vnějších pohromách (živelní pohromy, výpadek elektrické energie, nehody a havárie technologických celků – požár, exploze, kontaminace nebezpečnými látkami),
   - v lidském faktoru (selhání lidí, vandalismus, krádeže apod.),
   - v lidském úmyslu (viry, hacking, zneužití technologií proti lidem, skupinám, státům, terorismus apod.).
2. Dopady pohrom na aktiva kybernetického systému a jeho infrastruktury znamenají selhání řídicích systémů, jejichž činnost realizují.
3. Dopady pohrom na aktiva kybernetického systému a jeho infrastruktury, které se dále přenáší na veřejná aktiva, jsou přímé a nepřímé; např. dopady na bezpečí lidí jsou: psychická újma; kolaps naváděcích systémů; kolaps obranyschopnosti státu; policie nemůže využívat počítačové databáze; selhání bezpečnostních zařízení – zvýšení kriminality; nemožnost zajištění bezpečnosti letecké dopravy; kolaps v městské hromadné dopravě; nedostatek informací – občanské nepokoje; selhání přístupu k bankomatům; nefunkčnost dodávek tepla, elektrické energie aj.; problém v zabezpečení budov a následných kontrol lidí; nemožnost vyplácet sociální dávky a důchody apod.

Celkový přehled možných dopadů dlouhodobého selhání kybernetického systému na veřejná aktiva odvozený metodou What, If pomocí dat od 115 respondentů z veřejné správy v EU, kteří řeší bezpečnostní otázky, získané v rámci šetření prováděných během projektu FOCUS [12,19] lze shrnout takto:

1. Možné dopady na životy a zdraví lidí: ztráty na životech a poškození zdraví kvůli selhání zdravotní péče (nemožnost provádět operace), výpadek obslužných zařízení (roboti); ztráta zdravotnických výkonů založených na provozech přístrojů řízených počítačem; znemožnění akutních zákroků vedených pomocí počítačů; selhání počítačů hlídajících životně důležité funkce pacientů; zpomalení nemožnost transfuzí kvůli kolapsu registrů dárců krve a kostní dřeně; zpomalení operací - např. kolaps registrů pacientů čekajících na transplantaci orgánů; zhoršení zdravotní péče o nemocné kvůli laboratořím a oddělením závislým na počítačích; výpadky v péči kvůli nefunkčnosti záložních systémů nemocnic, centrální kartotéky (např. alergičtí lidé mohou být vystavení riziku léčby látkou, na kterou jsou alergičtí); poškození zdraví osob v souvislosti s nemožností předání lékařských zpráv; ztížená situace v podávání léků; nekvalitní zdravotní péče v důsledku ztráty cenných a citlivých informací; otravy lidí v důsledku znečištěné pitné vody, protože nefunguje kontrolní systém; škody na zdraví způsobené snížením úrovně hygieny kvůli výpadku čistících systémů; nemožnosti uspokojení základních lidských potřeb; při krachu firem možnost sebevraždy jejich majitelů apod.
2. Možné dopady na bezpečí lidí: psychická újma při uvíznutí v uzavřeném prostoru, např. v soupravě metra; vojenská technika je řízena elektronicky – při selhání řídicího systému je možné, že se samočinně aktivuje; kolaps naváděcích systémů, obranyschopnosti státu; ohrožena celková bezpečnost státu např. selhání spojení s vesmírnými družicemi a jinými navigačními systémy; komplikovanější práce policie a záchranných sborů; policie nemůže využívat počítačové databáze – registr vozidel, zjišťování a ověřování totožnosti, porovnávání stop (otisky prstů, balistika); špatná komunikace s nouzovou službou; růst kriminality; selhání bezpečnostních zařízení – zvýšení kriminality; kolaps komunikace mezi státní a mezinárodní policií; problémy s udržením veřejného pořádku a s tím spojený pokles důvěry v práci bezpečnostních složek; ztráta důvěry v koordinaci složek; nemožnost zajištění bezpečnosti letecké dopravy; kolaps kontroly a bezpečí v městské hromadné dopravě; nedostatek informací a z toho vyplývající dezorientace, pocit bezmoci, informační

kolaps; kolaps zpravodajství; vznik paniky, chaosu z nedostatku informací; občanské nepokoje; selhání přístupu k bankomatům, a tím k vlastním financím; nefunkčnost dodávek tepla, elektrické energií a jiných médií; požární hlásiče mimo provoz; problém v zabezpečení budov a následných kontrol lidí; nefunguje noční pouliční osvětlení; zhoršená komunikace mezi lidmi a jednotlivými institucemi a také mezi lidmi samotnými (zejména nemožnost komunikace přes internet, posílání emailů); lidé nebudou chodit do práce – nebudou výplaty; ztráta spojení s okolním světem; nemožnost vyplácet sociální dávky a důchody; ztráta dat uložených v počítači; zastavení vesmírných misí a programů apod.

3. Možné dopady na majetek: škody na objektech, zařízení, infrastrukturách a technologiích vyvolané dopravními a technologickými haváriemi vzniklými v důsledku selhání počítačových systémů; škody způsobené požárem (z důvodu ztráty funkčnosti regulačních mechanismů); škody způsobené vodou v souvislosti s nemožností převodu dat ohledně automatických systémů hašení; škody na domácích zvířatech způsobené selháním obslužných krmných procesů, případně regulací množství potravy; při dlouhodobějším výpadku sítě možnosti ohrožení ekonomiky státu; zatížení pojišťoven díky povinnosti úhrady škod; nemožnost plnit pohledávky a uspokojovat potřeby při nemožnosti přístupu k finančním prostředkům; selhání bezpečnostních systémů – krádeže majetku; škody na technologiích a jiném majetku vyvolané náhlým selháním informačních systémů doprovázené únikem nebezpečných tekutin a plynů + ztráty v důsledku výpadků výroby v provozech; škody na majetku vzniklé v důsledku nefunkčností techniky řízené počítačem apod.
4. Možné dopady na veřejné blaho: nefunkčnost správy věcí veřejných, protože státní správa nebude fungovat (ztráta uložených dat v informačních systémech); neplnění nároků občanů – nejsou data → nemožnost dostát všem úkolům vyplývajícím z odpovědností stanovených zákony o státní správě a samosprávě (nemožnost vydávat např. cestovní doklady, řidičské průkazy); snížení schopnosti řídit odezvu na nouzovou situaci; výpadek městské hromadné dopravy; oslabený pohyb lidí - při výpadku řídicích systémů dojde k mnoha haváriím v dopravě a nastane problém s přepravou lidí; kolaps letecké dopravy – letadla jsou řízena přes počítač; na letištích zůstane plno lidí, jelikož nemohou projít kontrolou a odbavovacím prostorem, a tudíž ani odletět, jelikož celá navigace se řídí pomocí počítače; čerpací stanice přestanou fungovat → omezena doprava i osobními automobily; nemožnost kontroly výdeje pohonných hmot u benzinových stanic; ztížený lodní a železniční provoz; kolaps podzemní dráhy; nedostatek tepla – energie; selhání dodávek vody do domácností, veřejných zařízení i provozů (regulační mechanismy, řídící mechanismy); selhání veřejného osvětlení; omezení sektoru služeb; znatelný odraz v projevech zasahujících do celého hospodářství a ekonomiky; ztráta informovanosti pocházející z informačních zdrojů; snížená možnost komunikace; zastavení obchodování plynoucí přes internet apod.
5. Možné dopady na životní prostředí: škody na technologiích vyvolané výpadkem počítačové infrastruktury → únik nebezpečných látek; k přenosu informací se použijí alternativní zdroje, které jsou méně šetrné k životnímu prostředí; selhání předávání a přijímání informací zabrání rychlému a efektivnímu odstranění ekologických havárií; havárie v průmyslových podnicích; ztráta funkčnosti chladících zařízení a čističek – únik nebezpečných látek – kontaminace vody – úhyn vodních živočichů a rostlin; o život přijdou někteří živočichové v důsledku znečištění životního prostředí; kontaminace v důsledku nefunkčnosti čističek odpadních vod; snížená kontrola úniku nebezpečných látek do vod; ztráta řízení kanalizačního systému vede ke kontaminaci složek životního prostředí; ztráta kontroly emisí → kontaminace ovzduší; selhání chemických reakcí v chemických závodech vedoucí k úniku nebezpečných látek do životního prostředí; zastavení provozů na zpracování a likvidaci odpadů → hromadění odpadů a všech problémů s tím spojených;

ztráta monitoringů a funkčnosti varovacích systémů (např. na vodních tocích před povodněmi); zvýšení plynných, kapalných a tepelných emisí do životního prostředí v důsledku chaotického předávání informací do programů řídících čističky, odlučovače, chladící zařízení aj.; ztráty řízení nad ropovody, plynovody a jinými produktovody a tím dojde k omezení dodávek a k haváriím apod.

6. Možné dopady na infrastruktury a technologie, které se dále člení:
   - možné dopady na dodávky energií (elektřina, teplo, plyn): ztráta osvětlení; nefunkčnost dodávek tepla, elektrické energie a jiných médií; výpadky ovládacích systémů v elektrárnách, teplárnách apod.
   - možné dopady na dodávky vody: selhání dodávek do průmyslu → odstavení elektráren (nemají vodu na chlazení); selhání dodávek vody do domácností, veřejných zařízení i provozů (regulační mechanismy, řídicí systémy); kvalita pitné vody se zhorší kvůli nedostatečnému vyčištění – není kontrola apod.
   - možné dopady na kanalizační systém: ztráta řízení kanalizačního systému; to znamená špatná funkčnost kanalizace, odstavení čističek odpadních vod apod.
   - možné dopady na přepravní síť: ztráta dopravního spojení; kolaps celé dopravní sítě; selhání řídících jednotek (nemožnost pilota letadla navázat kontakt s řídící věží, navigace); selhání regulačních mechanismů (světla na křižovatkách, tunelech atd.); selhání dopravní obslužnosti založené na kybernetice; zvýšený počet nehod v důsledku nefunkčnosti světelných semaforů; nefungují celnice, lidé uvíznou v kolonách na hranicích; čerpací stanice přestanou fungovat; kolaps kontroly a bezpečnosti městské hromadné dopravy; dopravní zácpy, dopravní nehody a postupem času nedostatek potravin v důsledku uvíznutí přepravních prostředků ve frontách apod.
   - možné dopady na kybernetickou infrastrukturu (komunikační a informační sítě): kaskádový efekt v systémech a sítích – poničení nebo zničení databází informací, nemožnost kontroly a řízení přes kybernetickou síť; ztráta spojení a zdrojů informací; cenná nezálohovaná data budou zničena; zhroucení komunikačních sítí domácích i zahraničních; selhání satelitové komunikace; selhání bezpečnostních zařízení; v případě ohrožení života nemožnost informovat záchranné sbory apod.
   - možné dopady na bankovní a finanční sektor: nebude přístup k peněžním prostředkům – bankomaty; selhání e-bank; dojde k vymazání centrálního serveru banky a tím i k zániku účtu klientů a k selhání obslužnosti klientů; nemožnost plnit pohledávky a uspokojovat potřeby při nemožnosti přístupu k peněžním prostředkům; nelze moci manipulovat s finančními prostředky v bankách; nemožnost nákupu a prodeje akcií; nedostupnost informací o vývoji světových cen (ropa, měnový kurz, ceny surovin); ztráty na finančním trhu v důsledku sankcí za neprovedené transakce a za promarněné příležitosti; omezení peněžního obchodování; zatížení pojišťoven díky povinnosti úhrady škod; nestabilita domácí měny; kolaps bank; burzovní ztráty apod.
   - možné dopady na nouzové služby (policie, hasiči, zdravotníci): ztráta spojení založeného na informačních systémech (problémy s varováním obyvatelstva); ve zdravotnictví ztráta schopnosti provádět operace a poskytovat péči založenou na provozech přístrojů řízených počítačem; nemožnost navázání spojení s nouzovými službami; oslabení akceschopnosti služeb; ohrožení záložních systémů nemocnic; nemožnost přístupu k databázovým údajům; kolaps komunikace mezi státní a mezinárodní policií apod.
   - možné dopady na základní služby v území (zásobování potravinami, likvidace odpadů, sociální služby, pohřební služby), průmysl a zemědělství: ztížení řízení výroby; selhání všeho, co je závislé na výpočetní technice; nefunkčnost dodávek a služeb závislých na elektrické energii; dlouhodobý výpadek informačních sítí a následně i elektrických sítí citelně ovlivní průmysl, zastaví provozy závislých na provozu zařízení počítačem,

zastaví provozy na zpracování a likvidaci odpadů, zastaví zemědělské provozy závislé na provozu počítače, zastaví přístroje v továrnách závislé na provozu počítačů; zastaví obchodování přes internet; zastaví poštovní služby; způsobí kolaps v zásobování; zhroucení obchodního systému (zastavení prodeje, znehodnocení potravin a z toho plynoucí finanční ztráty; krach internetových firem apod.

- možné dopady na státní správu a samosprávu: ztráta dat potřebných pro zprávu pocházejících z informačních zdrojů; přerušení spojení a ztráta vzájemné komunikace a komunikace s občany; znemožnění spolupráce mezi úřady; kvůli ztrátě zdrojů dat nemožnost plnit úkoly vyplývající z odpovědnosti státní správy a samosprávy (nemožnost např. vydávat cestovní doklady a řidičské průkazy); kolaps sociálního systému (lidé nedostávají státní dávky) apod.

Je si třeba uvědomit, že přerušení (narušení) poskytování telekomunikačních a informačních služeb může také způsobit:

1. Narušení (znemožnění) koordinovaného postupu orgánů krizového řízení, orgánů veřejné správy a samosprávy a složek integrovaného záchranného systému.
2. Ochromení nebo omezení činnosti orgánů státu a organizací pověřených výkonem veřejné správy.
3. Ztrátu informační podpory v krizové situaci.
4. Narušení řídících a monitorovacích systémů orgánů krizového řízení závislých na přístupu k datovým zdrojům a přenosu informací.
5. Ochromení nebo omezení činnosti subjektů kritické infrastruktury státu.
6. Četnost a nepřetržitost poskytování informační podpory pro veřejnost.

Z důvodu rozvoje průmyslu i veřejného sektoru se stále zvyšuje efektivnost a výkon kybernetických infrastruktur. Dnes jsou moderní inteligentní sítě (anglicky Smart grids), což jsou silové elektrické a komunikační sítě, které umožňují regulovat výrobu a spotřebu elektrické energie v reálném čase, jak v místním, tak v globálním měřítku. Jejich principem je interaktivní obousměrná komunikace mezi výrobními zdroji a spotřebiči nebo spotřebiteli o aktuálních možnostech výroby a spotřeby energie. Ochránci soukromí a bezpečnostní odborníci však varují před sledovacím potenciálem a náchylností této technologie [143,144], kterou mohou využít i zloději [145]. Předmětné sítě zahrnuje digitální kontrolní a řídicí systém, integrované senzory monitorující chování sítě a automatické obnovování provozu po poruše. Součástí je dostupnost informací v reálném čase o zatížení sítě, kvalitě dodávky, přerušení apod. Z pohledu poznání v kapitolách 2 a 3 je třeba počítat se selháními těchto sítí, protože jsou vysoce zranitelné a mít připravené kvalitní odezvy na možná selhání, a to včetně materiálního, technického, finančního a personálního zajištění.

V reálném životě v důsledku použití IT roste závislost na IT, a tím i roste zranitelnost technologií. Síťování IT (LAN, WAN, internet) zvýšilo počáteční potenciál rizika způsobený činností vnitřních pachatelů (insiderů). Vývoj síťování způsobil, že v dnešní době roste rychle počet externích pachatelů, kteří s poměrně omezenými prostředky (počítač, modem, telefonní přípojka a přístup na internet) a nepatrnými odbornými znalostmi jsou schopni rušit informační techniku důležitých oblastí infrastruktur [146]. Mobilní spojovací systémy elektronických komunikací jsou tak novými pohromami pro kybernetické systémy, a tím i pro společnost. Bohužel dopady předmětných pohrom v důsledku vzájemných propojení mají potenciál působit i mimo hranice států.

Tyto nové druhy pohrom (ve vojenském slangu hrozeb) vyžadují pečlivé pozorování vznikajících bezpečnostních otázek IT a také vypracování ochranných opatření. Přitom je třeba zajistit, aby ti, co odpovídají za vnitřní a vnější bezpečnost stejně jako ti, kteří odpovídají za bezpečnost komerčních systémů, vytvořili relevantní scénáře těchto pohrom (hrozeb) a vypracovali společné pomocné strategie ochrany a obrany.

V rámci našeho výzkumu [147] byly sledovány nástroje, kterými dochází k narušení kybernetických systémů, a to malware, phishing, spear-phishing, whaling a hacking. Jejich charakteristiky jsou následující:

1. Malware znamená škodlivý kód, který se infikuje do počítače pomocí různých programů. Zřejmě nejznámějšími druhy malware jsou viry, červy a trojské koně. Na obecné úrovni jsou viry programy schopné kopírování sebe sama (tzv. replikace) a červy jsou jejich podtypem, který pro své šíření nejčastěji využívá prostředky kybernetické sítě či e-mail (není to však pravidlem). Trojské koně jsou programy, které mají buď funkci rozdílnou od té, která je avizována (trojský kůň například může vypadat, jako počítačová hra), anebo bez vědomí uživatele provádějí v rámci systému určitou skrytou (škodlivou) činnost. Tou může být předávání určitého typu dat uživatele útočníkovi, umožnění vzdáleného převzetí kontroly nad infikovaným systémem, atd. Na rozdíl od virů a červů, nejsou schopny autonomní replikace, v praxi jsou tedy většinou šířeny útočníkem, manuálně či například pomocí automatizovaného rozesílání v přílohách e-mailů. V citované práci jsou detailně popsány červ Sircam, červ SQL Slammer / Saphire / Helkern, červ Stuxnet, trojský kůň Red October / Rocra, červ Flame, červ Gauss, trojský kůň Wiper, trojský kůň MiniDuke.
2. Manipulace cílové osoby útočníkem k tomu, aby provedla nějakou akci. Nejrozšířenější způsob manipulace je phishing, při němž je cílová osoba kontaktována pomocí e-mailu. Dle úrovně zaměřenosti útoku na specifický cíl můžeme rozlišovat tři různé varianty phishingu: klasický phishing; spear-phishing; a whaling. Při klasickém phishingovém útoku jsou rozesílány vysoké počty zpráv na de-facto náhodné e-mailové adresy. Text všech odeslaných zpráv v rámci jedné phishingové kampaně bývá v daném případě stejný, útočník se pomocí něj často snaží uživatele přesvědčit k zaslání soukromých dat, zadání bankovních informací na určité webové stránce, zaslání finančních prostředků, či k otevření určitého odkazu v prohlížeči. Popsaný typ zpráv tvoří značné procento spamu rozesílaného v rámci internetu a je též jednou z cest, kterou se šíří výše diskutované červy a trojské koně. Spear-phishing je podstatně sofistikovanější pohromou (hrozbou). Cílem je při něm získat konkrétní informace, data, či přístupové údaje od specifické skupiny osob, tradičně několika zaměstnanců jedné instituce. Při spear-phishingu jsou tudíž zprávy zasílány pouze na nízký počet adres, jejich obsah také zpravidla působí věrohodnějším dojmem, než v případě klasického phishingu. Toho je často dosaženo pomocí podvržení identity odesilatele zprávy – zasílané e-maily pak budí dojem, že jejich autorem je například nadřízený pracovník, nebo administrátor informačního systému organizace. Nejsofistikovanější a zároveň nejcílenější formou phishingu je tzv. whaling. Při něm bývá příjemcem zpráv pouze jediná (v rámci cílové organizace zpravidla vysoce postavená) osoba a záměrem útočníka bývá získání specifických dat – velmi často například přihlašovacích údajů k informačním systémům organizace. Obsah i formát zpráv bývá vytvořen specificky pro cílovou osobu, o níž útočník předem shromáždil určité informace, působí tedy zpravidla velmi důvěryhodně. V rámci phishingových kampaní obecně a specificky v případě sofistikovanějších variant útočníci často do zpráv vkládají odkazy na webové portály, které sami vytvořili a které budí dojem např. oficiálních stránek pro přístup k elektronické poště, či přístupového bodu do informačního systému organizace. To umožňuje snáze získat přihlašovací údaje cílové osoby a navíc pomáhá zvýšit důvěryhodnost související zprávy.
   V podmínkách reálného světa je phishing, jak již bylo zmíněno, velmi rozšířenou formou útoku využívajícího kybernetické prostředky.
3. Hackerské útoky mají mnoho různých podob. Nejvýše škodlivou formou dle současných znalostí pokus o obecný průnik do sítě a útok na dostupnost služeb, DoS (Denial of Service). Obecný pokus o průnik do sítě lze realizovat mnoha metodami. První krok je ve většině případů stejný. Je jím tzv. skenování, tedy zjišťování možností, které cíl nabízí – v praxi jde zejména o detekci otevřených portů a na nich naslouchajících aplikací. Na základě

oskenování cílového systému je možné určit další vhodný postup při průniku. Průběh skenování je však na straně cíle možno detekovat a reagovat na něj odpovídajícími opatřeními. V druhém případě jde o velmi jednoduchou formu útoku, spočívající v zahlcení kybernetické infrastruktury cíle datovými toky, které není infrastruktura schopna zpracovávat, tj. všechny infrastrukturou poskytované služby se stávají nedostupnými a často dochází k pádu celého systému. DoS útok se realizuje několika způsoby; nejjednodušší je prosté generování vysokého počtu požadavků (např. na předání konkrétní webové stránky) útočníkem a jejich předávání cílovému systému (např. webovému serveru). Uvedený útok neklade vysoké nároky na výpočetní kapacity zdrojového informačního systému a je možné jej tedy realizovat s de-facto libovolným počítačem jako zdrojem. Účinnost klasického DoS útoku bývá nejčastěji omezena rychlostí, s níž je útočník schopen odesílat požadavky (tedy rychlostí připojení k internetu), což ve většině případů činí datové toky generované jednoduchým DoS útokem nedostatečnými pro úplné vyřazení cílového systému či služby z provozu. V praxi je možné se setkat s velkým množstvím postupů, umožňujících zvýšení účinnosti popsaného typu útoku, například pomocí využití systémů třetí strany pro zesílení útoku (k posílení datových toků) nebo využitím slabin ve specifických softwarových komponentách užívaných cílovým systémem. Obecně je však nejčastější pokročilou formou útoku na dostupnost služeb jeho distribuovaná varianta, DDoS (Distributed Denial of Service). Při tomto typu útoku je datový tok zaměřený na cíl generován více zdroji současně, výsledkem čehož je zahlcení cíle snazší. Hackerských útoků typu DDoS bylo v rámci České republiky provedeno mnoho, vhodným příkladem s regionálními, resp. národními dopady bylo například vyřazení webového serveru Vlády ČR v roce 2012 v důsledku útoku provedeného skupinou Anonymous na protest proti dohodě ACTA [148].

Kybernetická infrastruktura zajišťuje provoz informačních a komunikačních technologií (ICT), a proto je jednou z nejdůležitějších součástí kritické infrastruktury. Proto stát musí ochraňovat a rozvíjet předmětné technologie, pokud má ambice vykonávat řádně veřejnou moc. Kvalita systémů informačních a komunikačních technologií je zásadní pro sběr, analýzu a šíření informací napříč celou státní organizací a na veřejnosti. Řízení kybernetické infrastruktury zahrnuje procesy, organizační aspekty a nástroje s cílem poskytovat stabilní komunikační a technologickou infrastrukturu.

Při definici řídících procesů nutných pro poskytování kvalitních služeb kybernetické infrastruktury je nutné vycházet z logické úvahy, že hlavní parametry těchto procesů by měly vycházet z požadavků efektivního výkonu veřejné moci. Dobré plánování, administrace a kontrola jednotlivých činností jsou pak klíčem k zajištění, že služby poskytované pomocí kybernetické infrastruktury jsou vytvářeny a naplňovány v souladu s požadavky efektivního výkonu veřejné moci. Zároveň je pak pomocí definovaných principů možné řídit kybernetickou infrastrukturu nákladově účelným způsobem. Aktivity spojené s plánováním, administrací a kontrolou kybernetické infrastruktury v sobě obsahují prvky, které zajistí, že jsou definovány odpovídající zdroje se správnými schopnostmi a kompetencemi k jejich vykonávání. To platí pro konkrétní procesy řízení kybernetické infrastruktury jakou je návrh, plánování, nasazení, provoz, technická podpora a kontrola.

Zřejmě nejcitelnější pohromy (hrozby) pro kybernetické systémy představují škodlivý kód a hackerské a sociotechnické útoky. V zájmu minimalizace rizika spojeného s uvedenými pohromami je na místě implementace odpovídajících preventivních i reaktivních opatření. I přes technický charakter uvedených pohrom (hrozeb) se jako velmi vhodná ukazují být opatření založená na netechnických základech, konkrétně odpovídající výcvik a vzdělání zaměstnanců organizace.

Minimálně stejně důležitým prostředkem obrany před útoky realizovanými pomocí škodlivého kódu, jakým jsou technické prostředky, je také odpovídající vzdělání a výcvik všech pracovníků v dané organizaci. Důraz při výcviku by měl být kladen zejména na objasnění

principů uživatelem umožněné infekce systému (např. otevírání neprověřených příloh, či odkazů zaslaných z neznámých adres) a vhodnou reakci v případě, že infekce je v systému detekována. Mezi reaktivní opatření by mělo patřit primárně zamezení dalšího šíření škodlivého programu, a to odpojením infikovaného systému od sítě. Po něm by mělo následovat očištění systému pomocí speciálních opatření, případně obnovení systému z neinfikované zálohy. V případech, ve kterých je k dispozici dostatečně vyškolený personál, je v rámci reaktivních opatření vhodné provést také určení původního zdroje infekce a přijetí opatření zamezujících jeho využití jiným malware [147].

Vhodná preventivní opatření jsou v případě obou uvedených typů útoků převážně technické povahy, konkrétně se jedná o instalaci softwarových a hardwarových komponent pro detekci útoku (resp. skenování). Vhodným reaktivním opatřením pro případ detekce pokusu o průnik do sítě i pro detekci DoS útoku by mělo být informování odpovídajícího CERT/CSIRT týmu a zablokování IP adres, z nichž je útok či průnik veden. V případě trvajícího DoS útoku může být na místě též provedení změny IP adresy postiženého systému či jeho dočasné odpojení od internetu. Přestože výcvik personálu organizace nemůže popsaným typům útoku zabránit, může značným způsobem přispět k jejich odhalení a včasné reakci. Ani v rámci implementace opatření proti hrozbě hackerských útoků by tedy tento aspekt prevence neměl být zanedbáván [147].

Opatření proti kybernetickým útokům jsou také: umožnění přístupu k řídicím systémům pouze přes specifické přístupové body; zavedení bezpečnostního monitoringu provozu na vnitřní síti; a zajištění dostatečné úrovně znalostí informační bezpečnosti u zaměstnanců. Standard NIST SP 800-53 [149] obsahuje opatření, která mohla daným útokům zamezit (např. monitorování/omezení vzdáleného přístupu, management uživatelských účtů apod.).

Z pohledu poznatků o bezpečnosti složitých systémů v předchozích kapitolách, lze na základě výše uvedených poznatků o kybernetických sítích konstatovat, že kybernetické sítě, a tím i automatické řídicí systémy jsou velmi zranitelné tím, že zvažují pouze náhodné odchylky a nezvažují neurčitosti způsobené jak znalostními nejistotami, tak změnami skokem, které jsou vyvolané pohromami všeho druhu, a to nejen úmyslnými útoky.

Řídicí systémy ve světě používají často software SCADA (Supervisory Control And Data Acquisition). Předmětné systémy jsou používané k monitorování a kontrole podniku nebo zařízení v průmyslu – telekomunikace, vodní hospodářství (pitná i odpadní voda), energetika, plynárenství, vzduchotechnika a doprava [150]. Z důvodu jejich bezpečnosti dle [151] je nutné, aby měly specifický program pro kybernetické zabezpečení, program na hodnocení rizik a postupy pro jeho realizaci. Podle údajů v práci [151] je četnost útoků na systémy SCADA největší v energetickém sektoru, za ním následují průmyslové podniky, doprava a zdravotnictví. Z provozních důvodů řídicí systémy ovládané software SCADA nejsou uzavřené systémy, tj. jsou propojeny s okolím, což znamená, že v těchto místech jsou nejčastěji narušovány (připojení na internet nebo přes přenos dat veřejně dostupným prostředkem (radiový signál, rozhlas apod.).

Z výzkumu řídicího systému metra [152], který bude dále podrobněji popsán v odstavci věnovaném dopravě, je zřejmé, že z důvodu ochrany řídicích systémů musí být chráněna data pro rozhodování, což znamená:

- vstup do kybernetického prostoru musí být chráněn hesly s tím, že se věnuje péče délce hesla, komplexnosti hesla, způsobu používání hesla, pravidelným změnám hesla, indikaci uživatelů, sdílení účtů a speciálně logice řízení přístupu,
- přístup k informacím nesmí být neomezený, musí být sledován a dokumentován nezávisle na uživateli, musí být dozorován a posuzován,
- integrita kybernetického prostoru musí být kontinuálně monitorována a pravidelně prověřována,

- každé narušení kybernetického systému musí být vyšetřeno, musí být posouzena jeho závažnost a musí být přijata opatření, aby se snížily četnost i závažnost jeho opakování,
- důležitá data i způsoby zpracování dat musí být zálohované,
- skartovaná data musí být bezpečně likvidována.

5.5.4. Příklad řešených problémů informačního systému na řídicím systému metra

Na základě platných legislativních požadavků je metro vybudováno jako zabezpečený systém, který je bezpečný z pohledu integrální bezpečnosti jen při splnění jistých podmínek, tj. odolává dopadům pohrom všeho druhu, jejichž velikost je nižší než projektová [153].

Metro je řízeno polo automatizovaným systémem z dispečerského stanoviště, tj. některé operace jsou vykonávány manuálně a některé pomocí informačních technologií. Z pohledu bezpečnosti technického díla oba způsoby musí být kvalitně provázané [1]. Úkolem je zajistit celkovou bezpečnost (tj. požadovanou kvalitu provozu), která zahrnuje jak bezpečný provoz (tj. provozní bezpečnost zajišťující bezpečí metra), tak stanovené přepravní parametry po celou dobu životnosti. Proto v systému metra jsou řízené, řídicí i ochranné systémy.

Výpadek resp. porucha některého z důležitých nebo více méně důležitých prvků systému metra má vliv na jiné systémy, které fungují paralelně anebo jsou nadřazené předmětnému systému. Předmětnými paralelními či nadřazenými systémy jsou např. další technické systémy včetně povrchové dopravy, infrastruktury vodohospodářské či energetické apod., dále to jsou systémy ekonomické s návaznostmi na financování údržby a obnovy infrastruktury v metropoli, a v neposlední řadě pak systémy sociologické – včetně lidského systému zajišťujícího lidskou bezpečnost, tj. kvalitu života a bezpečí lidí.

Z důvodu zajištění bezpečnosti, a především spolehlivosti má systém metra záložní systémy, které jsou specificky propojené a vytváří ochranný systém metra, který zajišťuje provoz na určité úrovni po dostatečně dlouhou dobu tak, aby cestující byli bezpečně přepraveni na bezpečné místo [154].

Aby systém metra byl schopen vykonávat funkce dopravní a ochranné, tak musí být dle údajů v odstavci 3.6 vybaven informačním systémem s vysokou mírou informačního výkonu. Pro zajištění vzájemných vazeb a umožnění reakce na změny v návazných systémech se informační systémy jednotlivých oblastí řízení propojují kybernetickou (informační sítí). Propojení informačních systémů vytváří ještě komplexnější otevřený systém náchylný na přenos chybných informací a také na fyzikální vlivy okolí; příklad je uveden v práci [155].

Z uvedených důvodů se musí v praxi aplikovat postupy pro hodnocení výkonu informační infrastruktury tak, aby bylo možné nevyhovující parametry informací identifikovat, monitorovat, vyhodnocovat a navrhovat nápravná opatření.

Obecné požadavky na funkci systému řízení metra dle definovaných úrovní stupně automatizace jsou dané evropskými normami. Teorie informačních systémů a technologií poskytuje vědecký základ pro tvorbu efektivních systémů řízení s podporou informačních technologií tak, aby byly zajištěné jak požadované cíle, tak dostatečná bezpečnost, kterou poměřujeme integritou bezpečnosti. Skutečnou bezpečnost však zajišťuje výběr komponent, způsob jejich propojení, kvalita algoritmů pro jejich propojení a úroveň jejich reálného provedení.

5.5.5. Opatření pro zvýšení bezpečnosti kybernetických systémů

Na základě analýzy dostupných dat pomocí vyhledávače [156] v České republice je používána celá řada software pro podporu systematického řízení vnitropodnikových procesů a služeb. U všech je uvedeno, že slouží ke zvýšení efektivnosti, výkonnosti a k posuzování přidané hodnoty pro organizaci. Součástí zavedených systémů řízení je nastavení pravidel

umožňujících zajištění požadavků všech zainteresovaných stran (zákazník, dodavatel, zaměstnanec, atd.). Z dostupných informací vyplývá, že činnosti, které jsou provedeny předmětnými řídicími systémy v oblasti technické, vychází ze sledování a vyhodnocování provozní spolehlivosti. Tj. uvažují jen náhodné odchylky a nejsou orientované na celkovou bezpečnost předmětných technických děl, což nakonec potvrzuje i práce [157] popisující konstrukci průmyslových řídicích systémů. Z hlediska bezpečnosti to znamená, že je u nich třeba připravit další nástroje, které zajistí bezpečnost nejenom řídicích systémů samotných, ale hlavně příslušného technického díla při podmínkách kritických vyvolaných podmínkami neuvažovanými v návrhu technického díla (jde např. o vnější požár, výbuch, fyzické napadení či povodeň nebo vichřici).

5.6. Výsledky studia rizik elektroenergetického systému a návrh ochranných opatření

Energetický systém České republiky se skládá ze tří subsystémů, a to:

1. Systém zdrojů primární energie a její získávání (těžba paliv, získávání primární elektřiny a tepla).
2. Systém energetických transformací a logistiky (zušlechťování paliv, výroba elektřina a tepla, transformace elektřiny a tepla, dopravní, přenosové a distribuční systémy, zásobníky).
3. Systém konečné spotřeby (užití energie pro technologické procesy, doprava, vytápění, příprava teplé užitkové vody a další spotřebiče).

Struktura energetického systému je tvořena objekty a liniovými stavbami (sítěmi), ze kterých jsou složeny zásobovací řetězce. Z hlediska strukturování existujících problémů je vhodné oddělit uhelný průmysl, ropný průmysl, jaderný průmysl, plynárenství, elektroenergetiku a teplárenství.

V oblasti uhelného průmyslu jsou liniové stavby pasová doprava do elektráren, objekty a zařízení tvoří doly, těžní stroje a velkorypadla. Hlavní nebezpečné látky tvoří odpady.

V oblasti ropného průmyslu jsou liniové stavby ropovody a produktovody, objekty a zařízeními jsou těžební zařízení, rafinérie a chemické závody. Hlavní nebezpečné látky jsou ropné produkty a chemické látky, které se používají v technologii.

V oblasti jaderného průmyslu jsou liniové stavby doly a procesní linky na zpracování jaderných materiálů a pro nakládání s odpady, objekty a zařízeními jsou doly, těžební zařízení, sklady, úložiště a zpracovatelské závody. Hlavní nebezpečné látky jsou jaderné odpady a zvýšená radioaktivita.

V oblasti plynárenství jsou liniové stavby plynovody, objekty a zařízeními jsou těžební zařízení, plynárny, zásobníky, kompresorové stanice a redukční stanice.

V oblasti elektroenergetiky liniové stavby tvoří přenosová a distribuční venkovní a kabelová vedení. Objekty a zařízeními jsou elektrárny, rozvodné stanice, transformátory, sklady vyhořelého paliva a vodní akumulační nádrže. Hlavní nebezpečné látky jsou vyhořelé palivo, radioaktivní a jiné nebezpečné odpady.

V oblasti teplárenství jsou liniové stavby tepelné sítě, a to parní a horkovodní, objekty jsou teplárny a výměníkové stanice atd.

V odstavci se dále soustředíme jen na elektroenergetickou soustavu, která je páteřní infrastrukturou, která zajišťuje kvalitu života lidí, při kritických podmínkách pak ochranu obyvatelstva a přežití lidí. Skutečná nebezpečí spojená s jejím selháním, která vyvolávají ztráty, škody a újmy na chráněných aktivech naznačily některé jevy (blackouts) spojené s rozsáhlými výpadky dodávek elektrické energie v posledním desetiletí na severoamerickém kontinentu a v Evropě.

5.6.1. Rozvod elektrické energie

Energetická soustava je soubor výroben energie (elektrické, tepelné, vodní, větrné, solární) se zařízením pro rozvod a spotřebu, kde jde o přenos elektrické energie od výrobců k dodavatelům. Vyrobená elektrická energie jde do rozvoden, ze kterých je pomocí distribuční soustavy rozváděna dále. Aby ztráty energie (ztráty výkonu jsou úměrné druhé mocnině proudu) byly přijatelné, tak celá síť má odlišné větve a při přenosech na velké vzdálenosti se používá vysoké napětí [158].

Přenosovou soustavu tvoří především soustava dlouhých nadzemních vedení velmi vysokého napětí. Dále pak kabely, transformátory, odpojovače, vypínače, bleskojistky, kompenzační prvky a systémy řízení a regulace sítě. Cílem řízení sítě je udržení konstantních standardních parametrů dodávané energie (především dodržení jmenovité frekvence, což je v Evropě 50 Hz, a jmenovitého napětí) a samozřejmě nepřerušená dodávka energie ke spotřebiteli.

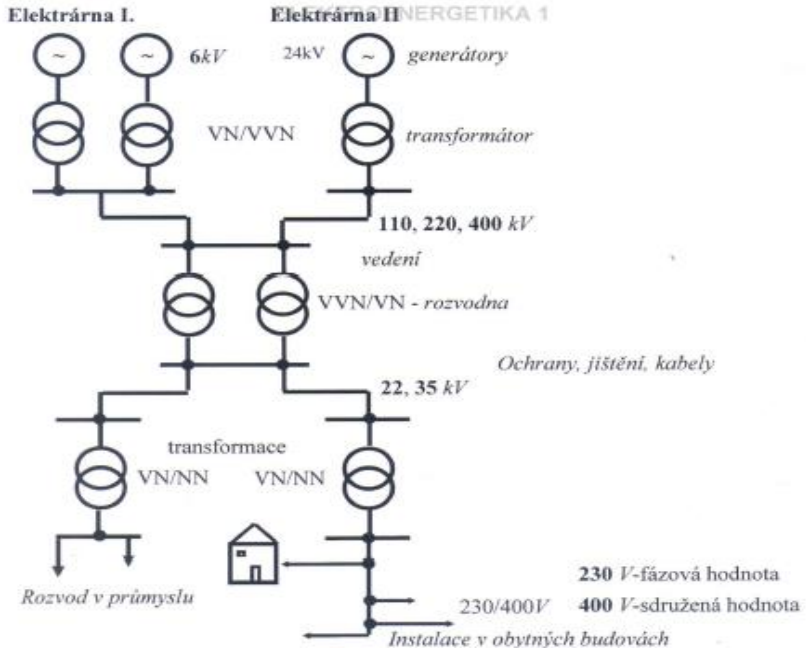
Elektrická energie je výjimečná tím, že v celé síti je nutné zajistit rovnováhu mezi její okamžitou výrobou a spotřebou. Elektrickou energii totiž nelze nijak skladovat (náhradou skladů jsou záložní elektrárny nebo režimová opatření využívající tzv. přečerpávací elektrárny jako jsou Dlouhé stráně). Kvůli energetické efektivitě soustavy je navíc potřebné udržet nízký fázový posuv mezi napětím a proudem, což vyžaduje zařazení zvláštních kompenzačních prvků dodávajících tzv. kompenzační výkon.

Potíže v přenosové soustavě bývají jednou z příčin rozsáhlých výpadků dodávky elektrické energie. Důvodem jsou jak poškození důležitých venkovních vedení působením nepříznivých přírodních podmínek (námraza, silný vítr, prudká letní bouře apod.), tak celkové přetížení soustavy. Zařízení přenosové soustavy jsou proto vybavena pojistnými prvky, které zajistí odpojení vybraných odběratelů v případě, že by hrozilo zničení nebo rozpad sítě vlivem jejího přetížení. Pokud by se tak nestalo, je zde reálná možnost tzv. kaskádového šíření poruchy, což znamená, že po selhání přetíženého vedení vzroste přetížení zbytku sítě, a to způsobí, že jsou postupně odpojeny další a další prvky sítě, případně až po zcela nežádoucí kompletní rozpad celé přenosové soustavy. Z ekonomických důvodů je vhodné, pokud to je možné v řídícím centru, odpojovat nejprve ty odběratele, kterým výpadek napájení způsobí nejmenší hospodářské škody.

Na správné funkci přenosové soustavy závisí i značná část primární výroby elektrické energie, většina elektráren potřebuje ke svému spuštění elektrickou energii dodávanou z elektrorozvodné sítě nebo elektřinu, kterou si elektrárna sama přímo vyrábí (tzv. energie vlastní spotřeby).

Přenosovou soustavu v České republice provozuje státní společnost ČEPS, a. s. Síť tvoří vedení vvn 400 kV, 220 kV, vybraná vedení 110 kV a třicet transformačních stanic. Mezinárodně je síť šestnácti vedeními propojena se sítěmi dalších členů ENTSO-E (Evropská síť provozovatelů přenosových soustav elektřiny). V roce 2006 se přenášený výkon pohyboval od 4.9 GW do 11.4 GW (rekordní hodnota v zimní špičce) [158].

Energetickou soustavu je možno členit na elektrizační soustavu a teplofikační soustavu [159]. Elektrizační soustava (ES) je soubor zařízení pro výrobu, přenos, transformaci a distribuci elektrické energie včetně elektrických přípojek a přímých vedení a systémů měřicí, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky. Přehledové schéma elektrizační soustavy je na obrázku 19, převzatém z dokumentu [159].



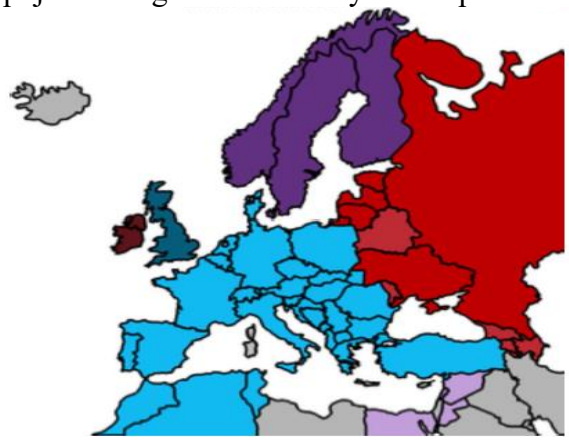
Obr. 19. Schéma elektrizační soustavy [159].

Přenosová soustava (PS) je část elektrizační soustavy, která tvoří přenosovou cestu pro napájení velkých stanic nebo uzlů, zpravidla vyššího napětí (zvn, vvn - 400, 220, část 110 kV). Představuje páteřní rozvedení výkonu z velkých elektráren po celém území ČR. Schéma přenosové soustavy zobrazuje obrázek 20, převzatém ze [159].

Obr. 20. Schéma rozvodné sítě v ČR [159].

Distribuční soustava (DS) je část elektrizační soustavy, která slouží pro dodávku elektrické energie odběratelům. Patří sem okružní a paprsková síť vvn, vn, nn (110; 35; 22; 0,4 kV), tedy

regionální a lokální distribuční soustavy pro rozvod a užití elektrické energie. Propojená elektrizační soustava je soustava, která vznikla propojením elektrizačních soustav několika zemí se společným operativním řízením. V současné době funguje v Evropě systém UCTE (Union for the Co-ordination of Transmission of Electricity), který představuje sdružení provozovatelů přenosových soustav v kontinentální Evropě. Na obrázku 21 jsou znázorněny propojené energetické soustavy v Evropě.



Obr. 21. Propojené energetické soustavy v Evropě [159].

Elektroenergetickou soustavu si lze představit jednak jako soubor fyzických prvků, které jsou propojené fyzickými a kybernetickými infrastrukturami a jednak jako hierarchický logický celek, který má inherentně vloženou jistou logiku, která je podstatná pro jeho bezpečnost, tj. i funkčnost a spolehlivost. Je zřejmé, že pojmový aparát obou uvedených pohledů nemůže být stejný a že druhý pohled vyžaduje daleko vyšší znalostní úroveň než pohled první. Na první úrovni lze řešit jen některé technické a operativní problémy spojené s dlouhodobým výpadkem elektroenergetické soustavy.

Chceme-li řešit úkoly na taktické a strategické úrovni řízení, musíme použít logický model. V praxi jsou ve vyspělých zemích používané dva logické modely, jeden (užší) používají provozovatelé elektroenergetické soustavy a druhý veřejná správa, která má za cíl zajistit bezpečnou komunitu a bezpečné území [160].

5.6.2. Selhání dodávek elektřiny

Elektroenergetický systém je ohrožen pohromami [12,161], do kterých patří:

1. Technologické havárie (tzv. vnitřní) kritických prvků, vazeb a toků v systému. Je nutno zvážit vady materiálu, stárnutí, nedostatečnou údržbu apod.
2. Chyby nebo selhání řídicího systému.
3. Lidské chyby.
4. Živelní pohromy nebo technologické havárie (tzv. vnější) jiného systému.
5. Teroristický útok, kriminální čin nebo válka.

Je skutečností, že infrastruktura dodávek elektrického proudu má největší provázanost s ostatními infrastrukturami, technologiemi a lidskou činností. Nejrůznější analýzy dopadů výpadku elektrické sítě se z reálných událostí opírají především o blackout, ke kterému došlo na územích USA a Kanady ve dne 14. 08. 2003 a který přetrval až do dne 22. 08. 2003, kdy byla úspěšně zahájena obnova normálního fungování společnosti a všeho podnikání. Z jeho analýzy [162] plyne, že výpadek elektrického proudu postihl oblast obývanou zhruba padesáti milióny lidí ve východní části USA a Kanady. V USA to byly státy Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut a New Jersey a v Kanadě provincie Ontario. Běžná spotřeba elektrické energie dané oblasti je 61 800 MW. Výpadek začal několik minut po 16 hodině místního času a dodávky nebyly obnoveny ani po 4 dnech

v některých částech USA a v některých částech Ontaria ani po více než týdnu. Událost vedla k řadě testů elektrických infrastruktur po celém světě. V USA a Kanadě proběhlo rozsáhlé společné šetření na základě rozhodnutí čelních představitelů obou zemí. Vznikla komise expertů, která zpracovala zprávu pro obě vlády. Náklady na obnovu byly v USA mezi 4 – 10 miliardami USD; 2.3 miliard CAD v Kanadě.

Expertní komise sestavená na úrovni vlád USA a Kanady identifikovala čtyři hlavní příčiny: neadekvátní chápání systému elektrické sítě; neadekvátní situační povědomí (nerozpoznání vážnosti situace při výpadku proudu); neadekvátní úprava stromu přenosových linií; a neadekvátní diagnostická podpora z řídícího centra. Přetížení sítě pak bylo vyvoláno menší ztrátou výkonu jaderné elektrárny Perry (1 852 MW) v době zvýšených nároků na dodávku elektrického proudu vlivem připojení velkého množství klimatizací při vysokých teplotách v území. Ztráta výkonu jaderné elektrárny mohla být řešena naběhnutím rychlých zdrojů elektrického proudu, nebo odpojením části spotřebičů. Šetření však zjistilo, že pro dané území nebyly vypracovány postupy a plány, které by pomohly danou událost řešit.

Na konci šetření předmětná expertní komise předložila v rámci závěrečné zprávy [162] celkem 49 doporučení na zlepšení situace. Doporučení lze shrnout do čtyř bodů:

1. Organizační zajištění spolehlivosti.
2. Podporu a posílení činností národní energetické sítě.
3. Zajištění bezpečnosti fyzických a kybernetických systémů tvořících energetický systém.
4. Zodolnění sektoru jaderných elektráren.

Přehled velkých blackoutů uvádí práce [163], obrázek 22; tabulka 7 uvádí počet postižených lidí u největších blackoutů na základě údajů v pracích [163-165].

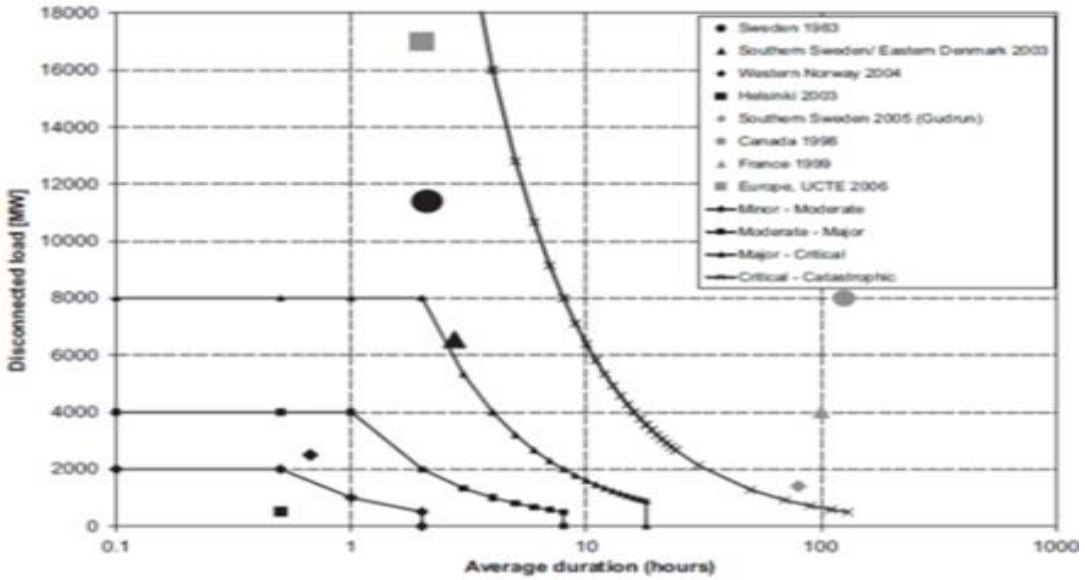
Obr. 22. Velké blackouty ve světě [163].

Tabulka 7. Počet postižených lidí u největších blackoutů ve světě [163-165].

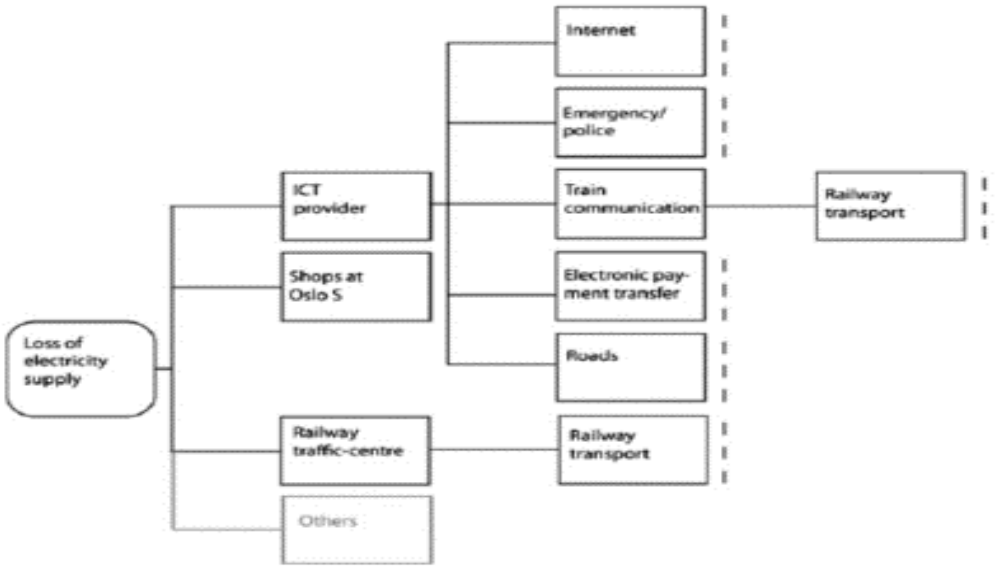
Datum	**Místo**	**Počet postižených lidí**
24. 9. 2014	Kazachstán – Alma Ata	1 milión
9. 9. 2012	Kuba	11 miliónů
30 - 31. 7. 2012	Indie	670 miliónů
20. 8. 2010	Rusko – Petrohrad	2.5 miliónů
10. 11. 2009	Brazílie	50 miliónů
9. 11. 2009	Tádžikistán	9 miliónů
5. 11. 2006	Západní Evropa	10 miliónů
4. 11. 2006	Německo, Benelux, Francie, Španělsko, Itálie	8 miliónů
14. 8. 2006	Japonsko – Tokio	14 miliónů
18. 8. 2005	Java – Bali	100 miliónů
11. 3. 1999	Brazílie	97 miliónů
10 – 11. 5.2009	Brazílie – Paraguayi	87 miliónů
14 – 15. 8. 2003	USA a Kanada	55 miliónů
28. 9. 2003	Itálie	55 miliónů
9. 11. 1965	Severovýchod USA a Kanada	30 miliónů
31. 3. 2015	Turecko	76 miliónů
27. 3. 2015	Holandsko	3 milióny

Z obrázku 22 i z tabulky 7 vyplývá, že blackout může nastat v každém státě. Z tabulky 7 je dále vidět, že nejvíce lidí bývá postiženo, když blackout nastane v rozvojové zemi. Je to způsobeno tím, že v rozvinutých zemích mají již postupy na rychlé zvládnutí rozpadu sítě, tj. k zastavení kaskádovitého šíření a mají náhradní opatření pro snížení kritičnosti dopadů.

V pracích [166-168] byla na základě údajů z různých blackoutů odvozena závislost mezi ztrátou výkonu a dobou trvání blackoutu; obrázek 23. Obrázek ukazuje, že čím větší výkon je postižen výpadkem, tím déle trvá rozpad sítě. Zjednodušená představa blackoutu z práce [166] je uvedena na obrázku 24; kaskádovitý výpadek dodávek elektřiny byl zpracován dle empirických dat sebraných po blackoutu v Oslu dne 13. 3. 2013.



Obr. 23. Závislost ukazující závislost ztráty výkonu na době trvání (v hodinách [166].



Obr. 24. Zjednodušený kaskádovitý výpadek dodávek elektřiny v Oslu dne 13. 3. 2013; čárkované čáry ukazují přerušené služby [166].

V České republice jsme v r. 2004 provedli expertní vyhodnocení dopadů blackoutu v Jihočeském kraji, který by trval 14 dní [11]. Nebyly zvažovány ztráty na lidských životech. Ostatní ztráty jsou uvedené v tabulce 8. Z tabulky vyplývá, že předmětný kraj vzhledem ke svému rozpočtu 12 061 000 tisíc Kč a k ekonomickým pravidlům OSN [5] nemá schopnost předmětné ztráty pokrýt.

Tabulka 8. Vyčíslení ztrát způsobených přerušením dodávek elektřiny na 14 dní [11].

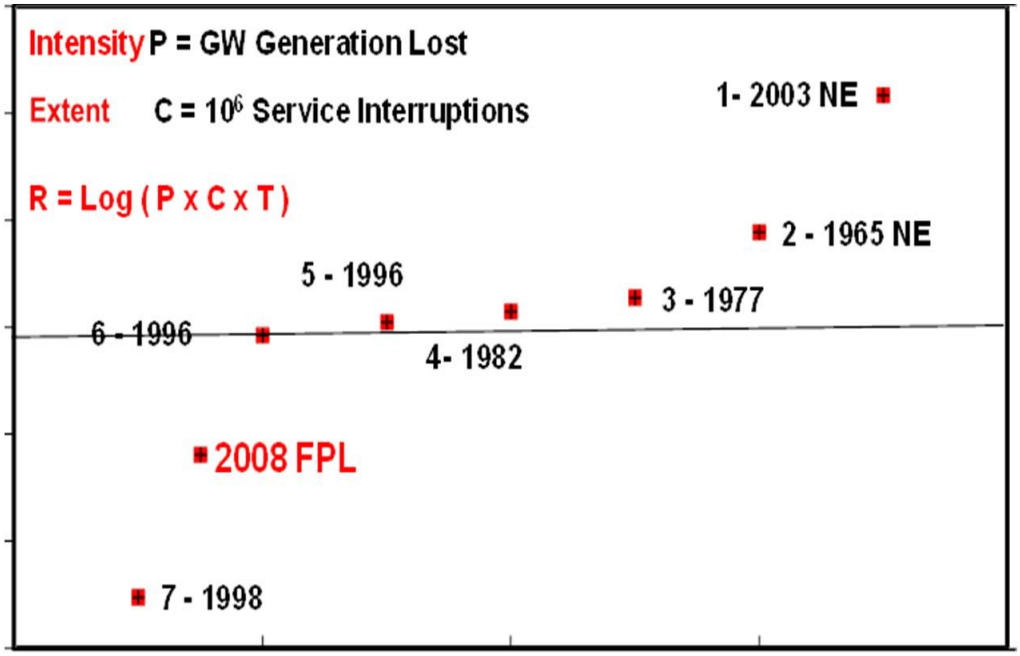
Ztráty	**tisíc Kč**
Na zdraví a životech	7 793 126
z toho: - na životech	49 914
- na zdraví	7 743 212
Na majetku a nákladech na obnovu	5 544 707
z toho: - na živočišné výrobě	3 476 912
- v průmyslu	1 815 892
- u obyvatelstva	251 903
Ztráty celkem	13 337 833

V práci [164] je provedeno hodnocení sedmi velkých blackoutů v USA; největší byl 14. 8. 2003, který byl zmíněn výše. Je sledována závislost mezi ekonomickými ztrátami a velikostí blackoutu měřenou specifickou veličinou R. Výsledek je na obrázku 25. Zváženy byly přímé i nepřímé ekonomické ztráty. Mezi přímé dopady jsou započítávány: zkažení potravin; odstavení výrobních závodů; poškození elektronických dat a ztráta služeb IT; ztráta životy podporujících systémů v nemocnicích, jeslích a domácnostech; přerušení elektrifikované dopravy; dopravní zácpy kvůli selhání prostředků pro řízení dopravy; a navýšení mezd pro pracovníky odezvy a obnovy. Nepřímé náklady byly rozděleny:

- krátkodobé: ztráty na majetku způsobené rabováním a žhářstvím; vypovězení sociálních podpor,
- střednědobé: náklady na obnovu po rabování; ztráty na daních z tržby během doby obnovy; související růst pojištění; a náklady na vězení rabovačů,

- dlouhodobé: náklady na soudní spory; kontaminace způsobená kanalizací a skládkami; následný výskyt epidemií.

Z obrázku 25 vyplývá, že blackout, který v r. 2003 postihl USA a Kanadu způsobil zatím největší ztráty.



Obr. 25. Závislost škod způsobených blackoutem R na velikosti blackoutů měřenou součinem P x C x T; T – doba trvání, C – rozsah (počet postižených osob x 10^6), P – intenzita (ztráta generovaného výkonu v GW), v USA [164]. Vodorovná osa (velikost blackoutu) – rozsah 0 - 8; svislá osa (ekonomické ztráty) – rozsah 0 – 6.

5.6.3. Příčiny selhání dodávek elektřiny

Analýza a vyhodnocení poznatků z odborné konference ESREL [160], z další odborné literatury, např. [169-175], empirických dat popisujících jednotlivá selhání [173,174] a výsledky analýz metody What, If aplikovaných na několik typových území [176] ukazují, že pro poznání výpadků elektroenergetické soustavy, pochopení procesů působení výpadků na chráněná aktiva a pro nalezení vhodných činností a opatření pro řízení bezpečnosti dodávek elektrické energie, které zajistí bezpečné dodávky dlouhodobě v určité kvalitě, je nutné modelovat nejen procesy v samotných elektrických sítích, ale i procesy, které jsou odezvou na dynamické chování okolí elektrických sítí, tj. v území. Je třeba vzít v úvahu pohromy různého druhu, protože konkrétní dopady závisí na naturelu pohrom, který koinciduje se zranitelnostmi soustavy, okolního území a způsobu místního ovládání soustavy [161]. Z dostupných dat vyplývá, že některá propojení v elektroenergetické soustavě jsou kompatibilní jen za určitých podmínek a že jednotlivé části soustavy spolupracují (tj. jsou interoperabilní) také jen za určitých podmínek, což znamená, že bezpečný provoz má zcela určité limity hodně dané místními podmínkami. Ve smyslu integrální bezpečnosti [1] je třeba mít připraveny postupy pro zvládnutí kritických podmínek, způsobených blackoutem; tj. když už k němu dojde, tak je ho třeba, co nejrychleji zastavit.

Srovnání dat o výpadcích dodávek elektrické energie ukazuje, že závažné výpadky elektrického proudu jsou velmi různorodé, téměř žádné dva nejsou stejné. Jejich iniciační události jsou rozmanité, včetně lidských činností nebo nečinností, topologie systému a rovnováhy zatížení sítě / generace proudu. Dalšími faktory jsou: vzdálenost mezi zdroji a

závažnými spotřebiteli, napěťový profil v síti a typy a polohy použitých ochranných relé [170]. Důležité poznání je to, že výpadek elektrické sítě má kaskádovitý tvar a že se jedná o dynamický jev, který zatím se nesnadno zastavuje lidským zásahem, když se vyskytne. To opět znamená, že pro přežití lidí při dlouhodobém výpadku musí být připravena realistická opatření, aby přežili.

5.6.4. Zranitelnost technických prvků elektroenergetické soustavy

Z obecné analýzy zranitelnosti elektroenergetického systému [176] vyplývá, že:

- nejvíce zranitelné jsou pozemní a nadzemní objekty, a to především liniové stavby jako venkovní elektrická vedení, nad zemí umístěné části a armatury plynovodů a produktovodů a bezobslužné objekty, kterými jsou malé transformátory, spínací stanice, redukční stanice a výměníkové stanice,
- existující energetické, chemické i jaderné technologie a provozy jsou projektovány na zvládnutí chyby obsluhy a na zvládnutí selhání zařízení. Pouze jaderné elektrárny mají ještě nadstandardní bezpečnostní zařízení. Téměř nechráněné jsou dlouhé liniové stavby (přenosová vedení, tranzitní a vysokotlaké plynovody, ropovody a produktovody) vedoucí územím, které není nijak chráněno a je veřejně přístupné. Jsou jen dálkově monitorovaná a řízena prostřednictvím řídících a dispečerských systémů. Největší problémy jsou u elektřiny, protože tu nelze skladovat.

Výše uvedené skutečnosti ukazují, že důvodů selhání je mnoho, a proto s nimi musíme počítat a z hlediska ochrany obyvatelstva mít připravena opatření, která provedeme v případě dlouhodobých výpadků elektroenergetického systému.

5.6.5. Dopady selhání dodávek elektřiny

Celkový přehled možných dopadů dlouhodobého selhání dodávek elektřiny na veřejná aktiva odvozený metodou What, If pomocí dat od 115 respondentů z veřejné správy, kteří řeší v EU bezpečnostní otázky získané v rámci šetření prováděných během projektu FOCUS [12,19,176]:

1. Možné dopady na životy a zdraví lidí: ztráta osvětlení, vytápění a klimatizace, možnosti přípravy jídla, přístupu k pitné vodě, spojení a zdrojů informací, přístupu k peněžním prostředkům (bankomaty) a tím i k nákupu potravin apod.; ztráta dopravního spojení založeného na elektrické energii (i čerpání benzínu a nafty je závislé na elektřině) apod.
2. Možné dopady na bezpečí lidí: ztráta naplňování základních lidských potřeb (jídlo, hygiena, teplo, spojení s lidmi, isolace, nedostatek informací apod.); ztráta lékařské péče založené na dodávkách elektrické energie (provoz moderních vyšetřovacích přístrojů a aparatur); ztráta sociální péče o děti, staré, nemocné a handicapované lidi; psychická újma při uvíznutí v uzavřeném prostoru (výtah, tubus metra aj.); vznik paniky a chaosu; zvýšení četnosti výskytu kriminálních činů a útoků apod.
3. Možné dopady na majetek: znehodnocení jídla ve skladech potravin a v lednicích; škody způsobené požáry, které jsou vyvolány ztrátou funkčnosti regulačních mechanismů na zařízeních s otevřeným ohněm nebo zařízeních, kde může dojít k požáru z jiného důvodu při selhání regulace; škody vyvolané dopravními a technologickými haváriemi; škody na technologiích a jiném majetku vyvolané náhlou ztrátou energie doprovázené únikem nebezpečných tekutin a plynů; škody na domácích zvířatech způsobené selháním obslužných procesů založených na elektrické energii; ztráty v důsledku výpadků výroby apod.
4. Možné dopady na veřejné blaho: zastavení obchodování a služeb občanům; zastavení společenských a kulturních akcí; zastavení rehabilitačních a pečovatelských služeb; snížení

úrovně zdravotnické péče; znehodnocení léků a materiálů nutných pro operace; znehodnocení potravin a poživatin; snížení úrovně hygieny apod.

5. Možné dopady na životní prostředí: zvýšení plynných, kapalných a tepelných emisí do životního prostředí v důsledku ztráty funkčnosti odlučovačů, separátorů odpadů, čističek, chladících zařízení apod.; dopady technologických havárií, které vzniknou v důsledku ztráty elektrického napájení apod.
6. Možné dopady na infrastruktury a technologie, které se dále člení:
   - možné dopady na dodávky energií (elektřina, teplo, plyn): selhání dodávek tepla z centrálních zdrojů (čerpadla a ovládací mechanismy); selhání centrálních dodávek plynu v důsledku nefunkčnosti čerpadel a ovládacích mechanismů založených na elektrické energii; selhání činnosti skladů (lednice, klimatizace, aj.); výpadek výroby, skladů, sítí fyzických i kybernetických a různých služeb podmíněných dodávkou elektrické energie apod.
   - možné dopady na systém dodávky vody: selhání dodávek vody do domácností, veřejných zařízení i provozů (čerpadla, regulační mechanismy, řídicí systémy) a tím nastartování některých havarijních stavů; problémy s regulací a údržbou pitné a užitkové vody v nádržích apod.
   - možné dopady na kanalizační systém: ztráta řízení kanalizačního systému; odstavení čističek odpadních vod, tj. selhání čistění odpadních vod; poškození potrubí v důsledku přeplnění odpadními vodami a následné znečištění životního prostředí, ztekucení podloží apod.
   - možné dopady na přepravní síť: selhání dopravní obslužnosti založené na elektrické energii (metro, vlaky, tramvaje aj.); výpadek čerpacích stanic pohonných hmot a velkoskladů pohonných hmot; dopravní zácpy, dopravní havárie a postupem času nedostatek potravin v důsledku uvíznutí přepravních prostředků ve frontách aj.; selhání regulačních mechanismů (světla na křižovatkách, tunelech aj.); nedostatek přepravních prostředků, které nejsou založené na elektrické energii (např. autobusů nahrazujících metro) apod.
   - možné dopady kybernetickou infrastrukturu (komunikační a informační sítě): ztráta řízení sítí v čase (po vybití záloh tvořených bateriemi); ztráta vzájemného spojení (po vybití záloh tvořených bateriemi); selhání bezpečnostní ochrany bankomatů; selhání provozů řízených kybernetickými řídicími systémy; ztráta dat uložených v informačních systémech a databázích; ztráta přístupu k informacím uloženým na médiích podmíněných provozem zařízení napájených elektrickou energií (po vybití záloh tvořených bateriemi) apod.
   - možné dopady na bankovní a finanční sektor: ztráta provozu sektoru (banky, bankomaty, pojišťovny aj.) v důsledku ztráty přístupu k datům v informačních systémech a v síti a ztráta funkčnosti ovládacích mechanismů; ztráty na finančním trhu v důsledku sankcí za neprovedené transakce a za promarněné příležitosti; selhání bankomatů a e-bank; selhání obslužnosti klientů; ztráta přehledu o situaci na finančním trhu v důsledku nefunkčnosti informačních prostředků apod.
   - možné dopady na nouzové služby (policie, hasiči, zdravotníci): ztráta informovanosti pocházející z informačních zdrojů závislých na provozu zařízení napájených elektrickým proudem z centrálních zdrojů; ztráta spojení založeného na systémech závislých na provozu zařízení napájených elektrickým proudem z centrálních zdrojů, tj. problémy s varováním obyvatelstva; ve zdravotnictví ztráta schopnosti provádět operace a poskytovat péči založenou na provozech přístrojů napájených elektrickým proudem z centrálních zdrojů; zastavení údržbářských a opravárenských prací závislých na provozu zařízení napájených elektrickým proudem z centrálních zdrojů apod.

- možné dopady na základní služby v území (zásobování potravinami, likvidace odpadů, sociální služby, pohřební služby), průmysl a zemědělství: zastavení výroby a prodeje potravin (mlékárny, pekárny, zpracování masa, restaurace a přípravny jídla); zastavení provozů na zpracování a likvidaci odpadů; v sociální péči ztráta schopnosti poskytovat péči založenou na provozuschopnosti zařízení závislých na dodávce síťové elektřiny; zastavení provozů skladů a v nich uskladněných potravin; zastavení provozu škol, školek a dalších sociálních zařízení; zastavení výroby průmyslových podniků; zastavení zemědělských provozů závislých na provozu zařízení napájených elektrickým proudem z centrálních zdrojů, tj. např. provozů na výrobu krmiv apod.
- možné dopady na státní správu a samosprávu: ztráta informovanosti pocházející z informačních zdrojů závislých na provozu zařízení napájených elektrickým proudem z centrálních zdrojů; ztráta řízení věcí veřejných; přerušení spojení a ztráta vzájemné komunikace a komunikace s občany; snížení schopnosti řídit odezvu na situaci a udržet situaci v území pod kontrolou; nemožnost dostát všem úkolům vyplývajícím z odpovědností stanovených zákony o státní správě i samosprávě, a to i zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) apod.

Celkově: ztráta funkčnosti dodávek, provozů a služeb, které jsou závislé na elektrické energii, a tím značné omezení schopnosti zvládnout situaci a zajistit návrat do stabilního stavu a obnovu; kaskádové efekty a dominové dopady v systémech a sítích; vznik neočekávaných velice nepříznivých situací jako důsledek kombinace nepředvídaných jevů apod.

Na základě poznatků uvedených v [1] i výše při selhání technologických systémů obvykle dochází ke sledu více dopadů externího i interního charakteru, primárních i sekundárních, které lze jen málo ovlivnit. Tyto dopady pak působí v různé intenzitě a v různém časovém období. Proto v přípravné fázi podkladů pro řízení bezpečnosti technologických celků (zvláště těch, jejichž modelem je systém systémů) je zapotřebí identifikovat spektrum těchto dopadů (tj. zdroje rizik) a určit, v jakých souvislostech působí, zda jsou orientované na politické, ekonomické, technické, personální a jiné prostředí a jaká vhodná opatření lze použít k jejich odstranění, případně ke zmírnění. Hodnocení a řízení možných ohrožení a z nich plynoucích rizik patří k náročným a klíčovým procesům řízení bezpečnosti. Zaváhání a odkládání řešení má velmi nepříznivý dopad na celé řízení věcí veřejných, a tím i na rozvoj lidské společnosti.

Analýza výsledků simulací blackoutu v ČR [11,176] umožnila určit kategorie nouzových situací způsobených výpadkem elektrické energie, tabulka 9.

Tabulka 9. Kategorie nouzových situací pro výpadek elektrické energie [11,176].

Kategorie	**Doba trvání výpadku elektrické energie v místě**
0	Doba trvání (0, půl hodiny)
1	Doba trvání (0.5 hodiny, 6 hodin)
2	Doba trvání (6 hodin, 1 den)
3	Doba trvání (1 den, 3 dny)
4	Doba trvání (3 dny, 10 dní)
5	Doba trvání větší než 10 dní

V prosinci 2011 a v únoru 2012, kdy nadměrné přetoky energie z vysoké výroby elektrické energie „německých větrníků“ ohrožovaly naši soustavu 14 dní a týden [177]. Podle údajů v předmětném zdroji by po odstranění příčiny výpadku dodávek trvalo nejméně 26 hodin, než se dodávky plně obnoví. To však neznamená, že se situace navrátí do původního stavu. Obnovit plné dodávky nezávadné pitné vody by trvalo i týden, ani obnova tepla by nebyla zcela automatická [177].

Nouzové zásobování obyvatel pitnou a užitkovou vodou představuje největší problém, který je nutné řešit. Proto se uskutečnilo cvičení Blackout 2014 dne 26. února 2014 v Praze (mělo řešit dlouhodobé plošné přerušení dodávek elektrické energie, ke kterému došlo na území hlavního města Prahy a částečně i Středočeského kraje). V důsledku přerušení dodávek elektrické energie by nastal stav nouze v elektrizační soustavě a teplárenství (zákon č. 458/2000 Sb.). Simulace se zaměřila na potřeby obyvatel Prahy a odhalila největší škody v dodávkách pitné vody (po 3 hodinách trvání celoplošného blackoutu by bez přístupu k pitné vodě bylo 600 tisíc Pražanů a situace by se dále zhoršovala). Situaci by nešlo řešit jinak než vyhlášením krizového stavu (zákon č. 240/2000 Sb.). Proto v závěrech cvičení Blackout bylo navrženo 32 doporučení ke zlepšení současného stavu [177]. Ukázalo se opět, že hlavní problém Prahy je v tom, že nemá náhradní zdroj energie.

5.6.6. Procesní model pro řízení bezpečnosti elektroenergetické soustavy zpracovaný podle principů inženýrství rizika

Procesní model pro řízení bezpečnosti elektroenergetické soustavy je založen na principech, metodách a postupech rizikového inženýrství uvedených výše, tj. je následující:

1. Elektroenergetickou soustavu zvažovat jako otevřený systém systémů, který je ohrožen vnějšími i vnitřními pohromami, včetně lidského faktoru.
2. Vyhodnotit zranitelnosti elektroenergetické infrastruktury při možných pohromách všeho druhu (viz dnes již všeobecně přijímaný princip „All Hazard Approach“ [8]), kterou je ztráta funkčnosti elektroenergetické infrastruktury.
3. Pro každou primární pohromu (zdroj rizika) vyhodnotit velikost ohrožení a četnost jeho výskytu.
4. Pro každou primární pohromu (zdroj rizika) stanovit zranitelnosti jednotlivých kritických částí systému. Klasifikaci zranitelnosti provést pomocí multikriteriálního hodnocení, které dovoluje zvážit vliv nesouměřitelných a nekvantifikovatelných kritérií. Doporučuje se použít více expertů a souboru otázek, které byly zpracovány pro zajištění bezpečnosti technologických celků.
5. Pro každou primární pohromu stanovit celkovou zranitelnost systému jako součet zranitelností jednotlivých kritických částí systému.
6. Pro každou primární pohromu stanovit závislost mezi celkovou zranitelností systémů a zranitelnostmi dílčích částí.
7. Pro každou primární pohromu určit kritické části, které přispívají nejvíce ke zranitelnosti systému.
8. Pro každou primární pohromu na základě dat ze speciálních zkušenostních databází určit pravděpodobnosti výskytu ztráty funkčnosti systému na základě příspěvků jednotlivých kritických částí systému.
9. Pro každou primární pohromu vytipovat preventivní opatření na snížení zranitelností.
10. Pro všechna uvažovaná rizika stanovit soubor preventivních opatření na snížení zranitelnosti systému a zajistit připravenost na zvládnutí pohrom, které vzniknou v důsledku zranitelností, které nebylo možno snížit.
11. Instalovat monitoring pro sledování kritických částí systému. Stanovit scénáře primárních pohrom. Stanovit scénáře odezvy pro očekávané scénáře primárních pohrom a postupy odezvy pro případ výskytu extrémních primárních pohrom.
12. Stanovit opatření pro projektování, výstavbu, provoz a vyřazení z provozu kritických částí systému infrastruktury a technologií.
13. Vytipovaná opatření promítnout do právních předpisů.
14. Provést odhad nároků opatření v oblastech finanční, technické, lidských zdrojů a organizační.

15. Vyhodnotit realizovatelnost opatření v závislosti na možnostech státu a na mezinárodních podmínkách.
16. Stanovit harmonogram aplikace opatření ve variantním provedení (varianty závisí na vnitřních i vnějších podmínkách).
17. Stanovit systém QA pro realizaci harmonogramu.
18. Stanovit harmonogram kontrol, jejichž cílem bude dosáhnout žádoucích cílů a v případě, že projektová opatření nebudou mít projektované výsledky, zajistit nápravná opatření, aby cíl nebyl ohrožen.
19. Zahájit a provést realizaci.

5.6.7. Nedostatky současného řízení bezpečnosti elektroenergetických soustav získané srovnáním s modelem řízení bezpečnosti zpracovaného podle poznatků rizikového inženýrství a návrh opatření k zodolnění

Je skutečností, že elektroenergetici vidí při řízení elektrické infrastruktury jen technické problémy a ne dopady na lidi a lidskou společnost, což nakonec potvrzuje platná legislativa pro elektroenergetiku (zákon č. 458/2000 Sb. - energetický zákon), která nevyžaduje zvažovat dopady výpadku elektroenergetické soustavy na lidi a dělat opatření pro přežití lidí v postiženém území. Jelikož nic není absolutně bezpečné, je třeba počítat i s dlouhodobým výpadkem elektroenergetické soustavy a k tomu je nutné minimálně vědět, co udělat, aby v takovém případě přežili lidé v postiženém území.

Pro zajištění bezpečnosti technologických celků se je třeba především soustředit na závažná rizika, tj. z možných zdrojů rizik vybrat ty zdroje rizik, které způsobí závažné dopady na chráněných zájmech a proti nim zaměřit preventivní a zmírňující opatření. Cíle hodnocení rizika u velkých technologických celků jsou následující:

1. Identifikovat iniciační jevy a sekvence následných jevů, které mohou významně přispět ke škodám a újmám na chráněných aktivech.
2. Poskytnout realistické kvantitativní míry pravděpodobnosti výskytu jevů, které způsobí realizaci rizika.
3. Poskytnout realistické vyhodnocení potenciálních dopadů spojených s hypotetickými sekvencemi jevů, které vedou k havárii technologických celků.
4. Poskytnout rozumné podklady pro rozhodování o umístění, projektu a provozu technologie.

K hodnocení směřujícím k určení priorit pro zavedení preventivních a zmírňujících opatření se nejčastěji používá metodika PSA (Probabilistic Safety Assessment), tj. analytická metoda pro podporu ochrany veřejného zdraví a bezpečnosti. Výsledkem hodnocení je pak:

- seznam odezev zařízení na iniciační jevy a na sekvence jevů, které je mohou následovat,
- vyhodnocení významnosti identifikovaných přispěvatelů k riziku. Identifikují se vysoce rizikové sekvence, které vedou k havárii a zároveň i činnosti, které vedou k jejich zmírnění.

Je si třeba uvědomit, že zatím se tento intelektuálně náročný a propracovaný postup používá jen u jaderných zařízení, u vybraných chemických komplexů a v poslední době i u některých elektroenergetických centrál, např. [160].

Z teorie systémů a zvláště z vlastností systému systémů je zřejmé, že komplexní systém, jakým je elektroenergetická infrastruktura, je bezpečný, tj. funkční a spolehlivý jen tehdy, když jsou spolehlivé a funkční jeho subsystémy a když vazby a toky mezi nimi a dokonce i ty napříč mezi jednotlivými zařízeními a sítěmi subsystémů jsou žádoucí, tj. takové, že nevedou k nežádoucím jevům, tj. dlouhodobým výpadkům elektroenergetické soustavy, které mohou mít nepřijatelné dopady na chráněná aktiva, anebo mohou způsobit úplné nebo částečné narušení systému. Zajištění funkčnosti systémů a subsystémů v elektroenergetické infrastruktuře je více či méně vytvořeno historickým vývojem lidské společnosti (právní předpisy, normy a standardy různého druhu). Současné předpisy, zásady a pravidla se obvykle

vztahují na jednotlivé prvky či položky subsystémů a jen málo na vztahy a toky, které jdou napříč systémem a jeho subsystémy.

Na základě výše uvedených faktů o elektroenergetické soustavě, je soustava řízena jako uzavřený systém (tj. nezvažuje vnější pohromy – vichřice, zemětřesení apod.) a používá pro řízení pravděpodobnostní modely, tj. připouští existenci pouze náhodných odchylek (nezvažuje neurčitosti, které působí extrémní jevy), do kterých patří i skokové změny počasí.

Situace u elektroenergetické infrastruktury je komplikovanější v tom, že jsou již identifikovány vnitřní závislosti napříč subsystémy elektroenergetické infrastruktury, které se vyskytují na několika úrovních, a to fyzické, kybernetické, územní a organizační. Jinými slovy vznikají v důsledku místních technických propojení, finančních toků, energetických toků, informačních toků a toků vyvolaných usměrněnou činností managementu. Nesprávné zásahy managementu, a to především vrcholového vedou k nenapravitelným ztrátám. Podle ESRA [160] sem patří i nesprávná rozhodnutí managementu, která vedou k nedostatečné údržbě, nedostatečné kvalitě oprav apod.

Aplikace metody AHP [15] na elektroenergetickou soustavu dovoluje rozložit složitý problém bezpečnosti elektroenergetické soustavy do horizontální a vertikální hierarchie. V horizontální hierarchii lze sledovat propojení distribučních úrovní (lokální, regionální, státní, evropské). Ve vertikálních rovinách lze sledovat propojení v jednotlivých distribučních úrovních. Na základě takto provedené analýzy [161], jsou odhaleny následující problémy:

1. Úsek elektroenergetické soustavy - struktury soustavy místní, regionální, státní a EU; propojení soustavy místní, regionální, státní a EU; vzájemná propojení místních soustav do regionální, regionálních soustav do státní a státních soustav do EU; kritické prvky soustavy místní, regionální, státní a EU; kritická propojení soustavy místní, regionální, státní a EU; kritická propojení napříč úrovní soustavy; bezpečný stav a jeho limity pro soustavu v čase a území na různých úrovních, který je odrazem dynamického chování soustavy v proměnných podmínkách – podmínky normální, abnormální a kritické; nejzranitelnější kritická propojení, která jsou nejpravděpodobnějšími příčinami selhání soustavy; a informační toky od elektroenergetiků k veřejné správě v případě kritických podmínek.
2. Úsek působení pohrom na elektroenergetickou soustavu - velikost ohrožení soustavy od všech možných pohrom, které postihnou úroveň místní, regionální, státní a EU; zranitelnost soustavy při nadprojektových pohromách na úrovni místní, regionální, státní a EU; zranitelnosti propojení soustavy u pohrom projektových i nadprojektových na všech úrovních (!!! - dosud se normativně nesleduje se při projektování, výstavbě a provozu); zranitelnosti toků (kybernetických, materiálových, řídících,...) v soustavě při pohromách projektových i nadprojektových na všech úrovních (!!! - dosud se normativně nesleduje při projektování, výstavbě a provozu); pružná odolnost (houževnatost) soustavy u kritických pohrom na úrovni místní, regionální, státní a EU; pružné odolnosti propojení soustavy u pohrom projektových i nadprojektových na všech úrovních (!!! - dosud se normativně nesleduje při projektování, výstavbě a provozu); pružné odolnosti toků (kybernetických, materiálových, řídících,...) v soustavě při pohromách projektových i nadprojektových na všech sledovaných úrovních (!!! - dosud se normativně nesleduje při projektování, výstavbě a provozu); adaptační kapacita u kritických pohrom na úrovni místní, regionální, státní a EU; adaptační kapacita propojení soustavy u pohrom projektových i nadprojektových na všech úrovních (!!! - dosud se normativně nesleduje při projektování, výstavbě a provozu); adaptační kapacita toků (kybernetických, materiálových, řídících,...) v soustavě při pohromách projektových i nadprojektových na všech úrovních (!!! - dosud se normativně nesleduje při projektování, výstavbě a provozu).
3. Úsek vztahu nouzových situací a chování elektroenergetické soustavy - soubor dopadů možných pohrom na soustavu v místě, regionu, státě a EU; riziko selhání soustavy při možných nadprojektových pohromách v místě, regionu, státě a EU.

4. Úsek řízení elektroenergetické soustavy - provozní předpisy pro normální, abnormální a kritické podmínky; odezva - postupy pro zvládnutí dopadů nadprojektových pohrom na různých úrovních soustavy a u různých propojení a toků napříč úrovní soustavy na úrovni elektroenergetiků; obnova – postup pro obnovení provozu v území po dlouhodobých výpadcích na různých úrovních soustavy a u různých propojení a toků napříč úrovní soustavy na úrovni elektroenergetiků; aplikace poučení (preventivní a zmírňující opatření) z dlouhodobých výpadků soustavy na úseku řízení elektroenergetiků.
5. Úsek vztahu řízení bezpečnosti území a řízení bezpečnosti elektroenergetické soustavy - odezva - postupy pro zvládnutí dopadů nadprojektových pohrom na různých úrovních soustavy a u různých propojení a toků napříč úrovní soustavy na úrovni veřejné správy, záchranných složek, právnických a fyzických osob a občanů; obnova – postup pro obnovení života v území po dlouhodobých výpadcích na různých úrovních soustavy a u různých propojení a toků napříč úrovní soustavy na úrovni veřejné správy, právnických a fyzických osob a občanů; aplikace poučení (preventivní a zmírňující opatření) z dlouhodobých výpadků soustavy na úseku řízení území u veřejné správy, právnických a fyzických osob, občanů a záchranných složek; vytipovat nároky na elektroenergetiky z pohledu řízení bezpečnosti území; najít zdroje a prostředky pro aplikaci požadavků na zodolnění soustavy z pohledu bezpečnosti území; vytvořit proces řízení aplikace požadavků na soustavu, které je nutno aplikovat z pohledu řízení bezpečnosti území (monitoring, nápravná opatření,..).

Zatímco první dva body jsou zásadní pro úsek prevence, další jsou důležité pro připravenost a další fáze zajišťování bezpečí a udržitelného rozvoje lidí v určitém území.

Cílem bezpečnosti, a tím i ochrany elektroenergetické infrastruktury, je při umísťování, projektování, výstavbě a provozu (tj. při každém z uvedených kroků) třeba zajistit, aby elektroenergetická soustava plnila požadované funkce za všech podmínek (normálních, abnormálních a kritických) a zabránit ji, aby neprováděla činnosti, které by mohly vyvolat nepřijatelné dopady na elektroenergetickou infrastrukturu i na celý lidský systém. To znamená, že do praxe se musí implementovat vhodná technická, právní, organizační, ekonomická a vzdělávací opatření, jejichž cílem je zajistit spolehlivý provoz konkrétních částí elektroenergetické infrastruktury za projektových podmínek a za nadprojektových podmínek omezit a zmírnit dopady na lidi a životní prostředí, přičemž povinnost jejich použití musí být vyžadována právem, protože jsou náročná na zdroje, síly a prostředky. Povinnost pro nadprojektové podmínky je však dnes v ČR a v řadě dalších zemí kodifikována jen u jaderných technologií, tj. není požadována u elektroenergetických infrastruktur.

Protože nelze náhle vytvořit elektroenergetickou soustavu v novém pojetí, je třeba zodolnit stávající elektroenergetickou soustavu. To znamená, že se musí územně zmapovat všechny možné problémy existujících částí elektroenergetické infrastruktury, které mohou vyvolat nežádoucí dopady na lidský systém. Pro spolehlivý provoz se musí připravit dobře zaměřená opatření odezvy a obnovy, které ve variantách musí předpřipravit výzkum, který je musí komplexně namodelovat, otestovat, určit priority a zásady řízení bezpečnosti.

Pro nové elektroenergetické soustavy, které mají být bezpečné, tj. neohrožovat lidi a přitom být funkční a spolehlivé, se musí kodifikovat nová pravidla pro umístění, projektování, výstavbu a provoz, která z inženýrského hlediska stanovují podmínky a limity provozu, zajišťují instalaci bezpečnostních systémů (aktivní, pasivní i hybridní) a zajišťují jejich vhodné zálohování. To znamená, že řeší otázky typu:

- jaké bezpečnostní systémy jsou vhodné a jaké musí být jejich zálohování?
- kde / ve kterých místech bezpečnostní systémy působí nejúčinněji?
- proč jsou použity právě tam a ne jinde?
- v jakých limitech spolehlivě pracují?

Protože nic není absolutně bezpečné, tak je třeba počítat s tím, že každá elektroenergetická infrastruktura selže nebo může selhat dříve nebo později. Proto musí existovat pravidla pro

zvládnutí nouzových situací, která zkrátí výpadek infrastruktury či technologie na minimum a zmírní dopady na lidi a životní prostředí, tj. vytvářet se vnitřní a vnější nouzové plány. U elektroenergetických infrastruktur se v praxi vyspělých zemí vytváří také nouzové plány ve formě plánů kontinuity, které zajistí, že daná elektroenergetická infrastruktura a tím i celý lidský systém přežijí toto selhání objektů, infrastruktur a technologií a pro nejhorší případy se připravují krizové plány, které zabrání nebo výrazně zmírní nepřijatelné dopady na zdraví a bezpečí lidí.

Pro zajištění spolehlivé funkce elektroenergetické infrastruktury příslušný management musí respektovat dále uvedené zásady:

- činnost zaměřovat vždy na podstatné aspekty,
- včasné varování obyvatel, zaměstnanců, návštěvníků před blížící se pohromou považovat za základ úspěchu, za základ snížení (lépe zabránění) ztrát na životech,
- cíl řízení stanovovat tak, aby zajišťoval udržitelný rozvoj a aby byl prozíravý, tj. aby upřednostňoval ochranu životů, zdraví a bezpečí lidí tím, že primární pozornost se vždy soustředí na snižování zranitelnosti systému,
- pozornost vždy věnovat tomu podsystému, který je nejzranitelnější,
- zvládání nouzových situací zaměřit na potřeby a priority, přičemž základní prioritou je ochrana lidí a ochrana kritických zdrojů a systémů, na nichž závisí existence společnosti,
- podporovat kulturu bezpečnosti a maximální pozornost věnovat prevenci,
- zajištění připravenosti na zvládnutí nouzových situací zahrnovat do programu rozvoje území,
- občané mají právo na pomoc (asistenční službu) a pomoc se musí poskytovat konzistentně bez ohledu na ekonomické a sociální okolnosti a územní lokalizaci,
- občané patří do systému odezvy na nouzové situace nejen jako potenciální oběti, ale i jako aktivní prvky odezvy,
- zajišťovat, aby občané věděli, co jsou krizové plány a plány odezvy na nouzové situace a co přinášejí, jaká je jejich odpovědnost, jak mohou napomoci v prevenci vzniku pohromy či nouzových situací, jak mají reagovat, a proč, apod.,
- systém řízení bezpečnosti i krizové řízení musí být transparentní i pro občany a musí být přizpůsobeny místním podmínkám,
- systém řízení bezpečnosti i krizové řízení musí mít legitimitu, musí být udržitelné a přijatelné a musí být založeny na systémovém přístupu.

Pro všechny výše uvedené a další potřeby je třeba pro rozhodování mít namodelované možné situace ve variantním provedení. Z důvodů reality je třeba mít namodelované případy, na které se nejčastěji zaměřuje metodika případových studií [15], a to:

- extrémní nebo úchylné případy (důvodem je, že zpravidla z hlediska bezpečí a rozvoje je třeba se těmto případům vyhnout, tj. přijmout vhodná opatření, aby se nemohly vyskytnout),
- kritických případů (důvodem je, že zpravidla z hlediska bezpečí a rozvoje jsou tyto případy strategicky důležité, protože vytváří rozhraní, na kterém jsou riziko selhání a ztráty spojené s realizací rizika vysoké, a při jeho překročení výskyt katastrofy je vysoce pravděpodobný a neodvratitelný, tj. jde o nepřijatelné riziko),
- paradigmatických (vzorových) případů (důvodem je z hlediska bezpečí a rozvoje navrhnout vhodnou realizaci možných řešení pro obvyklé případy v praxi).

V České republice je nutné u výzkumu sledovaného problému, tj. pro zvládání dlouhodobých selhání elektroenergetické soustavy, přejít od slohových prací na dané téma k vědeckému výzkumu, který bude opřen o:

- kvalifikovaná data pro potřebu aplikace přístupu All- Hazard-Approach [8],
- kvalifikovanou identifikaci, diagnostiku a prognózování dlouhodobých selhání elektroenergetické soustavy v souladu s přístupem All-Hazard-Approach,
- kvalifikovaný návrh opatření preventivních, zmírňujících, reakčních a obnovovacích,

- stanovení rolí všech zúčastněných a vytvoření systému pro jejich zapojení a způsobu řízení tohoto systému.

Protože úlohy spojené s dlouhodobými selháními elektroenergetické soustavy jsou rozmanité a značně různorodé, je třeba podle povahy úlohy sebrat data, vybrat vhodné metody jejich zpracování (metoda závisí na formátu, vlastnostech a vypovídací schopnosti dat) a udělat spolehlivé metody. Globálně bohužel nelze stanovit jeden postup, který vyřeší vše.

Na základě shromážděných poznatků a celoživotních zkušeností si dovoluji na závěr studie napsat několik doporučení:

1. Problém řízení území, které je zacílené na bezpečí a udržitelný rozvoj lidí s ohledem na dlouhodobá selhání elektroenergetické soustavy na úrovni lokální, regionální, státní i evropské je zásadního významu.
2. Sledovaný problém je mnoha oborový, interdisciplinární a vyžaduje znalosti, data, kvalitní strategické, taktické i operativní řízení založené na principech znalostního managementu. Proto v první fázi je třeba problém strukturovat tak, že jednotlivé odborné skupiny budou řešit to, co umí a budou vedeni týmem, který zajistí interoperabilitu jejich výstupů v území. To platí i o modelech, které musí vycházet ze stavu konkrétních znalostí o dílčích problémech a postupně být propojovány tak, aby byla zajištěna jejich kompatibilita a interoperabilita. Teprve posouzení kvality znalostí a kvality souboru disponibilních dat umožní pro jednotlivé problémy (uvedené výše) vybrat vhodné nástroje pro sestavení modelů, které mají vypovídací schopnost a které budou pracovat jak autonomně, tak ve větším celku s ohledem na požadovanou interoperabilitu.
3. Protože bez relevantních dat žádnou ochranu obyvatelstva vůči žádné pohromě, a to včetně dlouhodobého výpadku elektroenergetické soustavy, nezajistíme, je třeba v první fázi zajistit kvalifikovaná data o dopadech dlouhodobých selhání elektroenergetické soustavy v konkrétních lokalitách, regionech a státu. Protože v ČR žádnou takovou databázi nemáme, tak v první fázi stačí nástroj What, If; vrstva GIS a několik časových úseků – 1 hodina, 3 hodiny, 1 den, 3 dny, 14 dní, 1 měsíc, 3 měsíce, 180 dní. Vytvoření cílené databáze vyžaduje určitou odbornost a metodickou zručnost a je časově náročné. Výsledek však umožní kvalifikované řešení úkolů ochrany obyvatelstva ve variantách s ohledem na rozmanitou kombinaci náhodných jevů možných v konkrétním území. Vzhledem k tomu, že pohromy v nejširším pojetí, které je ve studii zvažováno, mají různou fyzikální podstatu (tj. nejsou to mimořádné události bez fyzického naturelu), tak konkrétní dopady či intenzita na elektroenergetickou soustavu se různí podle kombinace vlastností pohromy a místních zranitelností chráněných zájmů, proto databáze musí být sestavena odděleně pro jednotlivé možné pohromy.
4. Jestliže stát bude mít databázi možných dopadů selhání elektroenergetické soustavy v časoprostoru, tak může dělat modely nad územím, modely dopadů v časoprostoru a k nim pomocí základních kritérií pro přežití lidí určit potřeby ochrany obyvatelstva. Na jejich základě modelovat strom závislosti veřejných služeb ve variantách a podle těchto dat rozpracovávat například model zásobování, model chování obyvatelstva apod. (přitom aplikovat např. metody teorie grafů, metodu kritické cesty, síťové metody v deterministickém, stochastickém, fuzzy i expertním pojetí).
5. Protože odborný svět již více než 10 let řeší problémy systému systémů, je třeba zajistit kvalifikované vzdělávání a kvalifikovaný výzkum v předmětné oblasti i v ČR a upustit od toho, co je jednoduché a nevyžaduje úsilí a znalosti, protože podcenění složitosti a závažnosti problému by se mohlo nevyplatit a mohlo by v budoucnu přinést nemalé celospolečenské náklady.

5.7. Výsledky studia rizik produktovodů a návrh ochranných opatření

Produktovody jsou dlouhé liniové potrubní struktury a technologická zařízení, které slouží v přepravě tekutin, tj. kapalin a plynů. Jedná se o zařízení, která jsou umístěna na otevřených prostranstvích nebo uložena v podzemí. Vyznačují se vysokým stupněm automatizace, značnými objemy přepravovaných látek a vzájemnou provázaností s jednotlivými provozy a skladovacími zařízeními. Součástí dálkovodů jsou také přečerpávající stanoviště, zařízení sloužící pro měření, údržbu a regulaci procesu přepravy („šachty“) a zabezpečovací zařízení. Provoz dálkovodů je většinou ovládán z dispečerského pracoviště, se kterým je nutné se vždy kontaktovat [178,179].

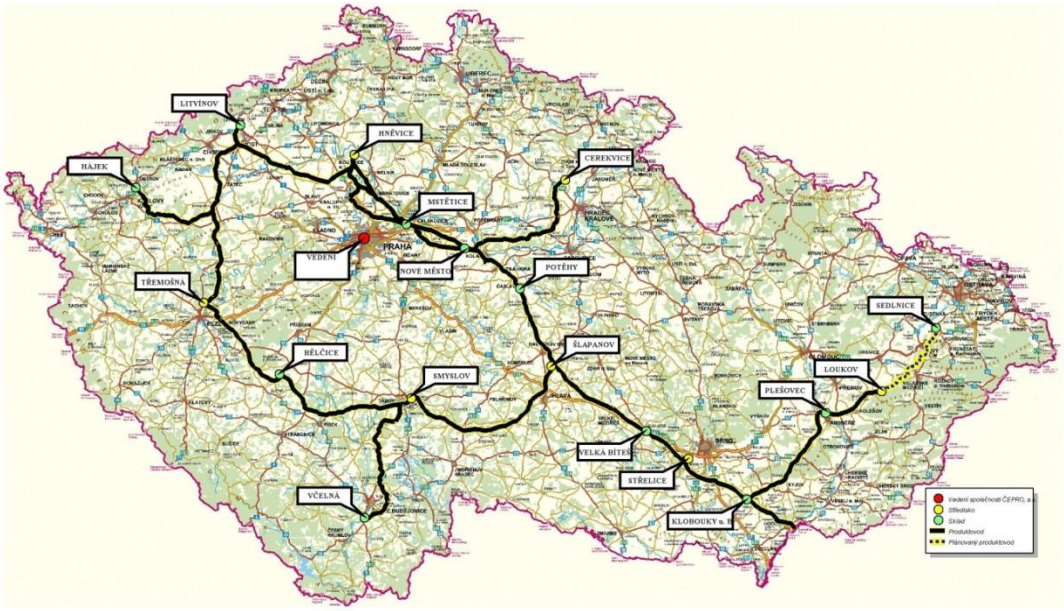
Z hlediska ochrany lidí jsou však velmi nebezpečné produktovody, jak ukazuje havárie produktovodu Sibiř – Ural – Povolží s uhlovodíkem dne 4. 7. 1989 u města Aša [10]. Zemřelo při ní 575 lidí, 181 z nich děti, zraněno bylo více než 600 lidi. Ztráta v penězích 3 miliony 318 tisíc rublů. Kořenovou příčinou byla chyba při výstavbě, nedodržené normy [12]. Pro ČR mají strategický význam ropovody a plynovody, a proto se na ně dále soustředíme.

5.7.1. Ropovody a jejich řízení v ČR

Nejdůležitější je ropovod Družba, který je nejdelší na světě, obrázek 26. Ropovod Družba vstupuje na české území na břehu řeky Moravy u Hodonína. Překonává Vysočinu, kde je v některých úsecích zdvojen, a míří polabskou nížinou ke Kralupům, kde přepravovanou ropu ukládá do nádrží v Centrálním tankovišti v Nelahozevsi. Odtud vede další pokračování ropovodu Družba do rafinérie u Litvínova. Ropovod má také odbočku poblíž obce Potěhy u Čáslavi, kterou je potrubím o průměru 200 mm zásobována rafinerie Paramo v Pardubicích. Česká část ropovodu Družba je dlouhá 357 km, včetně zdvojení a odboček 504 km. Přepravní kapacita je 9 mil. tun ropy ročně, průměr potrubí 528 mm. Ropa v tomto potrubí proudí rychlostí kolem 1.4 m/s, průměrná hloubka uložení potrubí v zemi je 1,3 metru. Potřebný tlakový spád k překonání výškových rozdílů na trase zajišťuje několik čerpacích stanic. Maximální vstupní tlak v potrubí hned za čerpací stanicí je 62 barů (6.2 MPa) a po délce trasy ropovodu postupně klesá až na hodnotu cca 22 barů (2.2 MPa) před další čerpací stanicí nebo skladovací nádrží.

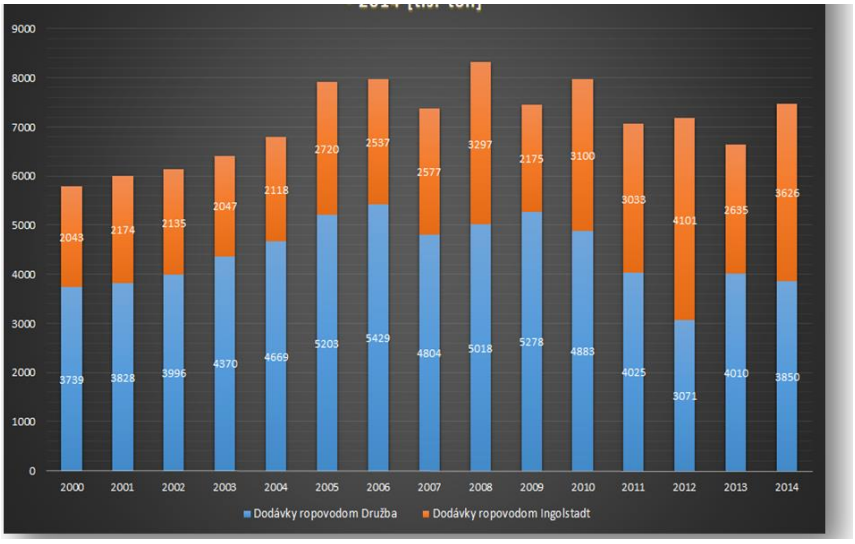
Ropovod Družba se stavěl v letech 1961 až 1972. Od té doby byl zmodernizován, po částech se také zlepšuje izolace potrubí na úroveň současných technologií. Vše je pod neustálým pečlivým dohledem řídicího systému, automatický sběr dat o stavu ropovodu doplňují hlášení terénních pracovníků, tzv. trasařů. Ti odečtou další doplňující údaje z přenosných přístrojů. Trasa ropovodu je rozdělena do mnoha desítek úseků, dělicími body jsou armatury ve speciálních šachtách. Armaturní šachty s ventily, které lze ovládat dálkově, ale v případě potřeby i ručně, jsou rozmístěny na trase nerovnoměrně, hustěji v exponovaných oblastech půdních zlomů nebo vodotečí. Elektronické snímače v těchto šachtách neustále vysílají údaje o teplotě přepravované ropy a teplotě okolí, o tlaku v potrubí, hustotě ropy a hodnotách dalších měřených veličin [178,179].

Optický komunikační kabel přenáší ze všech měřících míst na ropovodu údaje do řídicího systému ve velíně na Centrálním tankovišti v Nelahozevsi. Operátoři zjistí možné úniky ropy nejpozději do dvou minut; z centra okamžitě ropovod odstaví a uvědomí záchranné týmy v příslušné lokalitě. Dálkově ovládané ventily v armaturních šachtách totiž během několika málo minut přeruší tok ropy v podezřelém úseku, v ostatních úsecích se ropa také zastaví, ale potrubí zůstane v provozním stavu. Po opravě nebo jiném místním zásahu se tak ropa téměř okamžitě pohne po celé trase směrem k místu určení [179].



Obr. 26. Trasa ropovodu Družba [178,179].

Ropovod Ingolstadt (oficiální zkratkou IKL podle plánované trasy Ingolstadt - Kralupy nad Vltavou - Litvínov. Na území ČR je provozovatelem ropovodu Družba i IKL akciová společnost MERO ČR (MEzinárodní ROpovody). Porovnání množství ropy přepravené oběma ropovody je na obrázku 27. Obrázek 27 ukazuje, že ropovod Družba má pro ČR stále velký význam.



Obr. 27. Porovnání množství ropy přepravené ropovody v letech 2000 – 2014 [179].

Hospodaření s ropou upravuje zákon č. 189/1999 Sb., o nouzových zásobách ropy, o řešení stavů ropné nouze a o změně některých souvisejících zákonů (zákon o nouzových zásobách ropy) [180]. Zákonem č. 240/200 Sb., o krizovém řízení a na něho navazujícím nařízením vlády č. 432/2010 Sb. je stanoveno devět odvětví kritických infrastruktur. Ropa a ropné produkty patří pod první odvětví, energetiku. Jako všechny ostatní prvky kritické infrastruktury tak i ropovody vyžadují zvláštní ochranu před vznikem havárie nebo selháním systému [10,11]. Jedním z takových opatření je i povinnost vytváření zásob ropy státem na 90 dní (centrální úložiště Nelahozeves) plus další zásoby vytvářené ropným průmyslem na 30 dní.

Požadavky na výstavbu a provoz produktovodů jsou shrnuty v práci [181]. Dle práce [182] je třeba přijímat dostatečná opatření pro zabránění velkým haváriím na produktovodech a k omezení jejich dopadů na obyvatelstvo a životní prostředí. Jde hlavně o produktovody přepravující látky, které jsou: velmi jedovaté; jedovaté; hořlavé; velmi hořlavé; nebezpečné pro životní prostředí; a nebezpečné vzhledem k bouřlivé reakci při styku s vodou a uvolňování jedovatých plynů [29].

EU se snaží zavést do praxe v členských zemích povinnosti obdobné těm, co jsou pro průmyslové objekty v direktivě SEVESO, tj. provádět řízení bezpečnosti, a v jeho rámci zpracovávat nouzové plány pro případ havárií, jejichž cílem by bylo zvládání provozních nehod, provedení opatření na ochranu osob, životního prostředí a majetku, poskytování nezbytných opatření veřejnosti a zajištění obnovy a vyčištění životního prostředí.

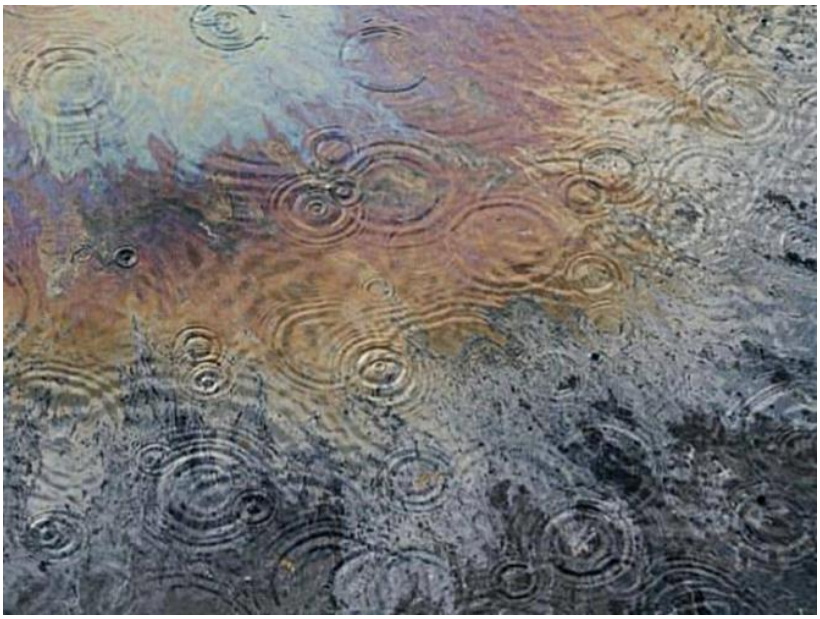
5.7.2. Havárie ropovodů a jejich scénáře

Únik ropy z dobře ošetřovaného potrubí se stane jednou za několik let, v naprosté většině po zavinění „třetích stran“, nikoliv tedy majitelem ropovodu nebo majitelem parcely dotyčného katastru, ale obvykle špatně navedenými stavebními mechanismy při zemních pracích pro zcela jiné účely [183]. Příklad havárie ropovodu Družba v Maďarsku je na obrázku 28.

Obr. 278. Příklad havárie ropovodu Družba v Maďarsku [184].

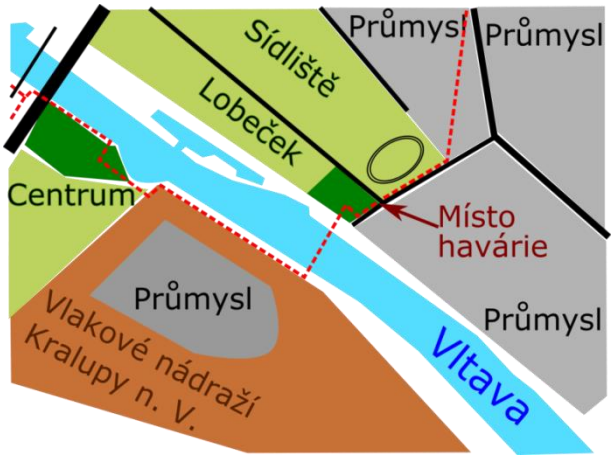
Na většině území České republiky jsou ropovody vedeny pod zemí. Jsou však místa, kde z důvodů geologických, nebo místně geografických je nutné ropovod vést nad zemí. Nadzemní části ropovodu jsou pak více zranitelné z pohledu havárií a úniků ropy. Za určitých okolností může dojít i k narušení podzemních částí. V souvislosti se sítí ropovodů můžeme identifikovat dvě různá ohrožení, a to selhání dodávek ropy a únik ropy do okolí. Při havárii ropovodu může dojít k realizaci jednoho nebo druhého ohrožení, popřípadě ke kombinaci obou. Dle údajů v [12,185] se v ČR vyskytly dále uvedené velké úniky ropy:

- 3. – 4. 11. 1980 u obce Bartoušov (v důsledku trhlina na svaru došlo k úniku ropy; uniklo cca 6000 t ropy do řeky a podloží; odstraňování následků trvalo 2 roky; obrázek 29 ukazuje znečištěnou řeku, což způsobila sledovaná havárie,
- 27. 1. 2005 u města Čáslav (poškození potrubí u obce Žáky; uniklo asi 130 m^2 surové ropy; znečištěno území o rozloze 8000 m^2).



Obr. 29. Únik ropy z ropovodu 3. – 4. 11. 1980 u obce Bartoušov [186].

Analýza dopadů dvou vybraných scénářů havárie ropovodů je provedena v práci [183]. První scénář havárie je umístěn na území města Kralupy nad Vltavou v místě, kde je ropovod vedený nad povrchem, a to kvůli překonání řeky. Kolem ropovodu vede silnice, obrázek 30. Havárie je způsobena motorovým vozidlem, které v zatáčce naboural do nadzemní části ropovodu a způsobí tak jeho mechanické poškození, které je následováno prudkým únikem ropy do okolí. U scénáře předpokládáme standartní klimatické podmínky. Dopady získané aplikací metody What, If jsou uvedené v tabulce 10.



Obr. 30. Kralupy nad Vltavou, místo havárie ropovodu; plné černé čáry značí pozemní komunikace, červená přerušovaná čára značí ropovod, který se v celé oblasti nachází nad zemí [187].

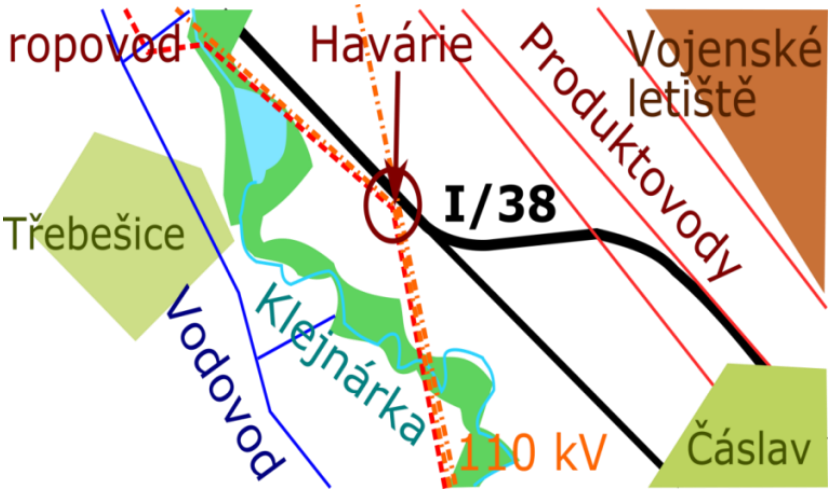
Tabulka 10. Dopady sestavené metodou „Co se stane, když“ pro scénář havárie v Kralupech nad Vltavou na obrázku 30 [183,187].

Chráněná aktiva	**Dopady na chráněná aktiva**
Životy a zdraví lidí	0h: poraněni / smrt posádky vozidla v důsledku havárie vozidla; poškození zdraví náhodní kolemjdoucích, kteří se dostanou do přímého kontaktu s ropou – vdechnuti ropy, styk pokožky s ropou, zasáhnuti očí – vážné ohrožení zdraví; velký požár způsobí i smrt buď přímo, nebo nadýcháním zplodin hoření ropy. 6h: nebezpečí poškození zdraví vlivem výparů a zplodin požáru u obyvatel okolního sídliště Lobeček; příslušníci integrovaného záchranného systému mohou vdechnout výpary ropy, styk pokožky s ropou, zasmahnutí očí. 12h: poškození zdraví osob zasáhnutých ropou/ ropnými výpary až s následkem smrti; poškození zdraví obyvatel okolního sídliště Lobeček na zdraví/ smrť v důsledku ropných výparů, zplodin hoření, ohně, výbuchů; poškození zdraví i u obyvatel města Kralupy nad Vltavou v důsledku šíření ropných výparů a zplodin požáru v závislosti na směru šíření větru. 24h: poškození zdraví obyvatel v důsledku zplodin hoření a ropných výpary přetrvávají, dokud se požár neuhasí. 3dni+:-
Bezpečí lidí a veřejné blaho	0h: - 6h: růst nebezpečí pro lidi okolitého sídliště Lobeček v důsledku vzniknutého požáru / výbuchu; ohrožení obyvatel města Kralupy nad Vltavou v důsledku šíření ropných výparů v závislosti na směru šíření větru; obavy panika. 12h: snížení dostupnosti nouzových služeb v důsledku zásahu IZS; přerušení dodávek elektrického proudu v důsledku přerušeni vedeni vysokého napětí 110 kV. 24h: - obavy panika se prohlubují, když nebude uhašen požár a budou se šířit ropné výpary a zplodiny hoření. 3dni+: ekonomické dopady na ropný trh; obava z očekávání růstu cen benzínu a nafty.
Majetek	0h: poškozeni/zničeni havarovaného vozidla; velké škody na tělesu poškození časti ropovodu; poškození majetku v místě havárie (vozovka, lampa pouličního osvětleni) vlivem požáru/ kontaminace ropou. 6h: poškození majetku v přilehlé oblasti sídliště/průmyslové oblasti Lobeček, (automobily, domy, obchody, občanská vybavenost, atd.) v důsledku rozšířeni požáru/ výbuchy / kontaminace ropou. 12h: poškození majetku celého sídliště / průmyslové oblasti Lobeček, (automobily, domy, obchody, občanská vybavenost, atd.) v důsledku rozšíření požárů/ kontaminace ropou; poškození majetku časti města Kralupy nad Vltavou v závislosti na směru šíření ropných výparů (kontaminace povrchu oken, automobilů, budov, atd.). 24h: škody na majetku v důsledku styku s ropou/požárům/ropnými výparům se prohlubují. 3dni+: -

Životní prostředí	0h: kontaminace zeminy v zasažené oblasti nehody (lesopark). 6h: kontaminace zeminy v zasažené oblasti sídliště/průmyslové oblasti Lobeček; kontaminace řeky Vltava; znečistění ovzduší ropnými výpary a zplodinami požárů. 12h: kontaminace hlubších vrstev zeminy v poškozené oblasti sídliště/průmyslové oblasti Lobeček; kontaminace podzemních vod; šíření ropné kontaminace po proudu řeky Vltavy (Labe); rozšířeni znečistění ovzduší ropnými výpary a zplodinami požárů v závislosti na směru šíření větru. 24h: škody a újmy na životné prostředí v důsledku kontaminace ropou/ požárem/ ropnými výpary se zvětšují. 3dni+: závažné narušení zasmahnutých biotopů (ekosystémy řeky Vltava / Labe, přírodní park Dolní Povltaví).
Dodávky energií (elektřina, pohonné hmoty)	0h: - 6h: poškození vedení vysokého napětí 110 kV v důsledku šíření požárů (přerušení dodávek elektrický energie v oblasti zásobované poškozenými větvemi); přerušení zásobovaní ropou okolního ropného průmyslu v důsledku poškození ropovodu. 12h: - 24h: Nutnost zásobování ropného průmyslu z nouzových zdrojů, nebo alternativními cestami; prohloubení problému zásobovaní místního ropného průmyslu. 3dni+: nárůst cen pohonných hmot a dalších ropných produktů; zhoršení veřejného mínění o spolehlivosti dodávek ropy.
Přepravní síť	0h:- 6h: uzavření a objížďky na pozemních cestách, silniční síť (č. 101), železniční síť (vlaková stanice Kralupy nad Vltavou), říční síť (Vltava); přetížení okolní infrastruktury pozemních komunikací v důsledku evakuace obyvatel. 12h:- 24h:- 3dni+: zvýšeni přepravních nákladů; náklady na obnovu poškozených komunikací.
Ostatní kritické infrastruktury	0h: - 6h: kontaminace vody v studních a podzemních vrtech; vyřadění kybernetické infrastruktury v oblasti výpadku elektrické energie; únik ropy do kanalizace, dosáhnutí kritické hodnoty koncentrace ropných výparů, výbuchy po celé oblasti Lobeček. 12h: nedostupnost prvků kritické infrastruktury (finanční služby, státní správa, komunikační služby, vzdělávací zařízení…) v uzavřené oblasti Kralupy nad Vltavou. 24h:- 3dni+: negativní vliv na finanční sektor; finance na zásah; ušlý zisk průmyslu v evakuovaných oblastech; ušlý zisk průmyslu vlivem problémů se zásobováním ropou.
Nouzové služby (policie, hasiči, zdravotníci)	0h: - 6h: zvýšená zátěž na složky IZS v důsledku řešení ropné havárie / snížená dostupnost záchranných složek v regióne.

	12h: zhoršení stavu IZS v důsledku poškození zdraví příslušníků a vybavení vlivem požárů / přímému kontaktu s ropou / vdechnutí ropných výparů. 24h: - 3dni+: chronická únava příslušníků IZS v důsledku dlouho trvajících zásahových prací; velké náklady na odezvu.
Veřejná správa	3dni+: zvýšené náklady na ochranná opatření pro obyvatelstvo; náklady na obnovu území – zvláště, když dojde ke kontaminaci podzemní vody a bude třeba zajistit dlouhodobé zásobování obyvatelstva pitnou vodou v postižené oblasti; náklady na opravu ropovodu.

Pro modelování dalšího scénáře je vybráno jako místo vzniku pole nedaleko města Čáslav, obrázek 31. V důsledku výkopových prací bez seznámení se s inženýrskými sítěmi a dalšími prvky v území dojde k mechanickému narušení ropovodu těžkým strojem (bagr) například podle vzoru [188]. Při sestavení dopadů metodou „Co se stane, když“, tabulka 11, jsme předpokládali velmi nepříznivé podmínky v podobě sucha a vysokých teplot (větších než 30°C). Dopady jsou uvedené v tabulce 11.



Obr. 31. Místo havárie ropovodu nedaleko Čáslavi; plné černé čáry značí pozemní komunikace, červená přerušovaná čára značí ropovod, oranžové čáry značí elektrické vedení [187].

Tabulka 11. Dopady sestavené metodou „Co se stane, když“ pro scénář havárie nedaleko Čáslavi na obrázku 31 [183,187].

Chráněná aktiva	**Dopady na chráněná aktiva**
Životy a zdraví lidí	0h: škody na zdraví / ztráty na životech původců nehody. U lidí, kteří poškodí ropovod 6h: škody na zdraví / životech lidí v blízkých obcí následkem šíření ropných výparů ovzduším; možné poškození zdraví příslušníků IZS přímém styku s ropou; poškození zdraví / lidí v blízkých obcí následkem sekundárních požárů. 12h: škody na zdraví / životech lidí v regióne v následku rozšiřováni sekundárních požárů. 24h: přehřátí a dehydratace příslušníků IZS zasahujících při likvidaci požárů.

	3dni+: škody na zdraví / životech lidí v rozsáhlých oblastech vlivem rozšiřováni požárů, které se vlivem tropických teplot nedaří uhasit.
Bezpečí lidí a veřejné blaho	0h: - 6h: Výrazné zvýšení nebezpečí u lidí v okolí zplodinami hoření a ropnými výpary, strach, panika 12h: obavy a strach u lidí v těsné blízkosti; snížení dostupnosti nouzových služeb v důsledku zásahu IZS; výpadky dodávek elektrického proudu v důsledku přerušeni vedení vysokého napětí. 24h: - růst paniky, když se bude požár dále šířit a ropné produkty budou v potoce a v rybníku nebo na zahrádkách občanů 3dni+: ekonomické dopady na ropný trh.
Majetek	0h: poškození/zničení zařízení zodpovědného za vznik nehody; poškození časti ropovodu; poškození sloupů elektrického napětí. 6h: poškození majetku v přilehlých obcích (automobily, domy, obchody, občanská vybavenost, atd.) v důsledku vzniku sekundárních požárů; poškození majetku, technického vybaveni a infrastruktury vojenského letiště Čáslav v důsledku vzniku požáru. 12h: poškození majetku v regionu v následku rozšiřovaní sekundárních požárů. 24h: - 3dni+: poškození majetku lidí v rozsáhlých oblastech vlivem rozšiřovaní požárů, které se vlivem tropických teplot nedaří uhasit.
Životní prostředí	0h: kontaminace půdy v poškozené oblasti nehody. 6h: kontaminace půdy v rozsáhlé oblasti okolo nehody; kontaminace říčky Klejnárka a přírodního biotopu rybníku Vrabcov a okolí. 12h: kontaminace hlubších vrstev půdy v rozsáhlé oblasti okolo nehody; kontaminace podzemních vod; kontaminace po proudu řeky Klejnárka; rozšířeni znečistění ovzduší ropnými výpary a zplodinami požárů. 24h: kontaminace potoka Brslenka; újmy na floře a fauně v okolí v důsledku kontaminace ropou/ požáry/ ropnými výpary a zplodinami požárů se prohlubují. 3dni+: kontaminace řeky Doubrava; závažné narušeni zasáhnutých biotopů (přírodní ekosystémy, orná půda, říční ekosystémy); kontaminace řeky Labe prostřednictvím řek Klejnárka / Doubrava.
Dodávky energií (elektřina, pohonné hmoty)	0h: poškození vedení elektrického napětí v důsledku tryskající ropy z potrubí (přerušeni dodávek elektrické energie v oblasti zásobované poškozeným elektrickým vedením). 6h: poškozovaní pevných prvků eklektické sítě (vedení, trafostanice) v důsledku vzniku sekundárních požárů. 12h: poškozovaní pevných prvků eklektické sítě v důsledku rozšiřujících se požárů. 24h: Nutnost zásobování ropného průmyslu z nouzových zdrojů, nebo alternativními cestami. 3dni+: nárůst cen pohonných hmot a dalších ropných produktů; zhoršení veřejného mínění o spolehlivosti dodávek ropy.
Přepravní síť	0h: - 6h: uzavření a objížďky na pozemních komunikacích, silniční síť (č. 38), železniční síť (trať SŽDC 230), letecká přeprava (vojenské letiště Čáslav); přetížení okolních pozemních komunikací v důsledku evakuace obyvatel. 12h: -

	24h: rozšířeni uzavírek na okolní pozemní komunikace v důsledku rozsáhlých požárů. 3dni+: zvýšeni přepravních nákladů.
Ostatní kritické infrastruktury	0h: - 6h: kontaminace vody v studních a podzemních vrtech; vyřazení kybernetické infrastruktury v oblasti výpadku elektrické energie; poškozovaní pevných prvků ostatních kritických infrastruktur vlivem vznikajících požárů. 12h: nedostupnost prvků kritické infrastruktury (finanční služby, státní správa, komunikační služby, vzdělávací zařízení, atd.) v zasáhnutých oblastech; poškozovaní pevných prvků ostatních kritických infrastruktur vlivem rozšiřujících se požárů. 24h: - 3dni+: negativní vliv na finanční sektor; finance na zásah; ušlý zisk průmyslu v evakuovaných oblastech; ušlý zisk průmyslu vlivem problémů se zásobováním ropou.
Nouzové služby (policie, hasiči, zdravotníci)	0h: - 6h: zvýšená zátěže na složky IZS v důsledku řešeni ropné havárie/ sekundárních požárů / snížená dostupnost záchranných složek v regionu. 12h: zhoršení akceschopnosti IZS v důsledku poškození zdraví příslušníků a vybavení vlivem požárů / přímému kontaktu s ropou / vdechnutí ropných výparů. 24h: : zhoršení akceschopnosti IZS v důsledku přehřátí a dehydratace příslušníků IZS zasahujících při likvidaci požárů. 3dni+: chronická únava příslušníků IZS v důsledku dlouho trvajících zásahových prací; velké náklady na odezvu
Veřejná správa	3dni+: zvýšené náklady na ochranná opatření pro obyvatelstvo; náklady na obnovu území – zvláště, když dojde ke kontaminaci podzemní vody a bude třeba zajistit dlouhodobé zásobování obyvatelstva pitnou vodou v postižené oblasti; náklady na opravu ropovodu.

Jak nám říkají zkušenosti ze světa [187], je sice ropovod nejbezpečnější způsob přepravy, nic méně i u ropovodů může dojít k významné poruše a úniku ropy do okolí. V případě takové události pak o rozsahu rozhoduje především rychlost odezvy a připravenost. Když se podíváme do tabulek 10 a 11 vidíme, že v prvních hodinách i při nepříznivých podmínkách dochází ke ztrátám, škodám a újmě na chráněných aktivech na relativně malém rozsahu území.

Z obrázků 30 a 31 je patrné, že v bezprostřední blízkosti ropovodů nejsou důležitá chráněná aktiva ve větší míře zastoupena. ***Pokud se ale připustí eskalace nouzové situace, zasažené území se rozšíří, pak začne docházet i k dopadům s fatálním rozsahem.*** Nejen že se rozšiřuje oblast zamořená ropou a s ní i množství ohrožených osob a chráněných zájmů především za nepříznivých podmínek, ale po několika hodinách může dojít i k nevratnému znečištění podzemních vod.

5.7.3. Vyhodnocení situace a návrh opatření na zvládnutí havárií ropovodů

Závěrem lze říci, že při kvalitní výstavbě a dostatečné údržbě je přeprava ropy za pomocí ropovodů nejbezpečnějším způsobem. Potvrzují to velké škody při přepravě ropy po železnici v USA a Kanadě, ke kterým došlo v posledním desetiletí [12], kterým se budeme věnovat v odstavci věnovaném dopravě. Avšak zatímco dostatečná údržba a správné řízení systému

můžou předejít havárii z vnitřních příčin, existuje neustále ohrožení ropovodu vnějšími vlivy, především v oblastech nadzemního vedení ropovodů. Vnější narušení ropovodu může být například způsobeno lidským faktorem, viz oba použité scénáře, který nelze nikdy zcela vyloučit. Když už dojde k předmětné havárii, hraje pak velkou roli rychlost a přesnost odezvy. V prvních hodinách je havárie spojena s malým množstvím mírných dopadů, ale se zvyšující se dobou trvání nouzové situace se dopady řádově prohlubují. Je proto potřeba, aby složky odezvy měly zajištěné včasné vyrozumění (monitoring), uměly rychle najít místo havárie (znalost trasy ropovodu) a věděly jak v místě postupovat (sestavení a procvičení plánu činností).

Z pohledu včasné odezvy na havárii ropovodu můžeme mluvit o několika nutných oblastech – monitoring, místo zásahu, plánování. V případě monitoringu jde o odhalení, že došlo k havárii a určení úseku jejího vzniku tak, aby mohlo dojít k vyrozumění příslušných složek odezvy. Kvalita monitoringu se zlepšuje s novými technologiemi a je tak o něco lepší v případě ropovodu IKL než v případě ropovodu Družba. V našich scénářích předpokládáme výrazné narušení a únik ropy, proto odhalení monitoringem je jednoduší než u drobných havárií, u kterých dochází k úniku malého množství po dlouhou dobu (následkem jsou pak významná znečištění půdy a podzemní vody).

Aby mohla být situace vyvolaná havárií správně a rychle zvládnuta, musí dorazit technické síly do místa havárie. Určení správného místa úniku ropy může být složité z několika důvodů. Monitoring poukáže na úsek potrubí, kde došlo k narušení potrubí a je nutné další zpřesnění lokalizace havárie. Místo havárie může být ve špatně přístupné oblasti (není případ popsaných scénářů), a jeho nalezení není jednoduché, protože přesné označení vedení ropovodů je utajené z bezpečnostních důvodů; před případným útokem zlodějů či jiných kriminálních živlů. Předmětná skutečnost brání dobré informovanosti zasahujících složek. Na území České republiky máme proto místa, kde je vedení ropovodu výrazně označené tabulkami, jde především o ropovod IKL, a místa kde je jeho přítomnost naopak zcela utajena [187].

Poslední oblastí je plánování, jde o sestavení plánu odezvy a jejich procvičování. Slabiny lze předpokládat především v nácviku odezvy na nouzovou situaci, kdy podobná událost nemá vysokou prioritu.

5.8. Výsledky studia rizik vodohospodářského systému a návrh ochranných opatření

Všechny formy života (tak, jak ho známe) závisí na vodě. Lidské tělo obsahuje 70 % vody, rostliny až 90 % vody. Z analýzy přírodních a lidských činností v historickém kontextu dále vyplývá, že: voda je základní podmínkou života; ve vodě vznikl život; voda je rozpouštědlo, ve kterém probíhají veškeré chemické děje v organismu; už ztráta 20 % tělesné vody je pro člověka smrtelná; na dehydrataci člověk umírá asi během 7 dnů; voda je nejdůležitější surovinou všech průmyslových odvětví, používá se k chlazení, ohřevu, oplachu, k výrobě elektrické energie, v potravinářství, k výrobě nápojů atd.; voda je základní podmínkou rostlinné a živočišné výroby; je zdrojem obživy v přímořských státech; vodní toky (řeky) a plochy (oceány, moře, jezera) hrají významnou roli v dopravě; přítomnost vodních ploch má vliv na klima krajiny; voda je využívána při hygieně, rekreaci a sportu; voda má léčivé účinky; a voda ve městech i krajině zlepšuje životní prostředí.

Nejvíce vody je v oceánech a mořích. Sladká voda tvoří jen nepatrnou část - 3 %, přičemž 69 % sladké vody je v ledovcích, které jsou v polárních oblastech, a dalších 30 % tvoří voda podzemní, tj. jen necelé procento tvoří voda povrchová na pevninách a voda atmosférická. Význam vody pro lidstvo podtrhlo vyhlášení „Evropské vodní charty“ dne 6. května 1968 ve Štrasburku, která shrnula základní skutečnosti a cíle pro nakládání s vodou:

1. Bez vody není života. Voda je drahocenná a pro člověka ničím nenahraditelná surovina.

2. Zásoby sladké vody nejsou nevyčerpatelné. Je proto nezbytné je udržovat, chránit a podle možnosti rozhojňovat.
3. Znečišťování vody způsobuje škody jak člověku, tak i ostatním živým organismům, závislým na vodě.
4. Jakost vody musí odpovídat požadavkům pro různé způsoby jejího využití, zejména musí odpovídat normám lidského zdraví.
5. Po vrácení použité vody do zdroje vody nesmí tato skutečnost zabránit dalšímu použití zdroje pro veřejné i soukromé účely.
6. Pro zachování vodních zdrojů má zásadní význam rostlinstvo, především les.
7. Vodní zdroje musí být zachovány.
8. Příslušné orgány musí plánovat účelné hospodaření s vodními zdroji.
9. Ochrana vody vyžaduje zintenzivnění vědeckého výzkumu, výchovu odborníků a informování veřejnosti.
10. Voda je společným majetkem, jehož hodnota musí být všemi uznávána. Povinností každého je užívat vodu účelně a ekonomicky.
11. Hospodaření s vodními zdroji se musí provádět v rámci přirozených povodí a ne v rámci politických a správních hranic.
12. Voda nezná hranic, jako společný zdroj vyžaduje mezinárodní ochranu.

Přestože výše bylo výše řečeno, že člověk bez vody dokáže žít jen krátce, tak od dob historických se člověk obává záplav a zvláště pak povodní. Zátopa je náhlé zvýšení průtoku vody a vzestup hladiny toku [6]. Dojde k překročení množství vody, které je tok schopný odvádět. Zátopy jsou jedním z přírodních živlů, které v případě dopadu na obydlenou oblast působí odedávna ztráty na lidských životech a velké škody na majetku a na životním prostředí. Povodeň označuje větší (ničivější) kategorii zátopy. Ke zvyšování průtoků vodních toků na území ČR dochází vlivem spadlých intenzivních (krátkodobých či dlouhodobých) dešťových srážek nebo táním sněhové pokrývky, popřípadě jejich kombinací. Podle uvedených příčin rozeznáváme povodeň dešťovou, sněhovou nebo smíšenou. Povodeň vzniklá v důsledku tvorby ledového nápichu nebo zácpy, se nazývá ledovou [6].

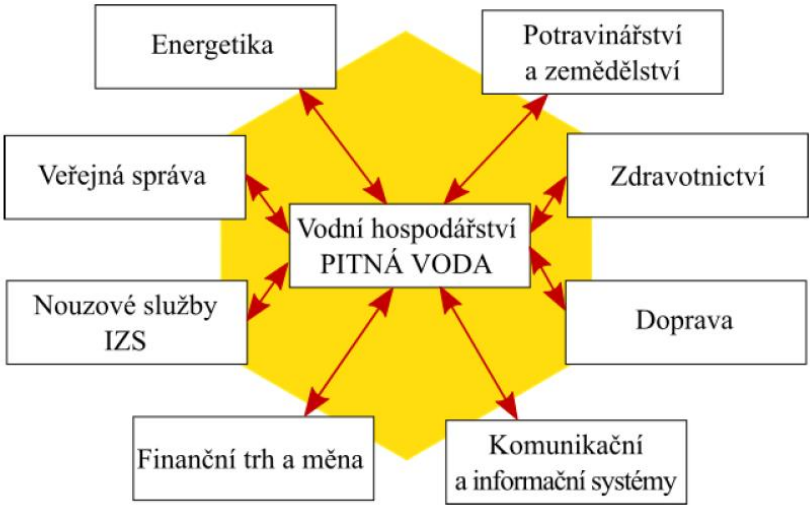
Každá povodeň vzniká jinak a v jiné době. Neklamným znakem povodní je skutečnost, že voda opouští svá koryta a rozlévá se po krajině (přitom se mluví o kulminaci vodní hladiny). Podle kulminační výšky vodní hladiny pak rozeznáváme dvacetileté, padesátileté, stoleté a jiné povodně. Při běžném územním plánování (zákon č. 183/2006 Sb.) se provádí ochrana objektů a infrastruktur proti stoletým povodním [6]. U důležitých objektů a infrastruktur je ochrana vyšší, např. u jaderných zařízení je ochrana proti desetitisíciletým povodním.

Bezpečnost vodohospodářského systému je velmi rozsáhlá problematika. Spolehlivost vodohospodářských děl je sledována v práci [189]. Důležitost systému zásobování vodou v rámci kritické infrastruktury ukazuje obrázek 32. Z obrázku vyplývá, že voda je potřebná ve všech důležitých systémech, které člověk potřebuje k životu. Další pozornost soustředíme především na dodávky pitné vody.

5.8.1. Topologie dodávek pitné vody

Systém zásobování pitnou vodou je systém systémů, tj. minimálně vzájemně propojených systémů: zdroje pitné vody; technologie úpravy vody; distribuční sítě. Vodovodní síť je tlakový trubní systém, při jehož hydraulické analýze se s výhodou využívá metod matematického modelování. Cílem hydraulické analýzy je získání potřebných informací o tlakových a průtokových poměrech v těchto sítích zejména pro potřeby provozování a řízení stávajících distribučních systémů, projektování nových trubních rozvodů a také pro potřebu jejich rekonstrukcí, případné rozšiřování a napojování nových odběratelů. Měření přímo na síti sice umožňuje získat informace o průtokových a tlakových poměrech přímo v místě měření, ale

k získání těchto údajů pro celou síť by bylo nutné osadit na síti velké množství měřicích zařízení. To je sice technicky proveditelné, ale ekonomicky velmi náročné.



Obr. 32. Interakce systému zásobování vodou s ostatními systémy kritické infrastruktury [65].

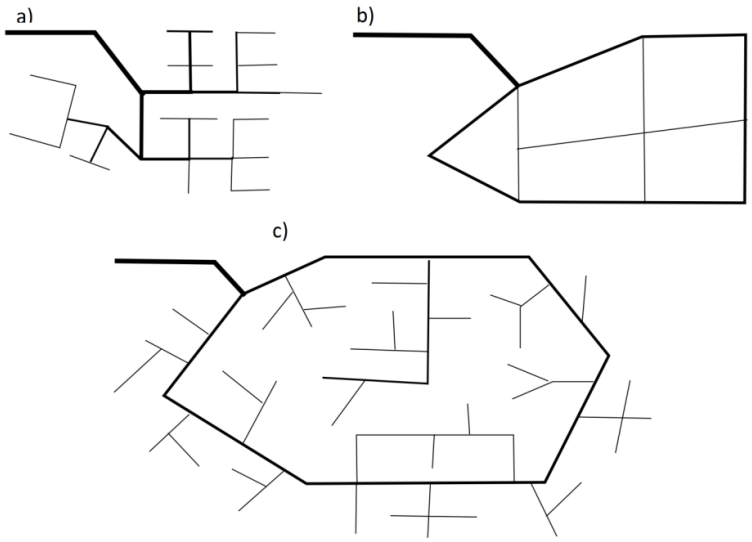
Zatímco charakter měkkých prvků a lidských zdrojů může být zcela odlišný pro různé firmy a různé regiony, pevná část infrastruktur má všude podobné základní aspekty. Máme zde zdroje, přenos a distribuci. Parametrů, které definují vlastnosti pevné části infrastruktury dodávek pitné vody je mnoho. My se zde zaměříme pouze na základní dva. První se nachází v oblasti zdrojů pitné vody. Druhý pak v oblasti transportu – topologie sítě.

Základní členění zdrojů pitné vody je na povrchové a podzemní, které lze dále členit podle dalších parametrů (plocha, hloubka, objem, kvalita). Oba dva typy zdrojů, podzemní i povrchové, mají své výhody i nevýhody, přičemž donedávna byly upřednostňovány ekonomické výhody podzemních zdrojů. Z pohledu analýzy rizik pak vypíchněme jednoduší úpravu podzemních vod. Zdroje podzemních vod mají menší pravděpodobnost kontaminace, i když kvůli nulové ochraně dochází občas ke kontaminaci menších zdrojů například vlivem dopravních nehod [190-192]. Čištění podzemních zdrojů není v současné době technologicky možné. Hlavní výhodou povrchových zdrojů je jejich obnovitelnost, která souvisí čistě jen se srážkami a není nijak závislá na poměru vsáknuté a odteklé vody.

Přenosová síť se vedle prvků, které zajišťují tlak vody v síti, skládá především z potrubí. Základním rysem distribuční sítě je její topologie, kde známe tři varianty, obrázek 33 [127,192,193].

Nejlevnější variantou na konstrukci je síť větvená, kde do většiny míst distribuce je voda dovedená jen jedním potrubím [175,192]. U větvené sítě je vysoká pravděpodobnost celkového kolapsu sítě i vlivem jednoduchých závad. Opakem k větvené síti je síť okruhová, která do všech bodů distribuce dodává vodu ze dvou směrů. Náklady na konstrukci okruhové sítě jsou vysoké, ale narušení byť jen části sítě vyžaduje souhru okolností a vyřazení celé sítě pak může být reálné, jen když je provedeno úmyslně. Jako nejlepším pro praxi se pak jeví řešení kombinované sítě, které při správném projektování a řízení přináší výhody obou sítí. Přiměřené náklady a vysoká odolnost na úrovni páteřní části sítě. Poměr kombinace obou přístupů pak záleží na stanovených cílech.

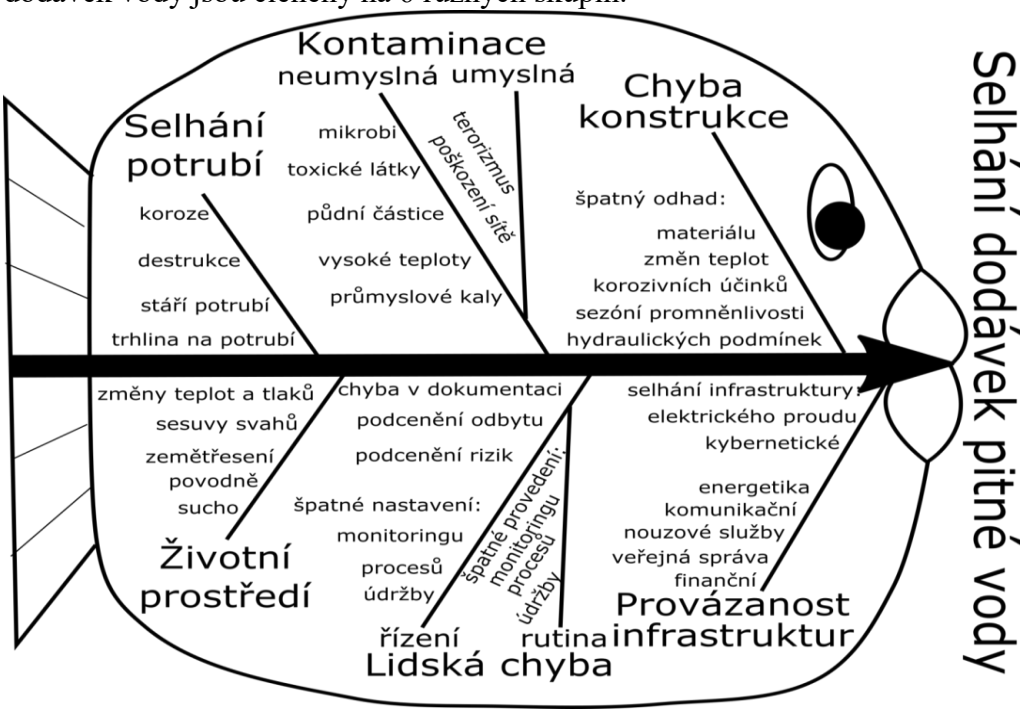
Kombinovaná síť je cílem distribuce pitné vody v České republice. Riziko kritického selhání se tak přesouvá jen do oblasti vodních zdrojů. Praxe je však závislá na financích, a proto zatím převládá síť větvená.



Obr. 33. Ukázky tří variant topologie sítí dodávek pitné vody: a) větvená, b) okruhová a c) kombinovaná [127,192,193].

5.8.2. Příčiny selhání dodávek pitné vody

Náchylnost infrastruktur k poškození je poměrně vysoká. Existuje mnoho příčin a procesů, které vedou k narušení sítě [10,11]. Některým příčinám, například živelním pohromám, nelze zabránit. Hlavním problémem mnoha zemí jsou ale příčiny, které jsou zcela v rukách veřejné správy a vlastníků vodovodní sítě, a to výstavba a údržba potrubí. Příčiny selhání dodávek vody můžeme členit různými způsoby. Podle prvků, které jsou narušeny, velikosti dopadů, oblasti vzniku pohromy, či její charakteristice. Příčiny, členěné podle posledních dvou vyjmenovaných položek, jsou na základě dat z [192] a za pomoci Išikavova diagramu [15] znázorněné na obrázku 34. Páteří rybí kosti na obrázku 34 je selhání dodávek pitné vody a příčiny selhání dodávek vody jsou členěny na 6 různých skupin.



Obr. 34. Išikavův diagram pro selhání dodávek pitné vody [127,192,193].

Chyba konstrukce je skupina příčin, které jsou způsobeny již při samotném návrhu nebo realizaci projektu konstrukce. Nekompetentní projektant, nebo snaha o co nevětší stlačení nákladů na výstavbu a konstrukci tak může vést ke vzniku velkého množství častých poruch, vysokým nákladům na opravy, nebo k nízké účinností plnění požadovaných služeb.

Okolní zemní prostředí působí na síť neustále roztahováním a smršťováním v závislosti na různých geomorfologických podmínkách. Pravděpodobnost narušení je pak dána konstrukcí, stářím materiálu a kvalitou údržby potrubí. Jiným problémem jsou živelní pohromy, které mohou dosahovat různých velikostí a působit škody na infrastruktuře. Proti menším pohromám je možné systém zodolňovat, kritické pohromy však infrastrukturu zcela jistě naruší ve velké míře a je nutné, mít v rámci krizového plánu připraveny různé dostatečně silné varianty náhradního zásobování [194]. Vlivům na životní prostředí nelze nijak předcházet.

Problémy spojené s provázaností infrastruktur již byly zmíněny vícekrát. Selhání infrastruktur, do kterých patří i infrastruktura zajišťující dodávky pitné vody, může vyvolat kritickou situaci, a proto je třeba mít dostatečně kvalitní krizový plán. Ochrana kritické infrastruktury je nezbytnou součástí moderního krizového řízení.

Lidská chyba má několik rozměrů. Patří sem chyby při projektování, či provádění konstrukce [5], které mají vlastní větev na obrázku 34. Na obrázku 34 tak jsou u lidských chyb uvedeny jenom příčiny způsobené při provozu sítě. Lidské chyby mohou nastat špatným řízením, například špatný odhad odběru vody. Zvýšení poptávky je nutné předvídat, protože budování nových zdrojů je časově náročné. Druhá oblast lidských chyb je způsobována nedodržením postupů a technických norem. Dojde-li při technických úkonech k problému, pak se jedná o chybu rutiny v případě, že nebyly dodrženy postupy. Pokud postupy dodrženy byly, pak jde o chybu řízení při nastavování postupů. V České republice je problém především s organizačními haváriemi [10], kdy v praxi řídící osoby neplní své odpovědnosti nebo odpovědnosti jsou nejasně stanovené.

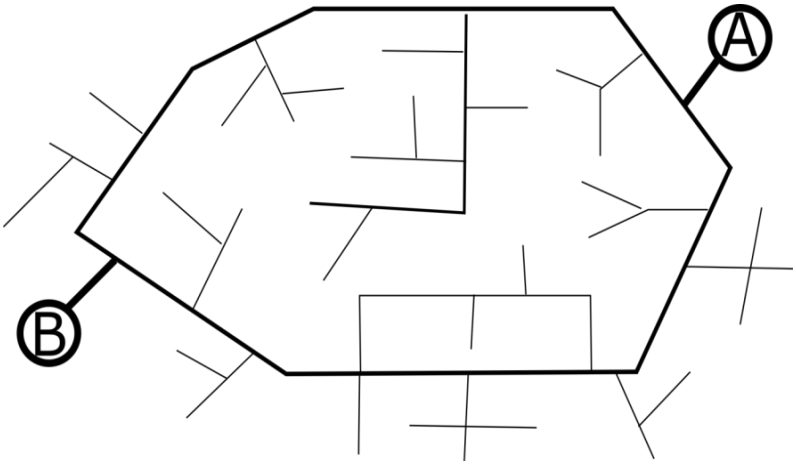
Selhání potrubí je nejběžnější příčina narušení dodávek pitné vody. Hlavními příčinami jsou nesprávná konstrukce, stáři a kvalita údržby. Pokud některý z uvedených tří faktorů selhává, dochází k narušení potrubí i vlivem běžných jevů.

Kontaminace může být rozdělena na úmyslnou a neúmyslnou. Vodní zdroje jsou jedním z možných cílů teroristických útoků, které mohou způsobit velké škody. V případě vysoce toxické látky může dojít i skrze malý zdroj k znečištění celé sítě. Důležitá je proto ochrana perimetru zdroje a především monitoring kvality vody dodávané do sítě [5,10]. Poměrně běžnou byly v posledních letech kontaminace neúmyslná. Sucho a vysoké teploty, špatná dokumentace, nehoda při přepravě nebezpečných látek, skladování nebezpečných látek a škodlivých věcí v blízkosti vodních zdrojů, což vše se během posledních let stalo v České republice [12,193]. Kontaminace vodního zdroje může vyvolat kritickou situaci i v případě odolné infrastruktury dodávek pitné vody.

5.8.3. Simulace dopadů selhání dodávek pitné vody

Pro sledování dopadů selhání pitné vody byly vybrány Střední Čechy. Použili jsme data o rozmístění zdrojů a o topologii distribuční sítě z prací [195,196]. Z bezpečnostních důvodů uvádíme jen model distribuční sítě, který jsme vytvořili na základě podrobných dat, obrázek 35. Z obrázku vyplývá, že jde o kombinovanou síť se dvěma vodními zdroji, která má ve vnitřní části sítě větvené. V sítí větvené se mohou realizovat všechny problémy sítě kombinované, plus ještě problémy navíc. Naše síť obsahuje dva zdroje, hlavním zdrojem je zdroj podzemní vody A - 80 %, zdroj B je povrchový a poskytuje 15 %. Zbytek je pokryt z menších zdrojů. Převaha podzemního zdroje odpovídá stavu, kdy použití podzemní vody vychází ekonomicky lépe než použití vody povrchové. Pod vlivem hydrologických změn a posledních such je ovšem tendence

dany stav změnit. Povrchové zdroje měly v době svého zakládání ambice zásobovat vodou větší podíl odběratelů [195,196].



Obr. 35. Kombinovaná síť dodávek pitné vody se dvěma hlavními vodními zdroji, A – podzemní 80 % a B – povrchová 15% [127,192,193].

Dopady kritického selhání dodávek pitné vody jsou místně specifické a závisí na scénáři, který vedl k selhání. Při všech kritických selháních jsou občané bez dodávky pitné vody. Při výzkumu dopadů kritického selhání dodávek pitné vody jsme použili metodu What, If modifikovanou pro potřeby řešení bezpečnostních problémů v integrálním a systémovém pojetí reality [10], a dva možné případy, a to velké narušení distribuční sítě a velká kontaminace zdroje vysoce nebezpečnou látkou.

Při kontaminaci vody nebezpečnou látkou je rozhodující nebezpečnost látky a velikost její koncentrace. Poškození zdraví, popřípadě ztráta života závisí právě na těchto veličinách [194]. V případě vysoce toxických látek tak může dojít k ohrožení života i při zředění v obrovském množství vody, a tudíž k nebezpečí pro všechny spotřebitele vody z kontaminované infrastruktury. Ve výsledku není vůbec zásadní, kde ke kontaminaci došlo, hlavní zdroj, vedlejší zdroje, vodojem, potrubí. Vedle přímé otravy uživatelů vody z kontaminované sítě je nutné vzít v potaz, že po odstavení infrastruktury může být velmi problematická dekontaminace celé sítě. Rozsáhlá síť tak nemusí v případě nedostatečné odezvy fungovat i několik dnů, což je z pohledu fyziologických potřeb člověka příliš dlouho [194].

Selhání dodávek pitné vody je jednou z možných kritických pohrom na území České republiky. Podle zákona č. 274/2001 Sb., o vodovodech a kanalizacích je sice již od 80. let minulého století zajištěno zásobování pitnou vodou pomocí balené vody i při nouzových situacích; ale to nelze dlouhodobě. Selhání kritické infrastruktury, kde selhání dodávek pitné vody má velkou kritičnost, ohrožuje vždy řadu dalších chráněných aktiv. Možností vedoucích k selhání dodávek pitné vody je celá řada a mají různě závažné dopady a také jejich výskyt je různě pravděpodobný.

Dále uvedeme simulace dopadů pro dvě odlišné příčiny, v obou případech spojených se zdroji pitné vody. Zdroje pitné vody jsou klíčové součásti infrastruktury, ale při špatné topologii sítě může být kritických míst podstatně více. První scénář se zabývá havárií potrubí, které zajišťuje distribuci vody. Havárie potrubí je poměrně běžný jev, který může být způsoben řadou příčin. Druhý scénář se zabývá kontaminací vodního zdroje.

Větší zdroje vody jsou vždycky kritickou součástí infrastruktury dodávek pitné vody. V případě větvené sítě je kritičnost hlavního řadu vysoká [192], ovšem u kombinované znatelně klesá. Na obrázku 35, v naší síti, máme ale pouze jednu spojnici mezi hlavním zdrojem A (80 %) a celým zbytkem sítě. Pokud v reálu není přípojek více, jsou přípojky stejně kritické, jako zdroje samotné. V prvním scénáři jsme předpokládali vyřazení právě takové přípojky. Je nutné

si uvědomit, že pro správné fungování sítě je nutný určitý tlak, dodávaná voda nesmí klesnout pod určité množství. Při výpadku vstupu o 80 %, bez zavedení tvrdé regulace na výstupu tak tlak velmi rychle poklesne a voda nebude dostupná, i když nebudou vyřazeny všechny zdroje [195]. Dopady selhání jsou v tabulce 12.

Tabulka 12. Dopady velkého narušení dodávek pitné vody v případě poškození vodohospodářské infrastruktury; 0 – čas vzniku přerušení, 12h po 12 hodinách od počátku přerušení, 24h – po 24 hodinách od přerušení, 3 dny a 7 dní po přerušení [192,193].

Veřejná aktiva	**Dopady**
Životy a zdraví lidí	0h: 12h: lehká dehydratace osob závislých na dodávkách pitné vody z vodovodní sítě (ti, kteří nemají přístup k vodě balené), znamenající poškození zdraví a životů osob s vyšší zranitelností vůči nedostatku pitné vody, tedy zvláště osob dlouhodobě nemocných, pacientů v nemocnicích, osob staršího věku a dětí. 24h: dehydratace všech osob závislých na dodávkách pitné vody z vodovodní sítě (ti, kteří nemají přístup k vodě balené). Nedostatek vody se projeví bolestmi hlavy a snížením tlaku. 3 dny: prohlubující se dehydratace. U osob se zvýšenou citlivostí na nedostatek tekutin se začíná vyskytovat úmrtí. Většina obyvatel pociťuje zesilující příznaky dehydratace, jako je bolest hlavy, tlak, zvýšení tepové frekvence a další fyziologické projevy. Dehydratace se již dotýká osob, které byly předzásobeny vodou balenou. U všech obyvatel postižené oblasti se začíná projevovat stres z nouzové situace a zhoršuje se taktéž duševní stav. Zhoršující se úroveň hygieny. 7 dní: závažná dehydratace způsobující smrt obyvatel.
Bezpečí lidí	0h: 12h: 24h: nárůst napětí ve společnosti. 3 dny: v důsledku poklesu kvality nouzových služeb dochází ke zvýšení možnosti vzniku dalších pohrom. 7 dní: vymizení veškerých vnitřních bezpečnostních prvků, a tím se možnost vzniku dalších pohrom výrazně zvýší.
Majetek	0h: 12h: poškození majetku požárem. 24h: narušení funkčnosti strojů a zařízení závislých na dodávce vody. Poškození majetku požárem. 3 dny: vznik nepokojů uvnitř společnosti, vedoucí k rabování a ničení majetku. Poškození majetku požárem, jehož pravděpodobnost se vlivem rozkladu společnosti zvyšuje. 7 dní: poškození majetku dlouhotrvajícími požáry.
Veřejné blaho	0h: 12h: přerušení pracovních činností v soukromé a veřejné sféře. Nucená dovolená z důvodu nesplnění požadavků na dodržení zákoníku práce. Nedostupnost restauračních a kulturních zařízení. 24h: 3 dny: zhoršení stavu společnosti. Negativní vliv na budoucí vnímání daného území.

	7 dní: v důsledku rozpadu společnosti vlivem psychického a fyzického stavu obyvatel ztrácí pojem veřejné blaho svůj význam.
Životní prostředí	0h: 12h: 24h: 3 dny: vlivem nepokojů a narušením nouzových služeb se zvyšuje nebezpečí vzniku pohrom působící na životní prostředí, např. požáry. 7 dní: nárůst dopadů neřešených pohrom na životní prostředí.
Systém dodávky vody	0h: výrazné zhoršení funkčnosti infrastruktury dodávek pitné vody. 12h: vyčerpání zásobních systémů sítě, vodojemů. 24h: 3 dny: nefunkčnost všech systémů v rámci infrastruktury dodávky pitné vody. 7 dní: degradace mechanických částí systému dodávky pitné vody (prvky systému nejsou ve stavu, na které byly projektovány).
Nouzové služby (policie, hasiči, zdravotníci)	0h: náhlý pokles tlaku ve vodovodním řadu, výpadek některých zdrojů vody určených pro hašení požárů. 12h: zhoršení stavu pacientů v hospitalizačních zařízeních. Zhoršená dostupnost zdravotní záchranné služby z důvodu převozu pacientů mimo postiženou oblast. 24h: 3 dny: pokles fyzických možností pracovníků nouzových služeb způsobených dehydratací. Postupné napadání zaměstnanců nouzových služeb v důsledku zhoršujícího se stavu společnosti. 7 dní: nefunkčnost vnitřních složek infrastruktury.
Přepravní síť	0h: 12h: 24h: možný vznik kolon následkem začínající migrace obyvatel mimo postiženou oblast. 3 dny: vznik kolon na silniční síti v důsledku evakuace obyvatel. Výpadek vnitřních prvků území železniční sítě. Narušení liniových prvků dopravní infrastruktury důsledkem sociálních nepokojů. 7 dní: nefunkčnost veškerých prvků dopravy spojených s lidskou činností. Poškození mechanických prvků dopravní infrastruktury důsledkem sekundárních pohrom, např. dopravní nehody, požáry, nepokoje apod.
Ostatní základní služby a kritické infrastruktury (informační, finanční, energetická, sociální, státní)	0h: 12h: nedostupnost základních služeb, např. vzdělávacích zařízení, státních a finančních služeb. 24h: úbytek balených tekutin v obchodech a distribučních centrech. 3 dny: nefunkčnost vnitřních prvků infrastruktur základních a kritických služeb. 7 dní: nefunkčnost vnitřních prvků infrastruktur základních a kritických služeb.

Druhý případ, tj. kontaminace se týká menšího ze zdrojů na obrázku 35, tj. povrchového zdroje B (15 %). Dopady jsou v tabulce 13. Kontaminace vodního zdroje patří do jednoho ze scénářů teroristických útoků. Ke kontaminaci ale může dojít i jinými způsoby, nehoda při přepravě nebezpečných látek, nebo špatné nakládání s nebezpečnými látkami například při skladování. Oba jevy se v České republice již vyskytovaly, naštěstí bez kritických následků.

Tabulka 13. Dopady velkého narušení dodávek pitné vody v případě kontaminace středně velkého zdroje silně toxickou látkou; 0 – čas kontaminace, 12h - po 12 hodinách vzniku kontaminace, 24h – po 24 hodinách od vzniku kontaminace, 3 dny a 7 dní po přerušení [192,193].

Veřejná aktiva	**Dopady**
Životy a zdraví lidí	0h: první osoby požívají kontaminovanou vodu, která startuje nežádoucí procesy v lidském těle. 12h: těžké poškození zdraví, které závisí na charakteru použité chemické látky, první oběti na životech. 24h: oběti na životech dosahují katastrofálního množství. Vznik společenského napětí. 3 dny: stres a zhoršení duševního stavu přeživších jak v zasažené oblasti, tak i v rozsáhlém okolí. Nedůvěra v centrální zdroje pitné vody, která může vyvolat paniku, či sociální nepokoje. Dehydratace způsobující bolesti hlavy a snížení krevního tlaku. 7 dní: U všech obyvatel se začíná projevovat stres z nouzové situace a zhoršuje se taktéž duševní stav. Zhoršující se úroveň hygieny. Dehydratace způsobující již závažné zdravotní komplikace.
Bezpečí lidí	0h: otravy kontaminovanou vodou v blízkém okolí. 12h: otravy kontaminovanou vodou v celé zásobované oblasti. 24h: nárůst napětí ve společnosti. 3 dny: 7 dní: pokles kvality nouzových služeb může vést k vzniku dalších pohrom.
Majetek	0h: kontaminace majetku, jehož funkce je spojena s přísunem vody v blízkém okolí, např. zařízení domácností, zařízení pracovišť, stroje. 12h: : kontaminace majetku, jehož funkce je spojena s přísunem vody v zásobené oblasti, např. zařízení domácností, zařízení pracovišť, stroje. 24h: 3 dny: Nedostatek vody pro hašení požárů v důsledku odpojení dodávek vody. 7 dní: nebezpečí vzniku nepokojů uvnitř společnosti, které vedou k rabování a ničení majetku. Poškození majetku požárem, jehož pravděpodobnost se vlivem rozkladu společnosti zvyšuje.
Veřejné blaho	0h: 12h: přerušení pracovních činností v soukromé a veřejné sféře v důsledku úmrtí. 24h: zhoršení stavu společnosti, panika vyvolaná počtem obětí. Negativní vliv na budoucí vnímání daného území. 3 dny: 7 dní: k obavám z otravy nebezpečnou látkou přibývá strach z dlouhodobého přerušení dodávky pitné vody.
Životní prostředí	0h: kontaminace vodní nádrže Klíčava, dolní toku potoku Klíčava, řeky Berounka. 12h: kontaminace dalších vodních toků (v povodí řek Vltava a Labe), kontaminace břehů. Úmrtí vodní fauny a možné odumření vodní flóry. 24h: Úmrtí živočichů využívající povrchové zdroje vody v zasažené oblasti.

	3 dny: 7 dní:
Dodávky vody	0h: kontaminace zdroje pitné vody nádrže Klíčava, kontaminace přilehlé sítě dodávky pitné vody. 12 h: kontaminace celého okruhu systému dodávky pitné vody. 24h: vypnutí postiženého systému dodávek pitné vody. 3 dny: 7 dní: degradace mechanických částí systému dodávky pitné vody (prvky systému nejsou ve stavu, pro který byly projektovány).
Nouzové služby (policie, hasiči, zdravotníci)	0h: 12h: extrémní zatížení zdravotní péče osobami se symptomy otravy a umírajícími, např. nemocnice a zdravotní záchranná služba. Zvyšování nároků na udržení veřejného pořádku. Zasažení lidských zdrojů nouzových služeb. 24h: výpadek některých zdrojů vody pro hašení požárů. 3 dny: 7 dní: pokles fyzických možností pracovníků nouzových služeb způsobených dehydratací.
Přepravní síť	0h: 12h: 24h: rozsáhlou paniku vyvolává vznik kolon na silniční síti v důsledku hromadné evakuace obyvatel z postižené oblasti. Výpadek vnitřních prvků území železniční sítě. Narušení liniových prvků dopravní infrastruktury důsledkem sociálních nepokojů. 3 dny, 7 dní
Ostatní základní služby a kritická infrastruktura (informační, finanční, energetická, sociální, státní)	0h: 12h: nedostupnost základních služeb, např. vzdělávacích zařízení, státních a finančních služeb. 24h: úbytek balených tekutin v obchodech a distribučních centrech. 3 dny: 7 dní: nefunkčnost vnitřních prvků infrastruktur základních a kritických služeb.

Když srovnáme dopady obou scénářů, tak vidíme rozdíly především v prvních hodinách, kde dopady kontaminace mají rychlejší náběh. Po překročení jednoho dne se však dopady obou scénářů začínají přibližovat. Předcházení fatálním dopadům v prvních hodinách kontaminace vyžaduje vysoce kvalitní monitoring (používají se ryby v akváriích nebo kontinuální měření fyzikálních parametrů), monitoring ovšem musí být prováděn ve všech kritických místech [19].

V případě obou scénářů se pak situace ostře mění po překročení jednoho dne. Zvládnutí situace do 24 hodin je spojeno s relativně malými dopady na chráněná aktiva. Překročení jednoho dne však vede již ke kritické situaci. Další hranice 5 - 7 dnů je pak dána především dobou, po kterou je zdravý člověk schopen vydržet bez vody [194,195].

Provedená analýza reálných výpadků dodávek pitné vody v posledních letech v České republice [12] odhalila dva základní problémy se zvládnutím situace. První je problematika s odpovědností [191]. Řada vysokých pracovníků veřejné administrativy nezná nebo si nepřipouští všechny odpovědností spojené s jejich pozicí v úřadu (např. odpovědnost starosty podle zákona č. 128/2000 Sb., o obcích). Uvedený fakt často vede k prodlevě v odezvě samotné, což je fatální především v případě kontaminace. Druhým problémem je robustnost odezvy na selhání dodávek pitné vody. Jak bylo zmíněno výše, selhání infrastruktury dodávek pitné vody je identifikováno jako jedna z možných pohrom, které mohou vyvolat krizový stav, a proto je pro ni zpracován typový plán [194].

Na základě analýzy skutečných událostí v České republice v posledních letech [192] některé činnosti odezvy například, informování obyvatel, varování obyvatel, nouzové zásobování, rychlá obnova sítě, nejsou dostatečně robustní. Řada územních celků je schopna uvedené nároky splňovat v případě malých lokálních havárií vodovodního řadu. Na kritické selháni však plány odezvy sestaveny nejsou.

Dnešní moderní koncept „smart cities“ musí vzít v úvahu výše uvedená fakta a musí mít připraveny plány na kvalitní a rychlé zvládnutí selhání životodárných infrastruktur, do nichž bezesporu patří infrastruktura dodávek pitné vody.

5.8.4. Péče o vodní systém v ČR

Péče o vodní systém zahrnuje ochranu vodních toků i další vody z komplexního pohledu. Jde o kvalitu i kvantitu vody, její disponibilitu i o ochranu chráněných zájmů před povodněmi. Zákon č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon) v platném znění se zabývá ochranou povrchových a podzemních vod a stanovuje podmínky pro hospodárné využívání vodních zdrojů. Předmětný zákon též zajišťuje zvládnutí povodní i havárií na vodních tocích.

Dle jmenovaného zákona je plánování v oblasti vod soustavná koncepční činnost, kterou zajišťuje stát. Zákon upravuje postupy pro případ havárie na vodních tocích a dílech i příslušné havarijní plány. Specifikuje povodňové orgány, povodňové plány i ochranu před povodněmi. Účelem zákona je chránit povrchové a podzemní vody, stanovit podmínky pro hospodárné využívání vodních zdrojů a pro zachování i zlepšení jakosti povrchových a podzemních vod, vytvořit podmínky pro snižování nepříznivých dopadů povodní a sucha a zajistit bezpečnost vodních děl.

Zákon upravuje právní vztahy k povrchovým a podzemním vodám, vztahy fyzických a právnických osob k využívání povrchových a podzemních vod, jakož i vztahy k pozemkům a stavbám, s nimiž výskyt těchto vod přímo souvisí, a to v zájmu zajištění trvale udržitelného užívání těchto vod, bezpečnosti vodních děl a ochrany před dopady povodní a sucha. Upravuje státní správu, dohled, sankce, pokuty a jiné prostředky pro vynucení opatření ve veřejném zájmu.

Plánování v oblasti vod je tvořeno Plánem hlavních povodí České republiky a plány oblastí povodí, včetně programů opatření. Účelem plánování v oblasti vod je vymezit a vzájemně harmonizovat veřejné zájmy, kterými jsou: ochrana vod jako složky životního prostředí; ochrana před povodněmi a dalšími škodlivými účinky vod; trvale udržitelné užívání vodních zdrojů a hospodaření s vodami pro zajištění požadavků na vodohospodářské služby, zejména pro účely zásobování pitnou vodou.

Havárií je mimořádné závažné zhoršení nebo mimořádné závažné ohrožení jakosti povrchových nebo podzemních vod. Za havárii se vždy považují případy závažného zhoršení nebo mimořádného ohrožení jakosti povrchových nebo podzemních vod ropnými látkami, zvlášť nebezpečnými látkami, popřípadě radioaktivními zářiči a radioaktivními odpady, nebo dojde-li ke zhoršení nebo ohrožení jakosti povrchových nebo podzemních vod v chráněných oblastech přirozené akumulace vod nebo v ochranných pásmech vodních zdrojů. Za havárii se též považují případy technických poruch a závad zařízení k zachycování, skladování, dopravě a odkládání nebezpečných látek, pokud takovému vniknutí předcházejí.

Zátopová území pro potřeby ochrany před povodněmi lze získat empiricky, expertním odhadem nebo použitím vhodných modelů. Jedním z velmi používaných modelů pro simulování povodně je procesní model s podpůrným software MIKE 11 [6,12].

Povodňovými plány pro účely zákona č. 254/2001 Sb. jsou dokumenty, které obsahují: způsob zajištění včasných a spolehlivých informací o vývoji povodně; možnosti ovlivnění odtokového režimu, organizaci a přípravu zabezpečovacích prací; způsob zajištění včasné

aktivizace povodňových orgánů; zabezpečení hlásné a hlídkové služby a ochrany objektů; přípravy a organizace záchranných prací a zajištění povodní narušených základních funkcí v objektech a v území a stanovené směrodatné limity stupňů povodňové aktivity. Jejich obsah se dělí: věcnou část; organizační část; a grafickou část. Pojišťovny a veřejná správa rozdělují v ČR zátopová území do 4 kategorií [6].

Havarijní plány pro účely zákona č. 254/2001 Sb. jsou dokumenty, které obsahují opatření a činnosti odezvy při kontaminaci vodního toku nebo zdroje. Vodní zákon obsahuje organizační a technická opatření pro řízení bezpečnosti vodního systému, povinnosti mají všichni zúčastnění.

Na základě komplexních analýz, hodnocení a syntéz provedených v práci [6] preventivní opatření, která vedou k zodolnění proti povodním a záplavám jsou:

1. Při územním plánování, umísťování, projektování, výstavbě a provozování objektů a infrastruktur zohledňovat nebezpečí kontaminace vod a nebezpečí povodní a zapracovávat příslušné normy a standardy, a to i s ohledem na jejich kritičnost v území.
2. U technologických objektů a infrastruktur považovat při vypracovávání bezpečnostních zpráv nebo jiných dokumentů kontaminaci vod a povodně jako zdroje technologických havárií a z tohoto pohledu provést příslušná opatření technická, právní (provozní předpisy) nebo organizační (nouzové pokyny a plány).
3. V zaplavovaném území povolit jen stavbu budov odolávajících záplavám, které výrazně nezdeformují hydrologické poměry tak, že dojde k ohrožení kritického majetku v okolním území.
4. Stavba protipovodňových hrází, vyvýšenin s objekty, retenčních nádrží a odvodňovacích kanálů opět s ohledem na kritický majetek v území.
5. Údržba koryt vodních toků a děl (např. pravidelné odstraňování bahna). 6. Monitorování průtoku a kvality vody ve vodních tocích.
6. Zpracování a implementace opatření povodňového plánu, který zohledňuje místní specifika a místní kritičnost území.
7. Výcvik zásahových jednotek, organizací i občanů v provádění krátkodobých ochranných opatření v případě bezprostředního nebezpečí.
8. Provozování hlásné protipovodňové služby.
9. Sledování a vyhodnocování meteorologických informací.
10. Vyčištění prostorů mezi povodňovými valy a korytem řeky.
11. Údržba a opravy povodňových valů a hrází.
12. Vytvoření a procvičení systému humanitární pomoci.
13. Vytvoření a procvičení evakuačních plánů.
14. Zpracování dokumentace (pasportizace) objektů pro dočasné ubytování obyvatelstva.
15. Příprava složek IZS a dalších sil a prostředků pro záchranu osob, hospodářských zvířat a majetku.
16. Zpracování a aktualizace povodňových plánů všech stupňů.
17. Vytvoření a procvičení systému varování obyvatelstva.
18. Zpracování systému zapojení všech zúčastněných do prevence, odezvy a obnovy s ohledem na kontaminaci vod a povodně.

Ze stejného zdroje jsou i dále uvedená opatření nutná pro zvládnutí dopadů povodně a obnovu objektů a území:

1. Pomoc postiženým lidem, zabránění domino efektům (a jimi způsobeným škodám) a volba vhodného technického zásahu na snížení ztrát na chráněných zájmech v území.
2. Odčerpat vodu z objektů, jakmile to okolní podmínky dovolí a provést vysušení s ohledem na fyzikální vlastnosti materiálu.
3. Odstranit bahno z komunikací a lidských obydlí.
4. Dekontaminovat zdroje pitné vody.

5. Vyčistit retenční nádrže, kanály, jezy atd.
6. Monitorovat nákazové situace a uplatnit preventivní hygienická opatření.
7. Osazovat břehy řek vhodnou vegetací.
8. Opravovat poškozené objekty.
9. Průběžně analyzovat povodňové situace.
10. Upravovat (aktualizovat) protipovodňová opatření.

V případě, že zdrojem povodně je vodní dílo, jde o tzv. Zvláštní povodeň a pro její zvládnutí se vypracovávají zvláštní povodňové plány [194].

5.8.5. Podklady pro správné řízení dodávek vody

Zajištění pitné vody pro lidi a zvířata a užitkové vody pro hygienu, průmysl a další závisí jednak na vodních zdrojích a jejich kvalitě, a jednak na distribuční síti vody. Vodní zdroje jsou podzemní a povrchové. Vzhledem k existenci povodní a období sucha, je nutné vodohospodářské systémy správně řídit, a to i dlouhodobě. Řízení musí brát v úvahu i neurčitosti v chování přírodního hydrologického systému.

Vodohospodářský systém se skládá e čtyř navazujících systémů, a to: systém dodávky surové vody; systém úpravy surové vody; distribuční systém upravené vody; a systém čištění odpadních vod.

Systém dodávky surové vody určené pro úpravu a konzumaci a jiné použití zahrnuje: vodní nádrže, přehrady a studně se zásobou surové vody; vodní potrubí; a čerpací stanice.

Systém úpravy surové vody na pitnou nebo užitkovou zahrnuje: mechanické čištění; filtrace; biologické čištění; a chemickou úpravu.

Distribuční systém upravené vody zahrnuje: čerpací stanice; potrubní síť upravené vody; nádrže; a tlakové rezervoáry.

Systém čištění odpadních vod zahrnuje: kanalizační síť; a čisticí stanice odpadních vod.

Cílem systému dodávky pitné vody a čištění odpadních vod je zásobovat lidská sídliště nebo průmyslové objekty pitnou, užitkovou nebo technologickou vodou a vyčistit odpadní vody od škodlivých látek na úroveň danou platnými normami. Podle účelu použití vody jsou navrženy parametry jednotlivých částí celého systému, tj. výkon, stupeň úpravy surové vody a způsob čištění odpadní vody. Systém úpravy surové vody je obvykle centralizován a umístěn ve vodárně, kde jsou většinou instalována rovněž dopravní čerpadla. Kritická aktiva vodohospodářského systému dle [65] jsou uvedena v tabulce 14.

Tabulka 14. Kritická aktiva systému dodávky vody a kanalizace – zpracováno dle údajů v [65].

Liniové stavby	Objekty	Zařízení	Materiály	Personál
potrubí surové vody potrubní síť upravené vody prvního a dalšího řádu kanalizační stoky a kanály	přehradní hráze vodní nádrže studně čerpací stanice úpravny vody čistírny odpadních vod	čerpadla armatury provozní budovy speciální zařízení přehradních nádrží	chemické sloučeniny používané pro úpravu vody	Zaměstnanci návštěvníci

Míry kritičnosti stanovené expertně podle multikriteriálního hodnocení popsaného v odstavci 4.2 (metoda SK1 a dohoda 2 expertů) jsou v tabulkách:

- pro potrubí surové a upravené vody – tabulka 15 – zpracováno dle údajů v [65],
- pro kanalizační stoky a kanály – tabulka 16 – zpracováno dle údajů v [65],
- přehradní hráze a vodní nádrže – tabulka 17 – zpracováno dle údajů v [65],
- studně – tabulka 18 – zpracováno dle údajů v [65],
- čerpací stanice – tabulka 19 – zpracováno dle údajů v [65],
- úpravny vody – tabulka 20 – zpracováno dle údajů v [65],
- čistírny odpadních vod – tabulka 21 – zpracováno dle údajů v [65],
- armatury – tabulka 22 – zpracováno dle údajů v [65],
- provozní budovy – tabulka 23 – zpracováno dle údajů v [65],
- speciální zařízení přehradních nádrží (výpustě, ovládací zařízení) – tabulka 24 – zpracováno dle údajů v [65],
- chemické sloučeniny pro úpravnu vody – tabulka 25 – zpracováno dle údajů v [65].

Celkové vyhodnocení kritičnosti je v tabulce 26; míra kritičnosti je vyjádřena vztahem

$$K = \sum_{i=1}^{14} k_i \; / 70,$$

ve kterém k_i jsou hodnoty od expertů, kteří použili stupnici 1 až 5 a dělení 70 znamená normování výsledné míry kritičnosti do intervalu 0 až 1.

Tabulka 15. Míra kritičnosti pro potrubí surové a upravené vody; zpracováno dle údajů v [65].

Kritérium	Míra	Komentář
1	5	Malá schopnost ochrany; nelze v celém rozsahu chránit
2	4	Velká možnost poškození; poškození potrubí nevyžaduje zvláštní technologii, ani příliš času, zejména, není-li hluboko pod zemí
3	4	Je možnost zamoření toxickými látkami
4	1	Malá
5	3	Podle velikosti potrubí
6	3	Podle velikosti potrubí, relativně velká
7	2	Případ od případu
8	1	Ne
9	1	Ne
10	2	Obvykle ano
11	1	Ne
12	1	Malý
13	4	Případ od případu
14	1	Malá

Tabulka 16. Míra kritičnosti pro kanalizační stoky a kanály; zpracováno dle údajů v [65].

Kritérium	Míra	Komentář
1	5	Malá schopnost ochrany; nelze v celém rozsahu chránit
2	4	Poškození kanalizace nevyžaduje zvláštní technologii, ani příliš času
3	4	V případě umístění výbušnin ano
4	1	Malý

5	3	Podle velikosti
6	3	Podle velikosti, relativně malá
7	1	Ne
8	1	Ne
9	1	Ne
10	2	Obvykle ano
11	1	Ne
12	1	Malý
13	2	Případ od případu
14	1	Malá

Tabulka 17. Míra kritičnosti pro přehradní hráze a vodní nádrže; zpracováno dle údajů v [65].

Kritérium	**Míra**	**Komentář**
1	5	Malá, nelze v celém rozsahu chránit
2	4	Poškození vyžaduje zvláštní technologii a příliš času
3	5	V případě protržení hráze
4	2	Malý
5	5	Podle velikosti
6	5	Podle velikosti
7	1	Ne
8	1	Ne
9	1	Ne
10	4	Obvykle ne
11	2	V některých případech
12	3	V případě zabudované elektrárny, malý
13	2	Případ od případu
14	1	Malá

Tabulka 18. Míra kritičnosti pro studně; zpracováno dle údajů v [65].

Kritérium	**Míra**	**Komentář**
1	5	Malá, nelze v celém rozsahu chránit
2	4	Ano
3	5	V případě otrávení vody
4	1	Malý
5	2	Malá
6	2	Malá
7	1	Ne
8	1	Ne
9	1	Ne
10	2	Obvykle ano
11	1	Ne
12	1	Ne
13	3	Případ od případu
14	1	Malá

Tabulka 19. Míra kritičnosti pro čerpací stanice; zpracováno dle údajů v [65].

Kritérium	Míra	Komentář
1	3	Ano
2	4	Ano
3	2	Ne
4	1	Malý
5	3	Malá
6	2	Malá
7	1	Ne
8	1	Ne
9	1	Ne
10	2	Obvykle ano
11	1	Ne
12	1	Ne
13	2	Případ od případu
14	1	Malá

Tabulka 20. Míra kritičnosti pro úpravny vody; zpracováno dle údajů v [65].

Kritérium	Míra	Komentář
1	4	Malá
2	5	Velká, možnost otrávení vody
3	5	Ano
4	3	Malý
5	3	Malá
6	3	Malá
7	3	Ano
8	1	Ne
9	1	Ne
10	3	Obvykle ano
11	1	Ne
12	1	Ne
13	5	Případ od případu
14	1	Malá

Tabulka 21. Míra kritičnosti pro čistírny odpadních vod; zpracováno dle údajů v [65].

Kritérium	Míra	Komentář
1	3	Malá
2	2	Malá
3	1	Ne
4	3	Malý
5	3	Malá
6	3	Malá
7	1	Ne
8	1	Ne
9	1	Ne

10	3	Obvykle ne
11	1	Ne
12	1	Ne
13	2	Případ od případu
14	1	Malá

Tabulka 22. Míra kritičnosti pro armatury; zpracováno dle údajů v [65].

Kritérium	**Míra**	**Komentář**
1	3	Malá
2	2	Malá
3	1	Ne
4	1	Malý
5	1	Malá
6	1	Malá
7	1	Ne
8	1	Ne
9	1	Ne
10	2	Obvykle ne
11	1	Ne
12	1	Ne
13	2	Případ od případu
14	1	Malá

Tabulka 23. Míra kritičnosti pro provozní budov; zpracováno dle údajů v [65].

Kritérium	**Míra**	**Komentář**
1	3	Malá
2	2	Malá
3	2	Ne
4	1	Malý
5	3	Malá
6	3	Malá
7	1	Ne
8	1	Ne
9	1	Ne
10	3	Ne
11	1	Ne
12	1	Ne
13	3	Případ od případu
14	1	Malá

Tabulka 24. Míra kritičnosti pro speciální zařízení přehradních nádrží (výpustě, ovládací zařízení); zpracováno dle údajů v [65].

Kritérium	**Míra**	**Komentář**
1	4	Malá
2	4	Velká

3	4	Ano
4	1	Malý
5	3	Malá
6	3	Malá
7	1	Ne
8	1	Ne
9	1	Ne
10	4	Obvykle ne
11	1	Ne
12	1	Ne
13	4	Případ od případu
14	1	Malá

Tabulka 25. Míra kritičnosti pro chemické sloučeniny pro úpravu vody; zpracováno dle údajů v [65].

Kritérium	**Míra**	**Komentář**
1	4	Malá
2	5	Ano
3	5	Ano
4	3	Malý
5	1	Malá
6	1	Malá
7	1	Ne
8	1	Ne
9	1	Ne
10	2	Obvykle ano
11	1	Ne
12	1	Ne
13	2	Případ od případu
14	1	Malá

Množství aktiv i příčiny havárií vodovodních řadů [12] ukazují, že příčin selhání vodohospodářského systému je mnoho. Nejčastější příčiny jsou: technologická vada způsobená buď konstrukční chybou anebo stářím; nesprávný způsob provozu; nedodržení technologické kázně; živelní pohromy nebo havárie jiných systémů, např. povodně, zemětřesení, orkány apod.; úmyslné jevy, např. teroristický útok. Z kritického vyhodnocení tabulek 15 – 26 vyplývá:

- nejkritičtější částí systému dodávky vody jsou přehrady a vodní nádrže. Teroristický útok na velké přehradní hráze je však technicky velmi náročný, jak ukázaly podobné útoky za druhé světové války a vyžaduje speciální technologii a postup, který bude záviset na tom, zda hráz je gravitační, skořepinová nebo sypaná. Reálné nebezpečí však představuje přirozené narušení hráze při velkých povodních, zejména při povodních na zamrzlém toku. V uvedených případech může narušení hráze způsobit pohromy s dopady velkého rozsahu i v případě menších vodních nádrží,
- na druhém místě co do kritičnosti jsou úpravny vody. V tomto případě je kritičnost dána především možností teroristického útoku dávkováním toxických látek (chemických nebo biologických škodlivých látek) do pitné vody. V případě, že by se nepodařilo takovému

útoku zabránit, nastává nebezpečí intoxikace relativně velkého počtu obyvatel v sídlištích. I když by však mortalita takového útoku byla malá, je jeho psychologický efekt značný,

Tabulka 26. Celkové vyhodnocení kritičnosti aktiv (kritických míst) vodohospodářského systému.

Aktivum	**Kritérium**														**Míra kritičnosti**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	
Přehradní hráze a vodní nádrže	5	4	5	2	5	5	1	1	1	4	2	3	2	1	0.59
Úpravny vody	4	5	5	3	3	3	3	1	1	3	1	1	5	1	0.56
Speciální zařízení přehrad	4	4	4	1	3	3	1	1	1	4	1	1	4	1	0.47
Potrubí surové a upravené vody	5	4	4	1	3	3	2	1	1	2	1	1	4	1	0.47
Kanalizační stoky a kanály	5	4	4	1	3	3	1	1	1	2	1	1	2	1	0.43
Studně	5	4	5	1	2	2	1	1	1	2	1	1	3	1	0.43
Chemické sloučeniny	4	5	5	3	1	1	1	1	1	2	1	1	2	1	0.41
Čistírny odpadních vod	3	2	1	3	3	3	1	1	1	3	1	1	2	1	0.37
Provozní budovy	3	2	2	1	3	3	1	1	1	3	1	1	3	1	0.37
Čerpací stanice	3	4	2	1	3	2	1	1	1	2	1	1	2	1	0.36
Armatury	3	2	1	1	1	1	1	1	1	2	1	1	2	1	0.27

- na třetím místě co do kritičnosti lze uvést speciální zařízení přehrad, tj. uzávěry výpustí, ovládací zařízení uzávěrů apod. Kritičnost těchto zařízení spočívá v tom, že při teroristických útocích lze dosáhnout u velkých přehrad narušením nebo nesprávným ovládáním těchto zařízení podobného účinku jako při částečném protržení hráze a za příznivých okolností i trvalé narušení pomocného zařízení přehrady nebo i samotné hráze,
- kritičnost potrubí surové nebo pitné vody spočívá v obtížné ochraně celé trasy porubí a v možnosti teroristického útoku injektováním toxických látek do pitné vody. Technické provedení takového útoku není příliš náročné, nevyžaduje speciální technologii a pro teroristu je prakticky bez nebezpečí dopadení,
- kritičnost ostatních částí systému je nižší než v předchozích případech a může dosáhnout vyšších hodnot pouze ve výjimečných případech. Kanalizační stoky a kanály lze napadnout teroristickým útokem, který by spočíval v umístění výbušniny ve vhodném místě a která by byla dálkově odpálena. Při povodních představuje kanalizace obtokový systém, kterým může voda zaplavit jinak chráněnou oblast. Studně a chemické sloučeniny představují

potenciální nebezpečí umístění toxických látek, přičemž rozsah ohrožení může být značně rozdílný případ od případu.

Jestliže vezmeme v tabulce 26 prvních šest nejkritičtějších položek, použijeme multikriteriální hodnocení:

- s kritérii: úroveň společenského vnímání; množství postižených obyvatel; dostupnost veřejnou komunikací; zabezpečení vstupu; dopad nebezpečných látek na člověka a životní prostředí; a množství uvolněné nebezpečné látky,
- stupnici 1 až 5, přičemž 1 je nejmenší a zranitelnost a 5 nejvyšší zranitelnost,
- v souladu s prací [64] budeme zvažovat míru zranitelnosti vyjádřenou vztahem:

$$Z = [k_1 . k_2 + k_3 . k_4 + k_5 . k_6]/ 75,$$

ve kterém k_i jsou hodnoty získané od expertů, tj. míry zranitelnosti se pohybují v rozmezí 3 až 75; dělení číslem 75 znamená převod míry do intervalu (0,1), a dostaneme hodnoty míry zranitelnosti uvedené v tabulce 27.

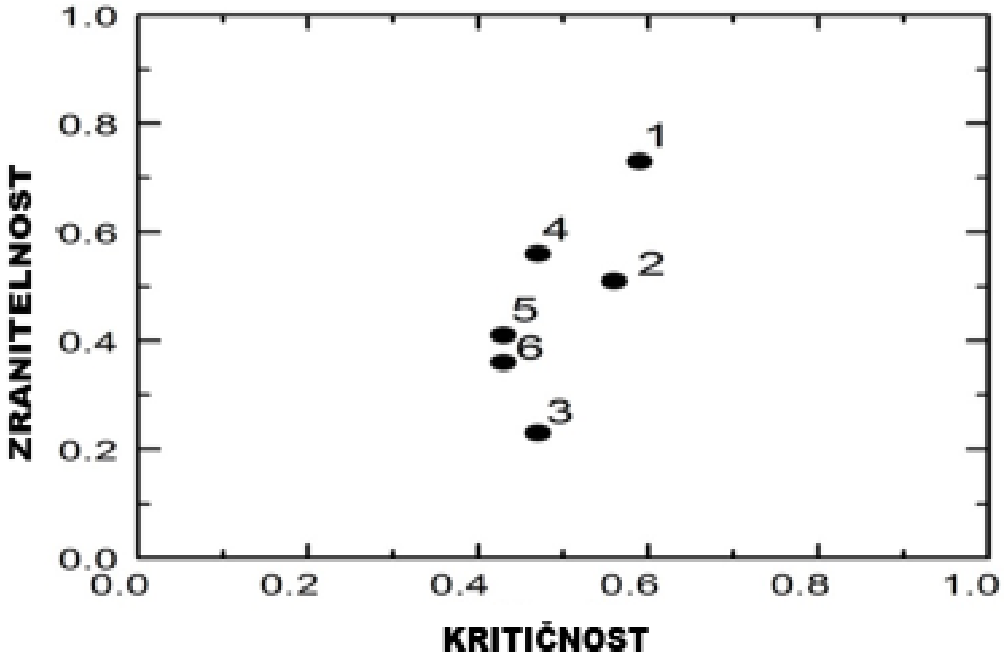
Tabulka 27. Zranitelnost nejkritičtějších aktiv vodohospodářského systému; zpracováno dle tabulky 26 a údajů v [65].

Kritérium	**Míra zranitelnosti**					
	Přehrady a nádrže	**Úpravny vody**	**Speciální zařízení přehrad**	**Potrubí**	**Kanalizace**	**Studně**
Úroveň společenského vnímání	5	5	2	4	2	2
Množství postižených obyvatel	5	5	3	4	2	3
Dostupnost veřejnou komunikací	5	5	5	5	5	5
Zabezpečení vstupu	5	2	2	5	5	4
Dopad nebezpečných látek na člověka a životní prostředí	1	3	1	1	2	1
Množství uvolněné nebezpečné látky	5	1	1	1	1	1
Míra zranitelnosti	0.73	0.51	0.23	0.56	0.41	0.36

Z tabulky 27 vyplývá, že nejvíce zranitelné jsou přehradní hráze a vodní nádrže, následují potrubí, zejména na pitnou vodu a nejnižší zranitelnost mají speciální zařízení přehrad kvůli špatné dostupnosti.

Vztah mezi zranitelností a kritičností je uveden na obrázku 36. Je si třeba uvědomit, že uvedené hodnocení je relativní, protože všechny hodnoty vychází z původního vyjádření dvou expertů v práci [65]. Slouží jako příklad multikriteriálního hodnocení, kterým je možno ocenit složitý systém vazeb, ve kterém působení jednotlivých faktorů na výsledek nelze jednoduše

kvantifikovat. Celkové hodnocení je proto relativní a může být ovlivněno subjektivním přístupem jednotlivých hodnotitelů. Je proto výhodné, jestliže hodnocení provede několik na sobě nezávislých expertů. Výsledky hodnocení platí pouze pro hodnocený systém a nelze porovnávat výsledky hodnocení různých systémů posuzovaných zvlášť.



Obr. 36. Vztah mezi zranitelností a kritičností pro vodohospodářský systém; 1 - přehradní hráze a vodní nádrže; 2 - úpravny pitné vody; 3 - speciální zařízení přehrad; 4 - potrubí pitné vody; 5 – kanalizace, 6 – studně.

Obrázek 36 je přehledný a ukazuje, že body odpovídající aktivům v pravém horním kvadrantu jsou z vyšetřovaného systému nejohroženější, neboť jejich zranitelnost i kritičnost je největší. Proto je jim třeba věnovat největší pozornost při návrhu ochranných opatření. Pravý dolní kvadrant zahrnuje části, které jsou sice méně zranitelné (např. lze zabezpečit jejich dokonalou ostrahu), avšak narušení jejich funkce může mít závažné důsledky. Těm je potřeba věnovat pozornost v druhé řadě. Při návrhu ochranných opatření je třeba přihlédnout k hodnocení jednotlivých dílčích kritérií a k typu pravděpodobných příčin narušení a podle toho zvolit prioritu a charakter zvolených opatření.

Analyzovaná aktiva vodohospodářského systému z hlediska dopadů jejich selhání při realizaci rizik spojených s jejich zabezpečením lze v souladu s návrhy v práci [65] rozdělit na dvě části:

- aktiva, jejichž selhání ohrozí velký počet obyvatel zátopami (přehrady, vodní nádrže),
- aktiva, která mohou být použita při teroristickém útoku jako systém šíření škodlivých látek, přičemž může být ohroženo rovněž velké množství obyvatel (úpravny vody, potrubí pitné vody).

Ostatní aktiva mají menší rizika, protože při jejich narušení není ohroženo větší množství obyvatel, nebo jsou pro teroristické útoky neatraktivní z jiných důvodů.

Do první kategorie patří velké přehrady, jejichž teroristické narušení je však technicky náročné, nebo menší vodní nádrže, které jsou jako teroristický cíl málo atraktivní. V případě velkých přehrad je teoreticky možné provést destrukci hráze umístěním velkého množství trhaviny ve vnitřních chodbách hráze. To však vyžaduje eliminaci činnosti provozního personálu a určitý čas, což snižuje zranitelnost hráze. U vodních nádrží je proto nebezpečí

narušení větší v případě přirozených příčin, tj. velkých povodní, zejména povodní na zamrzlé řece, při kterých plovoucí kry mohou vodní dílo poškodit, a vyvolaná povodňová vlna může zvětšit dopady původní vlny. Hlavní problém, který vyplývá z existujících technologií, spočívá v dimenzování přehradních hrází. Při jejich návrhu se obvykle uvažoval určitý povodňový stupeň (např. stoletá voda). Vlivem globálního oteplování je třeba počítat s tím, že klimatické změny budou mít větší výkyvy a velké povodně se budou pravděpodobně vyskytovat častěji. V souladu s návrhy, uvedenými v práci [65], je třeba provést revizi výpočtů hrází, a to s uvážením nových předpokladů, které zváží možný větší rozsah povodní v důsledku oteplování biosféry.

Aktiva zmíněná v druhé části mají z hlediska technologie rozdílný charakter. Úpravny vody jsou centralizované výrobny, ve kterých největší riziko je spojeno s úmyslnou kontaminací pitné vody škodlivými látkami. V těchto případech je možné uskutečnit klasická ochranná opatření jako v ostatních průmyslových objektech, tj. řádnou kulturu bezpečnosti v podniku, dokonalou ostrahu a průběžnou automatickou redundantní kontrolu kvality vody pomocí moderních technologií.

Potrubí pitné vody je odlišný typ technologie, který má charakter liniových sítí. Je proto nesnadné zajistit ostrahu potrubí v celém rozsahu. Největší nebezpečí je od kontaminace nebezpečnými látkami, ke které může dojít v důsledku nějaké průmyslové havárie, anebo v důsledku úmyslného (teroristického) útoku, při kterém útočník např. navrtá nebo jinak naruší potrubí a vsype do něho nebezpečnou látku. I když vodovodní potrubí je obvykle uloženo relativně hluboko pod zemí, odlehlost některých částí potrubí může poskytnout útočníkům možnost. Potrubí pitné vody je proto považováno za nejzranitelnější část systému na druhém místě za přehradními hrázemi.

Vodohospodářské stavby

Vodohospodářské stavby jsou: přehrady, zavlažovací systémy, čističky odpadních vod, úpravny vody apod. jsou významnými technickými díly, jejichž porušení znamená závažné nebezpečí pro jejich funkčnost a zároveň bezpečnost obyvatel a jejich okolí.

Výstavba vodních děl se datuje od 5. století; masivní rozvoj pak od počátku 20. století. Současné přehradní nádrže akumulují asi pětkrát více vody než koryta všech světových řek, přesto je v některých zemích její množství nedostačující. V současné době je na světě přibližně 45 000 velkých a dalších asi 800 000 malých přehrad [197]. Mezi největší přehrady na světě patří Tři soutěsky, Itaipú, Nurecká přehrada [198]. Největší přehradou na světě jsou Tři soutěsky na řece Jang-c'-ťiang, která představuje 640 km dlouhou údolní nádrž, jež pojme 39 miliard m^3 vody. Kvůli stavbě muselo být přestěhováno přes dva miliony lidí. Itaipů je sedm a půl kilometru dlouhá a má 196 m vysokou přehradní hráz, která v sobě ukrývá vodní elektrárnu, téměř se rovnající Třem soutěskám. Množství použitého betonu bylo 15krát větší než množství spotřebovaného k výstavbě tunelu pod Lamanšským průlivem a množství použitého železa a oceli, pro srovnání, by stačilo na postavení 380 Eiffelových věží [199]. Kvůli silným dešťům byla přehrada napuštěna již za 14 dní. Mezi nejobjemnější přehrady patří také přehrada Kariba v Zambii, kvůli které bylo přesídleno přibližně 57 tisíc obyvatel.

V České republice je v současné době 124 přehrad [200]. Největší z nich je Lipenská přehrada, která je zároveň největší vodní plochou na území České republiky. Vodní dílo Orlík na řece Vltavě má největší hloubku 74 m, stálý objem 280 milionů m^3 vody a zásobní objem 374.5 milionů m^3 vody [201].

Poruchy přehrad a jejich důsledky v minulých dobách dle [12]:

1. Přehrada Desná (16. 9. 1916) [202]. Technické parametry: výška hráze: 13.16 m; šířka paty hráze: 54 m; šířka koruny hráze: 5.2 m; délka hráze v koruně: 172.80 m; kóta koruny hráze: 820 m; kubatura hrázového tělesa: 310 920 m^3 Přehrada na říčce Bílá Desná v Jizerských horách se zhruba po roce své existence protrhla a smetla část obce Desná. 95 rodin s

380 příslušníky bylo pak bez přístřeší, 1020 osob bez možnosti zaměstnání, 370 občanů ztratilo veškerý majetek. 29 obytných domů a 11 brusíren skla zmizelo ve vlnách a 62 domů a závodů bylo vážně poškozeno. Druhý den bylo 59 osob nezvěstných. Škody byly odhadnuty na několik milionů korun. Dodnes jde o největší katastrofu spojenou s přehradou v historii českých zemí.

2. Přehrada Malpasset – Francie (2. 12. 1959). Protržení přehrady mělo za následek 420 obětí na životech a značné škody na majetku. K protržení hráze došlo kvůli špatnému založení (chyba v zadávacích podmínkách z oblasti geologie a geotechniky [203]). Tragédii způsobil tektonický pohyb okolních skal v kombinaci s vydatnými srážkami, které způsobily přeplnění nádrže, která nevydržela tlak hornin i vody.
3. Přehrady na řece Chuaj v provincii Chen-an – Čína (Srpen 1975). Při protržení dvou přehradních hrází během dvou hodin údajně zahynulo 85 000 lidí; dalších 145 000 osob podlehlo následujícím epidemiím a hladomoru.
4. Přehrada Teton, Idaho – USA (1976). Sypaná hráz byla protržena při prvním naplnění.
5. Přehrada Mačhu-2 – Indie (11. 8. 1979). Ve městě Módví se protrhla hráz přehrady kvůli dlouhotrvajícím dešťům, tj. přeplněním; odhady počtu obětí se pohybují od 1500 do 15 000.
6. Protržení hráze u Města Neustadt nad Dunajem - Německo (1999).
7. Přehrada na říčce Havasu, oblast Grand Canyonu – USA (srpen 2008).
8. Protržená hráz u města Plock, na Visle (asi 100 km od Varšavy) - květen 2010.
9. Přehrada na řece Maquoketa, Iowa - USA (26. 7. 2010).
10. Odkaliště u města Ajka - Maďarsko (4. 10. 2010). Protržení si vyžádalo 9 obětí, onemocnění desítek lidí a velké ekonomické ztráty.
11. Protržená přehrada Vaiont (Langarone) v Itálii dne 9. 10. 1963. V roce 1960 byla postavena přehrada napříč údolím Vaiont v severovýchodní Itálii blízko hranic se Slovinskem a Rakouskem. Hráz měla být nejvyšší v Evropě s rozměry: výška je 262 m, šířka u báze přehrady 27 m, na koruně hráze 3.4 m. Údolí probíhá podél spodku geologické struktury (synklinály), kde jsou skály ohnuty směrem dolů a ponořeny do údolí z obou stran. Skály jsou převážně z vápence, ale některé jsou složitě prostoupeny písky a jíly. Tyto pískové a jílové vrstvy tvoří podkladové plochy souběžné synklinální struktury a jsou zanořené příkře do údolí z obou stran. V době stavby přehrady různí profesionální i amatérští geologové upozorňovali na to, že podloží hory Monte Toc je nestabilní; tj. svrchní pevné vrstvy horniny leží na vrstvě jílu a teprve pod ním je pevná skála; jíl při nasycení vodou ztekutí, tj. stane se perfektní klouzačkou, po které se do přehradního jezera mohou realizovat sesuvy podloží z vrcholu hory. Už v průběhu napouštění začalo docházet k problémům v okolí přehrady. V listopadu 1960, kdy byla přehrada naplněná do výše 190 m z cílových 262 m, došlo k menšímu sesuvu o objemu asi 800 tisíc m^3 horniny do přehrady. Hladina byla tedy dočasně snížena o 50 metrů a na pravé straně jezera byl vybudován tunel, aby mohla voda při přesuvech kudy odtékat a nedošlo k poškození hráze. Poté se začala opět přehrada napouštět. Tlak obrovské masy vody na podloží vyvolával otřesy půdy, které poškozovaly domy obyvatel okolních měst a vesnic, tj. nejen v obci Longarone. V zemi se objevovaly trhliny. Lidé se začali stěhovat do větších měst pod horami a povodí Vajontu se vylidňovalo. Stavitel přehrady, společnost SADE, si poté nechala vypracovat model sesuvu o objemu 50 milionů tun horniny do přehrady. Ukázalo se, že dynamika vody při takovém sesuvu by byla smrtící pro Longarone, ale zadavatelé se spolehli na štěstí, a protože přehradu již odkoupila italská vláda, výpočty utajili. Poté se v hoře Toc objevily další trhliny a slabá zemětřesení neustávala. Došlo k sérii dalších sesuvů a vedení přehrady se nakonec rozhodlo v září 1963 hladinu vody přece jen snížit. Jenomže upuštěním vody došlo k tomu, že ustoupil protitlak vody, který přidržoval vodou nacucanou zeminu na úbočí hory a zabraňoval sesuvu. Začátkem října se denní sesuv zrychlil z centimetrů na decimetry. V den katastrofy byl již sesuv tak rychlý, že se dalo předpokládat uvolnění celého vrcholu hory,

nicméně nikdo se neodhodlal k vyhlášení evakuace. 9. října 1963 ve 22,39 hod. se z úbočí hory Monte Toc definitivně utrhlo a do jezera zřítilo ***270 miliónů tun*** horniny. Sesuv proběhl během několika sekund, hmota se řítila rychlostí 60 km/hod. Sesuv vytlačil vodu o objemu ***50 milionů tun vody*** a vyvolal v mžiku vlnu vody a bahna vysokou 100-150 metrů nad hráz. Během 4 minut vlna dorazila rychlostí 100km/hod do Longarone, kde měla výšku 70 metrů, narazila na protější břeh a smetla Longarone z povrchu. Ještě u Belluna, které je vzdálené 25 km měla vlna výšku 12 metrů a opadla až u ústí do moře u Benátek 120 km daleko. Bylo přes 2000 obětí na životech [204].

Proto, jak již bylo řečeno, ČR pro každé vodní dílo vyžaduje zákonem č. 274/2001 Sb. zpracování zvláštních povodňových plánů a má typové plány pro odezvu na protržení hrází vodních děl.

5.9. Výsledky studia rizik dopravního systému a návrh ochranných opatření

Dopravu tvoří rozsáhlá síť dopravních cest, objektů, podpůrných systémů a dopravních prostředků různých druhů a typů. Dopravní sektor zahrnuje objekty, technické a informační infrastruktury a také personál. Dopravní infrastruktura je také základní infrastrukturou, která tvoří kritickou infrastrukturu v území; při kritických situacích zajišťuje základní úkony, a to evakuaci lidí z postiženého místa a přesun techniky do postiženého místa, aby bylo možné odstranit škody, stabilizovat situaci a provést obnovu.

Pro zajištění bezpečného území s dostatečným potenciálem udržitelného rozvoje je třeba dbát o udržitelnou dopravní infrastrukturu. Zranitelnost dopravní infrastruktury je míra selhání dopravní infrastruktury (tj. dopravní infrastruktura přestane fungovat nebo bude fungovat nesprávně) v území a čase. Předmětnou míru lze měřit např. normovaným souhrnným (integrálním) rizikem od všech očekávaných pohrom v daném území nebo pravděpodobností výpadků infrastruktury, ke kterým dojde v důsledku očekávaných pohrom, do nichž se zahrnují i vnitřní problémy infrastruktury samotné.

Bezpečná dopravní infrastruktura je infrastruktura, která zajišťuje požadovanou dopravní obslužnost, tj. je provozně spolehlivá, funkční a neohrožuje sebe, ani okolí, tj. chráněná veřejná aktiva. Představuje systém systémů, který vznikl propojením několika systémů, tj. systém komunikací, systém dopravních prostředků, systém materiálně technické podpory dopravy, systém dopravních pravidel, který je vložen do systému životního prostředí, sociálního systému a systému ostatních infrastruktur. Systém, který vznikl propojením, je dynamický systém, jehož chování je ovlivněno pohromami všeho druhu. Propojení mají povahu fyzickou, kybernetickou, logickou a územní. Proto existují různé typy jejich poruch a selhání, a to: kaskádní a eskalující; a porucha ze stejné příčiny (např. poruchy od jisté živelní pohromy), a provozní stavy: normální, abnormální a kritický. Míra těsnosti jejich vztahů a propojení je: volná; těsná; a složitá. Jejich charakteristiky jsou: časové, územně prostorové, organizační, vlastnické a institucionální.

Důsledkem propojení vznikají vzájemné závislosti, které znamenají specifické zranitelnosti a v jejich důsledku porucha či selhání jednoho dílčího systému způsobí poruchu či selhání dílčího systému druhého, což přispívá ke kritičnosti systému systémů v území. Proto na úrovni systému systémů mají zvláštní význam emergentní (náhle se vynořující) vlastnosti, mezi které patří bezpečnost, spolehlivost, upotřebitelnost, použitelnost, reprodukce, růst a rozvoj, využívání energie, evoluční adaptace. Od složitého systému se dopravní infrastruktura liší tím, že se skládá z velkého počtu prvků s nelineárními interakcemi a kauzálními smyčkami, ale na rozdíl od něho má části, které mohou fungovat samostatně; tj. dopravní infrastruktura je systém systémů (SoS) [9].

Pro zajištění bezpečnosti zahrnující funkčnost, provozní spolehlivost a stabilitu dopravní infrastruktury se musí znát prahová hodnota – kritičnost, která určuje stav, při kterém systém systémů zaměřený na plnění určitých cílů nezajišťuje očekávané funkce v požadovaném čase, místě a v požadované kvalitě. Pro odhalení slabin systému systémů zaměřeného na plnění určitých cílů se používají metody multikriteriální analýzy: matice kritičnosti (porovnává zranitelnost a důležitost); měkké metody (Soft System Methodology), Strategic Choice Approach, scénáře; či kauzální metody (Causal Loops Analysis) nebo analýza závislostí [15].

Zvláštní pozornost při zajišťování bezpečnosti dopravní infrastruktury vyžadují specifické objekty, kterými jsou mosty a tunely, a to na dálnicích, silnicích i železnicích. Dále je uveden pouze dílčí výsledek pro silniční most; pro tunely se specifická studie chystá, protože dle požadavků ministerstva dopravy České republiky [205] jsou konkretizovány technické podmínky pro zajištění bezpečnosti pozemních komunikací.

5.9.1. Dopravní infrastruktura a její ohrožení

Přepravní systém, který zajišťuje dopravu osob a nákladů, zahrnuje souborně všechny způsoby dopravy, které v rámci koordinace jednotlivých dopravních systémů spolupracují a vytváří tak logistickou síť [11]. Dopravní logistická síť se v současné době stává velmi významnou oblastí podnikatelských činností, a to nejen v regionálním a státním měřítku, ale též v mezinárodních vazbách. Přepravní síť lze společně s energetikou považovat za jeden ze základů hospodářské prosperity států i organizací. Proto je důležité sledovat všechny jevy, které ho mohou ohrozit.

Přepravní systémy pro svoji činnost vyžadují značné množství prostředků, a to investičních, provozních i administrativních, které většinou vytvářejí autonomní podsoubory, jejichž činnost je vzájemně koordinována. Charakteristickým znakem uvedených podsouborů je jejich schopnost vlastní samostatné činnosti, a proto se často považují za uzavřené celky, což se promítá i do konceptu bezpečnosti a při řízení rizik to znamená, že se používá nejjednodušší přístup, tj. postupy pro uzavřený systém, ve kterém jsou zdrojem rizik pouze technické problémy a lidský faktor [11].

Infrastruktura přepravní sítě je v současné době zatím v převážné části vlastněna veřejným sektorem, její vývoj je však převážně určován požadavky soukromého sektoru. Současně tvoří významný prvek ekonomiky i životního způsobu občanů. Dopravní síť má značný mezinárodní politický vliv, neboť umožňuje mezinárodní spolupráci jednotlivých států a turismus přispívá k integraci občanů.

Přepravní systém je vybudován ze samostatných částí, které tvoří jisté celky, které samostatně zajišťují jistý okruh činností. V provozu území (lidském systému) se však celky vzájemně překrývají, tj. vytváří systém systémů [2,11]. Základem každého jednotlivého celku je určitý druh dopravního prostředku, doplněný komplexem provozních a administrativních podsouborů. Charakteristickým znakem předmětných technologických celků je jejich specializovaná schopnost samostatného provozu, tj. autonomie. Schopnost samostatného provozu je však jen zdánlivá, dílčí celky jsou svázány pravidly dopravní logistiky, která jejich činnost nejen koordinuje, ale též činí ekonomicky výhodnější tím, že snižuje provozní náklady. Na straně druhé je však zdrojem vnitřních závislostí „interdependences“ [11].

Bezpečnost přepravních sítí byla v minulosti zajištěna pouze jednoduchou ostrahou. Ostraha se většinou omezovala pouze na dohled, který měl zabránit převážně majetkovým trestným činům, jako je např. rozkrádání dopravovaného zboží, případně ohrožování osobní bezpečnosti dopravovaných cestujících.

Na základě současného poznání je cílem řízení bezpečnosti dopravního systému, který se skládá z objektů a infrastruktur, zajištění bezpečí a rozvoje, jak dopravního systému, tak okolí dopravního systému, protože jen tak lze zajistit bezpečný lidský systém. Proto musíme

aplikovat nástroje z disciplín, které zajišťují komplexní řízení bezpečnosti systému systémů [10,11]; tj. multikriteriální přístup založený na expertním vyhodnocení možných variant popisujících chování systému systémů určených rozdílným chováním jednotlivých dílčích systémů [5].

Dopravní systém České Republiky

V České republice je přepravní síť ve své podstatě vytvořena z následujících oblastí: železniční dopravní systém; silniční dopravní systém; letecká doprava; a vodní doprava. Hlavní činností podnikání v dopravě je osobní a nákladní doprava. Zajištění racionálního provozu vyžaduje značné zdroje - pracovní síly, kapitál, informace, neboť v moderní vyspělé společnosti je běžné, že propojování a provozování přepravních sítí a poskytování přepravních služeb je významnou součástí prakticky všech ostatních činností. Například zajišťování dopravní obslužnosti ve velkých městech je realizováno městskou hromadnou dopravou, která je založená na většinou koordinované spolupráci silniční a železniční dopravy, někdy též doplněné podzemní drahou, v podstatě se jedná o tzv. integrovaný dopravní systém.

V posledních několika desetiletích se dopravní infrastruktura stala významným cílem teroristických útoků. Zvláště zřetelně se to projevilo v letecké dopravě, ve které se původně teroristé zaměřovali pouze na únosy a ničení letadel, zejména za letu. Po útocích dne 11. 9. 2001 na obchodní centrum v New Yorku se ukázalo, že letadlo se může změnit ve zbraň s katastrofálně ničivými důsledky.

Z historické praxe je známé, že živelní pohromy (v našich podmínkách povodně, vichřice, zemětřesení a sesuvy) často působí značné a prakticky obtížně vyčíslitelná poškození částí železničního a silničního dopravního technologického systému a životního prostředí. Proto lze konstatovat, že dopravní systémy jsou zvláště citlivé na útoky a na živelní pohromy. Jsou též oblíbeným terčem činnosti teroristů, kteří útokem na některý z dopravních systémů mohou způsobit značné škody na majetku i na zařízeních infrastruktury. Je si třeba uvědomit, že nepřímé dopady útoků a jejich důsledky mohou ohrozit dokonce i stabilitu části ekonomie průmyslu či dokonce státu.

Z výše uvedených skutečností vyplývá, že je nutné věnovat problematice destrukce infrastruktury dopravních systémů zvláštní pozornost. Aby se zabránilo ekonomické destabilizaci podnikatelských celků a dalších subjektů průmyslových oblastí, je třeba definovat zvláště citlivé části a hledat způsoby jak snížit nebezpečí zničení důležitých částí, které mají potenciál přerušit činnosti dopravních systémů. Jestliže chceme řídit dopravní systém s cílem zajistit jeho bezpečí a rozvoj, tak musíme znát prioritní aspekty, na nichž závisí dosažení cíle a na které musíme soustředit pozornost, tj. opatření a činnosti [10]. Ze stejného zdroje vyplývá, že kritická místa v technologickém systému (objektu, infrastruktury, podniku, území) jsou místa, kde probíhají základní technologické procesy a pro která platí specifické předpisy zajišťující bezpečnost za normálních, abnormálních a kritických podmínek (např. jednoúrovňové křížení železnice a silnice v obci). Tabulka 28 uvádí aktiva dopravního systému oddělená pro čtyři jeho části, vybraná dle dat v [206].

Tabulka 28. Aktiva dopravního systému.

Aktiva	**Železniční doprava**	**Silniční doprava**	**Letecká doprava**	**Vodní doprava**
Liniové stavby	Kolejová železniční síť ~ 9500 km	Úplná silniční Síť	Systém vzájemně propojených letišť	Vodní cesty

	Elektrifikační síť železnic ~ 32% Železniční zabezpečovací síť			
Objekty	Železniční nádražní budovy pro řízení provozu, odbavovaní cestujících a překladiště Depa vozidel Železniční dílny Železniční mosty Železniční tunely Traťové distance - objekty údržby kolejové sítě a sítě zabezpečovací techniky Železniční dílny pro servis lokomotiv všeho druhu a vozového parku Napájecí stanice elektrifikační sítě železnic Čerpací stanice pohonných hmot	Silniční mosty Silniční tunely Sklady pohonných hmot pro silniční dopravní účely Objekty pro řízení silničního provozu Čerpací stanice pohonných hmot pro silniční vozidla Objekty pro řízení havarijních situací v silniční síti	Letištní dráhy pro start a přistání, síť osvětlení drah Pojezdové dráhy Stojánky letadel Servisní stanice pro leteckou dopravu Běžná předletová příprava - vstupní a generální prohlídky Objekty řízení letového provozu - letištní, oblastní Radarové stanice pro řízení letového provozu Radarové stanice pro meteorologii Výpočetní středisko letiště Zařízení pro sdílení provozních informací pro oblastní službu Zařízení pro sdílení provozních informací pro řízení činnosti letiště Středisko pro zásah při nouzových provozních událostech (havárie….) Čerpací stanice a sklad pohonných hmot	Přístavy se zařízením Zdymadla Doky Hydrometeorologické stanice Objekty údržby plavidel Čerpací stanice pohonných hmot
Zařízení	Železniční vozidla - lokomotivy a vozy Vybavení nádraží a kolejové železniční sítě Zařízení pro ovládání míst křížení silniční a železniční dopravy	Zařízení pro sdílení provozních informací s rámci silniční sítě Vybavení středisek technikou pro řešení havárií	Letadla	Lodě

	Zařízení pro sdílení provozních informací v rámci řízení provozu železničního systému Zařízení pro zásobování pohonných hmot vozidel	Autobusy Nákladní auta Osobní auta		

Na základě současného poznání dopravní infrastrukturu a její provoz ohrožují jednak jevy zahrnuté do přístupu All-Hazard-Approach [2,8] a jednak jevy spojené s vnitřními příčinami v technologickém provedení (změny způsobené stárnutím materiálu i zastaráním samotné technologie, nedostatky v propojení aktiv technické i informační, zdroje organizačních havárií).

5.9.2. Kritičnost jednotlivých dopravních systémů v ČR

Jelikož dopravní systém jako celek i jeho základní podsystémy jsou systémy systémů, tj. jde o několik vzájemně se prolínajících systémů různé povahy (technické, organizační, finanční, personální a právní), tak hodnocení kritičnosti se provádí multikriteriálním přístupem SK1, který je popsán v odstavci 4.2, a dle údajů od expertů. Pomocí faktů v dokumentaci dopravního systému ČR [206] a pomocí údajů od 5 expertů, vybraných dle kritérií EU [10] z oblastí: přeprava; řízení přepravy v území; dodavatelských řetězců; veřejné správy; a Integrovaného záchranného systému, byla získána slovní hodnocení faktorů uvedených v SK1.

Slovní hodnocení sledovaných faktorů pro železniční dopravu, získané od expertů je následující:

1. Míra schopnosti ochrany - ochrana železnice je obtížná v důsledku značné složitosti systému. Při útoku teroristů na hlavní části či při živelní pohromě mohou vzniknout rozsáhlé škody, které znemožní provoz značné části systému. Lidský faktor i organizační havárie mohou rovněž způsobit značné škody.
2. Míra zranitelnosti vůči útoku - zranitelnost železnice je značná, neboť některé části lze poměrně jednoduše rozsáhle zničit (nádražní komplexy, mosty, tunely atd.).
3. Míra ohrožení zdraví a životů lidí - zdraví a životy cestujících jsou ohrožovány prakticky při všech haváriích železničního systému.
4. Míra dopadu selhání na životní prostředí - železniční havárie mohou mít značný dopad na životní prostředí, zejména při přepravě pohonných hmot, chemických látek a podobných surovin. Odstranění zamoření životního prostředí je většinou obtížné a nákladné.
5. Míra nákladnosti výměny či opravy - odstranění škod způsobených destrukcí kolejového systému lze většinou provést bez velkých nákladů. Nákladné jsou velké stavební opravy porouchaných mostů a tunelů. Oprava či obnova zničených železničních vozidel je též často drahá.
6. Míra doby výměny či opravy - oprava kolejí je poměrně rychlá. Velké stavební opravy mostů a tunelů vyžadují delší dobu.
7. Míra důležitosti pro zajišťování záchranných a nouzových funkcí v území – při nouzových situacích je železnice pro zajišťování záchranných a nouzových činností významná a často zcela nezbytná.

8. Míra důležitosti pro zajišťování funkcí správy a samosprávy - pro zajišťování činnosti správy a samosprávy je železnice důležitá, ale její služby lze pro dané činnosti ve většině případů nahradit jiným způsobem dopravy.
9. Míra důležitosti pro zajišťování funkcí armády a policie - pro potřeby armády a policie je železnice nezbytná.
10. Míra redundance nebo substituční služby – zálohování u železnice je poměrně vysoké (je více okruhů), zejména v dopravě základních průmyslových surovin, potravin, pohonných hmot ve větších množstvích. Významnou službou je kontejnerová doprava propojující různé dopravní systémy přičemž kontejnerová doprava vyžaduje vlastní technologii. Zvláště významnou roli hraje kontejnerová doprava v mezinárodní dopravě, ovšem vyžaduje vybudování investičně náročných terminálů, které mohou být citlivým terčem terorismu.
11. Míra důležitosti pro zajišťování komunikačních funkcí - v případě nouze lze využít komunikační síť železnice, která je ve své funkci nezávislá.
12. Míra dopadu selhání obslužnosti na ekonomiku regionu (státu) - narušený železniční dopravní systém nepříznivě ovlivňuje plynulý chod regionálního respektive státního hospodářství a způsobuje značné ekonomické ztráty.
13. Míra důležitosti provozuschopnosti - provozuschopnost železnice je velmi důležitá jak vnitrostátně tak též v mezinárodním měřítku.
14. Míra důležitosti v oblasti symbolické, kulturní apod. - úroveň a stav železničního dopravního systému je svědectvím kulturní a technické úrovně státu.

Slovní hodnocení sledovaných faktorů pro silniční dopravu, získané od expertů je následující:

1. Míra schopnosti ochrany – ochrana silniční sítě je složitá neboť i když narušení vlastní cesty lze poměrně snadno a rychle opravit, citlivé části jako např. mosty a tunely je nutné proti teroristickým útokům a živelním pohromám zvláště důsledně chránit, neboť jejich poškození či zničení často vyžaduje dlouhodobou opravu, investičně většinou náročnou. Lidský faktor i organizační havárie mohou rovněž způsobit značné škody.
2. Míra zranitelnosti vůči útoku - zranitelnost silniční sítě určují zejména citlivé části systému, jako jsou mosty, tunely atd.
3. Míra ohrožení zdraví a životů lidí - zdraví a životy jsou ohrožovány haváriemi při provozu, jejichž počet lze při účinném řízení silničního provozu minimalizovat.
4. Míra dopadu na životní prostředí – silniční doprava silně znečišťuje životní prostředí plyny, které vozidla vypouštějí do ovzduší. Při haváriích vozidel dochází ke znečišťování životního prostředí, zejména rozlitím pohonných hmot a případně též vlivem dopravovaného zboží, které je rozseto v přírodě.
5. Míra nákladnosti výměny či opravy – mimo nákladných oprav citlivých míst sítě - mosty tunely atp. lze většinou opravy škod silniční sítě poměrně levně a v krátkém čase provést.
6. Míra doby výměny či opravy - mimo oprav mostů, tunelů a jiných nákladných částí lze opravy sítě provést v poměrně krátkém čase.
7. Míra důležitosti pro zajišťování záchranných a nouzových funkcí v území – provozuschopnost silnic je velmi důležitá, ale v případě nouze lze při destrukci nejvýhodnější cesty nalézt náhradní cestu, která se vyhýbá poškozeným částem.
8. Míra důležitosti pro zajišťování funkcí správy a samosprávy - je třeba.
9. Míra důležitosti pro zajišťování funkcí armády a policie - zásadně nutná.
10. Míra redundance nebo substituční služby - existuje v principu logistická redundance, umožňující vzájemnou náhradu jednotlivých dopravních systémů.
11. Míra důležitosti pro zajišťování komunikačních funkcí - komunikační funkci lze částečně silniční dopravou v nouzi nahradit.

12. Míra dopadu selhání obslužnosti na ekonomiku regionu (státu) - stav a úroveň silničního systému má významný vliv na ekonomiku.
13. Míra důležitosti provozuschopnosti - provozuschopnost silničního systému je velmi důležitá a zásadně ovlivňuje veškerou činnost regionu i státu.
14. Míra důležitosti v oblasti symbolické, kulturní apod. - Úroveň silniční dopravy a silničního systému svědčí o úrovni státu i jeho tradici.

Slovní hodnocení sledovaných faktorů pro leteckou dopravu, získané od expertů je následující:

1. Míra schopnosti ochrany – ochrana letecké dopravy je velmi náročná, neboť systém letecké dopravy je v současné době nejsložitější ze všech dopravních systémů. K haváriím v letectví dochází jak z technických důvodů, tak z meteorologických důvodů. Letecká doprava je též vyhledávaný cíl útoků teroristů. Lidský faktor i organizační havárie mohou rovněž způsobit značné škody.
2. Míra zranitelnosti vůči útoku – zranitelnost je vysoká. Příprava letadel pro provoz je velmi náročná. Proto letový a technický personál je pečlivě vybíraný a školený. Obrana proti útokům teroristů je prováděna sice intenzivně, ale ne vždy úspěšně.
3. Míra ohrožení zdraví a životů lidí - při leteckých neštěstích dochází ke zranění a smrti posádek letadel i cestujících. Proto zabránění havárií v leteckém provozu je velmi důležité.
4. Míra dopadu na životní prostředí - letecká neštěstí jsou téměř vždy provázena značným místním poškozením životního prostředí, avšak zasahující většinou malou část území.
5. Míra nákladnosti výměny či opravy – náhrada poškozené letecké techniky je téměř vždy finančně velmi nákladná a časově často náročná. Opravy vyžadují značnou zásobu náhradních dílů a práci opravářů specialistů. Opravu je nutné provádět u výrobců nebo v pověřených servisních podnicích.
6. Míra doby výměny či opravy – délka opravy je různá, dle charakteru závady.
7. Míra důležitosti pro zajišťování záchranných a nouzových funkcí v území – letecká technika má výrazné postavení a je téměř nezbytná při reálném řešení krizových situací všeho druhu.
8. Míra důležitosti pro zajišťování funkcí správy a samosprávy – je důležitá jen podmínečně.
9. Míra důležitosti pro zajišťování funkcí armády a policie - je nezbytná.
10. Míra redundance nebo substituční služby - letecká doprava má podmíněnou redundanci, která v důsledku nezávislosti na pozemních sítích umožňuje řešení zvláštních úkolů.
11. Míra důležitosti pro zajišťování komunikačních funkcí – v některých mimořádných případech představuje letecká doprava jediné schůdné řešení.
12. Míra dopadu selhání obslužnosti na ekonomiku regionu (státu) – letecká doprava má velký význam pro ekonomiku, neboť mimo vlastního provozu letecké dopravy je hybným článkem průmyslu.
13. Míra důležitosti provozuschopnosti - velká.
14. Míra důležitosti v oblasti symbolické, kulturní apod. - letecká doprava v ČR má ve světovém měřítku významné postavení. Letecký průmysl ČR má dlouholetou tradici, výrobky se vyvážely prakticky do celého světa.

Slovní hodnocení sledovaných faktorů pro vodní dopravu, získané od expertů je následující:

1. Míra schopnosti ochrany – s ohledem na omezený rozsah sítě vodních cest v ČR lze daný dopravní systém patrně úspěšně chránit. Lidský faktor i organizační havárie mohou rovněž způsobit škody.
2. Míra zranitelnosti vůči útoku – zranitelnost sítě vodních cest určují zejména citlivé části - zdymadla, jezy apod., které zajišťují splavnost vodních toků.
3. Míra ohrožení zdraví a životů lidí - zdraví a životy obyvatel a pracovníků v dopravě jsou ohrožovány v míře, obvykle v ostatních odvětvích průmyslu.

4. Míra dopadu na životní prostředí - zejména znečišťování vodních cest pohonnými hmotami a působí nepříznivě na životní prostředí a biosféru ve vodě a na březích toků.
5. Míra nákladnosti výměny či opravy – havárie lodí nejsou časté, nedochází k velkému rozsahu škod.
6. Míra doby výměny či opravy – pohony lodí se většinou opravují v přístavu, kde opravu lze provést v krátkém čase. Poškození lodního tělesa lze však většinou provádět jen v doku, což prodlužuje dobu opravy.
7. Míra důležitosti pro zajišťování záchranných a nouzových funkcí v území – potřebná jen pro záchranné práce určitého charakteru.
8. Míra důležitosti pro zajišťování funkcí správy a samosprávy - malá.
9. Míra důležitosti pro zajišťování funkcí armády a policie – významná jen ve zvláštních případech.
10. Míra redundance nebo substituční služby - vodní dopravu lze nahradit železniční či silniční dopravou.
11. Míra důležitosti pro zajišťování komunikačních funkcí – malá.
12. Míra dopadu selhání obslužnosti na ekonomiku regionu (státu) – vodní doprava svojí nízkou nákladovostí příznivě ovlivňuje dopravu surovin a těles velkých rozměrů.
13. Míra důležitosti provozuschopnosti – menší - jen v omezené míře.
14. Míra důležitosti v oblasti symbolické, kulturní apod. - vodní doprava má patrně nejdelší tradici a tím se řadí mezi symboly země.

Jelikož hlavním cílem lidí je bezpečí a rozvoj lidí [1,2], pro které je bezpečná dopravní infrastruktura zcela zásadní, je kritičnost dopravní infrastruktury chápána z pohledu zacíleného na přežití lidí. Proto slovní hodnocení byla převedena s pomocí panelové diskuse 5 expertů do numerické stupnice v tabulce 29.

Tabulka 29. Hodnotová stupnice pro stanovení míry kritičnosti dopravní infrastruktury.

Míra kritičnosti	**Bodové hodnocení**		
	Procenta celkové hodnoty	**Jednotlivé dopravní systémy**	**Celý dopravní systém**
Extrémně vysoká	více než 95%	více než 66.5	více než 266
Velmi vysoká	70 - 95%	49 – 66.5	196 – 266
Vysoká	45 - 70%	31.5 – 49	126 - 196
Střední	25 – 45%	17.5 – 31.5	70 – 126
Velmi malá	5 – 25%	3.5 – 17.5	14 - 70
Nevýznamná / zanedbatelná	méně než 5%	méně než 3.5	méně než 14

Míry kritičnosti stanovené metodickým postupem SK1 jsou v tabulce 30.

Tabulka 30. Míry kritičnosti hlavních systémů dopravní infrastruktury v České republice.

Faktor / kritérium	**Železniční doprava**	**Silniční doprava**	**Letecká doprava**	**Vodní doprava**	**Celý dopravní systém**
1	5	4	5	2	16
2	5	4	5	3	17
3	4	3	4	3	14
4	4	3	3	2	12
5	4	3	5	2	14

6	3	2	4	3	12
7	5	5	4	1	15
8	3	3	2	2	10
9	5	5	5	2	17
10	3	2	3	1	9
11	3	2	3	1	9
12	5	4	4	4	17
13	4	4	4	2	14
14	3	2	3	2	10
Všechny faktory	56	46	54	30	186

Z tabulky 30 vyplývá, že největší kritičnost má železniční doprava, za kterou následují letecká doprava, silniční doprava a vodní doprava. Dle zvoleného konceptu, zvolené stupnice a hodnocení získaného od expertů je míra kritičnosti železniční dopravy a letecké dopravy velmi vysoká, míra kritičnosti silniční dopravy vysoká a míra kritičnosti vodní dopravy střední, a míra kritičnosti celého dopravního systému vysoká.

Detailní analýza tabulky 30 ukazuje, že nejvíce ke kritičnosti přispívá velká zranitelnost infrastruktur vůči útokům a malá schopnost ochrany (ochrana sítí v území je vždy velký problém), velká důležitost pro zajišťování funkcí armády a policie, velký dopad selhání obslužnosti na ekonomiku regionu (státu), a velká důležitost pro zajišťování záchranných a nouzových funkcí v území.

5.9.3. Návrh opatření na zvýšení bezpečnosti dopravního systému

Z výše uvedeného rozboru dopravních systémů vyplývá, že se jedná o jednu z nejvýznamnějších oblastí hospodářského i sociálního dění ve státě. K její vysoké kritičnosti přispívá skutečnost, že v posledních desetiletích si danou skutečnost uvědomily též skupiny obyvatel v různých státech, které nejsou spokojeny se současným státním zřízením v domovských zemích, vytvářejí si svoji vlastní politickou ideologii, která většinou silně kritizuje současné politické zřízení státu, ve kterém žijí a snaží se své názory a životní cíle násilně prosazovat nelegálním způsobem a jako nevýhodnější postup pro prosazení své ideologie pokládají terorismus.

Terorismus v současné době má globální podobu, takže jeho mezinárodní charakter vede k nutnosti ochrany proti útokům. Ve sledovaném případě je skutečností: velká důležitost dopravních systémů, vysoká zranitelnost dopravních systémů, a též skutečnost, že části dopravních systémů lze použít jako útočnou zbraň s velkým ničivým potenciálem, jak ukázaly útoky v New Yorku dne 11. 9. 2011. Je proto třeba vyvinout protiopatření pro snížení možnosti napadení dopravních systémů a zabránit tak zničujícím důsledkům na chod státu a na životy občanů.

Ve spojitosti s výsledky projektu Evropské unie FOCUS [19] je nutné zvážit, že nejen terorismus, ale i živelní pohromy, organizační havárie a korupce spojená s oblastí řízení často způsobují rozsáhlé škody na dopravních systémech. Příprava a tvorba ochranných opatření vyžaduje značné investiční akce, a proto je třeba investice koordinovat a dle možnosti slučovat opatření pro ochranu dopravních systémů proti škodám způsobeným možnými pohromami [2,8] teroristickou činností a živelními pohromami, tak jak to vyžadují zásady strategického řízení [1,2].

Vzhledem k tomu, že ani terorismu, ani živelním pohromám nelze zabránit, hlavním cílem předmětných činností jsou zmírňující opatření při výskytu pohrom s cílem snížit ztráty na lidských životech a minimalizovat škody [1,2,10,11]. Protože význam dopravních systémů je

značný, je velmi naléhavé provést opatření a činnosti, které umožní kritickou infrastrukturu dopravních systémů účinně chránit před činností mezinárodního terorismu a dalších pohrom. Je třeba provést opatření ke snížení zranitelnosti, opatření zajišťující rychlou odezvu na selhání kritických prvků a opatření na zajištění kontinuity kritických prvků a na rychlou obnovu dalších důležitých prvků. Je třeba:

- provést odhad zranitelnosti funkčních prvků dopravního systému v rámci posuzování objektů dopravního systému jako jsou mosty, tunely, silnice, dálnice, letiště a vodní cesty,
- stanovit nejzranitelnější části infrastruktur, jejichž selhání mohou způsobit největší ekonomické škody v infrastruktuře až znemožnit dopravní činnost,
- vytvořit scénáře dopadů významných pohrom a možných útoků a na základě scénářů dopadů stanovit postupy rychlé odezvy a postupy pro zajištění dopravní obslužnosti v co nejvyšší možné míře,
- zlepšit opatření a činnosti v oblasti plánování s cílem zlepšit ochranu proti možným pohromám a teroristickým útokům na dopravní systém, a to nejen z hlediska jednotlivých systémů, ale v rámci logistiky daná opatření plánovitě propojit a zvýšit bezpečnost celého systému chápaného jako systém systémů,
- stanovit opatření vedoucí ke snížení možnosti napadení dopravních infrastruktur a ke zlepšení detekce útoků na dopravní infrastruktury,
- odhadnout výši investic a pracovních nákladů, které si vyžádá provedení zmírňujících opatření v případě selhání dopravních infrastruktur a navrhnout postup jejich aplikace,
- provést rozbor a návrh ochrany infrastruktury přepravní sítě proti škodám, které mohou vzniknout v důsledku možných pohrom a provést odhad vzniku provozní neschopnosti v důsledku vyřazení funkčních prvků, příp. jejich částí,
- snížit četnosti přerušení provozu dopravních systémů v důsledku selhání, které nelze ani při pravidelných kontrolách spolehlivě předem odhalit.

Výše uvedená fakta ukazují, že je naléhavě nutné otázkám bezpečnosti dopravních systémů věnovat značně zvýšenou pozornost. Je třeba zpracovat jak samostatnou koncepci, tak koncepci kritické infrastruktury tak, jak ukazuje práce [60]. Z odborného pohledu je nezbytné k řešení otázek bezpečnosti zavést systémový přístup, který umožňuje držet krok s technologickým vývojem dopravních systémů, zvažuje potřeby lidí a dopravní obslužnost, ochranu životního prostředí a snižuje ekonomické škody. Je třeba expertním způsobem definovat problematiku, kterou je nutné vyřešit a zpracovat příslušné studie ve smyslu shora doporučeného postupu.

5.9.4. Výsledky studia dopravního systému a vybraných selhání

Problematika dopravy je velmi široká. Proto se dále nebudeme zabývat např. haváriemi raket, ani haváriemi na kosmodromech (např. na Bajkonuru dne 24. 10. 1960 došlo k požáru, který se rozšířil na nádrže s pohonnými látkami, což mělo za následek ztrátu života 76 lidí a 126 zraněných) [12]. Jejich důkladné zpracování vyžaduje sběr specifických dat a vytvoření databází s dobrou vypovídací hodnotou, což je náročné na čas, data a detailní znalosti problematiky u zpracovatelů, což nedovoluje časový rozsah projektu.

Na základě údajů v odborné literatuře k dopravním nehodám dochází při přepravě na silnicích, železnicích, řekách, mořích i oceánech a ve vzduchu. Na základě šetření inspekcí v různých zemích světa k nim dochází i tehdy, když řidiči dodržují předpisy. Na základě šetření v USA a UK z r. 1985, jejichž výsledky jsou shrnuté v [185], ukazují, že příčiny dopravních nehod na silnicích jsou rozděleny následujícím způsobem:

- 57% lidský faktor řidiče,
- 27% kombinace faktoru silnice a faktoru řidiče,
- 6% kombinace faktoru vozidla a faktoru řidiče,
- 3% faktor silnice,

- 3% kombinace faktorů silnice, řidiče a vozidla,
- 2% faktor vozidla,
- a 1% kombinace faktoru silnice a vozidla.

Ke vzniku nehody přispívají design vozidla, rychlost provozu, design vozovky, prostředí kolem vozovky, dovednost a defekty v chování řidiče. Zkušenosti i všechny dostupné modely ukazují, že příčina dopravní nehody je zpravidla důsledkem kombinace několika faktorů, tj. její odhalení vyžaduje multikriteriální přístupy. Na základě uvedeného poznatku je výzkum, jehož výsledky jsou dále uvedeny, proveden nejen pomocí statistických metod, ale i pomocí metod rizikového inženýrství

5.9.4.1. Doprava silniční

Doprava silniční patří mezi nejrozšířenější obory národního hospodářství, které se nejvíce rozvíjí. Její velký rozvoj však nepřináší pouze zisky, ale i dopady. Stinnou stránkou dopravy, která ovlivňuje hospodářský vývoj státu a regionů, způsobuje nemalé škody v oblasti životního prostředí a způsobuje velké ztráty na zdraví a životech obyvatelstva, je nehodovost, která je v České republice v silniční dopravě obzvláště vysoká. Proto bezpečnost silniční dopravy je jedním ze základních cílů státu. Jelikož bezpečnost dopravy značně závisí na kvalitě opatření a činností zacílených na zvládnutí existujících rizik, je nutné zjistit místa, ve kterých jsou rizika dopravních nehod velmi vysoká a na ně zaměřit pozornost.

Běžné dopravní nehody

Cílem provedeného výzkumu dopravních nehod na silnici bylo určit kritická místa z pohledu nehodovosti na dálnici D1 v úseku Praha – Mirošov, a navrhnout opatření na zvýšení její bezpečnosti. Pro určení kritických míst byl zvolen kontrolní seznam [5,15], a to ve formě uvedené v tabulce 31.

Tabulka 31. Kontrolní seznam pro posouzení kritičnosti dálnice D1 [207].

Otázka	**Odpověď ANO**	**Odpověď NE**
Nachází se v daném místě zatáčka o poloměru větším než 200 metrů?		
Je v daném místě sklon vozovky větší než 5 %?		
Je v daném místě 3 a více problémových míst (sjezdy, nájezdy, mosty, čerpací stanice)?		
Nacházejí se na vozovce velké výmoly?		
Je denní intenzita provozu větší než 72000 vozidel?		
Je průměrný počet dopravních nehod za jeden měsíc větší než 1,6?		
Mohou nastat v daném místě 2 a více meteorologických komplikací?		

Podle tabulky 31 byla vytvořena hodnotová stupnice pro konkrétní případ, která je uvedena v tabulce 32.

Tabulka 32. Hodnotová stupnice pro daný případ [207].

Rozmezí hodnot pro určení kritičnosti	**Míra kritičnosti**
Více než 6.65	Katastrofálně velká
4.9 – 6.65	Velmi velká

3.15 – 4.9	Velká
1.75 – 3.15	Střední
0.35 – 1.75	Malá
Méně než 0.35	Zanedbatelná

Tabulka 32 určuje mezní hodnoty kritičnosti (počet odpovědí „ANO“) a vyplývá z ní, že pokud je počet odpovědí „ANO“:

- větší než 6, je kritičnost katastrofálně velká,
- mezi 5 – 6, je kritičnost velmi velká,
- roven 4, je kritičnost velmi velká,
- mezi 2-3, je kritičnost střední,
- roven 1, je kritičnost malá,
- roven 0, je kritičnost zanedbatelná.

Pro syntetické vyhodnocení kritičnosti jednotlivých míst, tj. pro určení kritičnosti jednotlivých úseků sledované části dálnice D1 jsme na základě expertního posouzení konkrétních dat z dálnice D1 sestavili hodnotovou stupnici uvedenou v tabulce 33.

Tabulka 33. Hodnotová stupnice jednotlivých parametrů kritičnosti [207,208].

Počet bodů	**Parametry kritičnosti**
0	technická a environmentální kritičnost je malá nebo zanedbatelná
	intenzita provozu je menší než 43 000 vozidel za 24 hodin
	průměrný počet dopravních nehod je menší než 0,8 za 1 měsíc
1	technická a environmentální kritičnost je střední až velká
	intenzita provozu je v rozmezí 43 000 - 72 000 vozidel za 24 hodin
	průměrný počet dopravních nehod je v rozmezí 0,8 - 1,6 za 1 měsíc
2	technická a environmentální kritičnost je velmi velká a větší
	intenzita provozu je větší než 72 000 vozidel za 24 hodin
	průměrný počet dopravních nehod je větší než 1,6 za 1 měsíc

Nově jsme použili též intenzitu provozu. Její prahové hodnoty jsme zvolili na základě vyhodnocení počtu průjezdů vozidel ve sledovaných místech. Analýza konkrétních údajů pro průjezd vozidel [207] ukazuje, že pokud pozorovaným úsekem projede méně než 30 vozidel za minutu, což znamená hodnotu menší než 43 000 za 24 hodin, je silniční provoz obvykle bez komplikací. V případě průjezdu 30 až 50 vozidel za minutu (43 000 – 72 000 za 24 hodin) se zvyšuje počet dopravních nehod. Pokud pozorovaným úsekem projede více než 50 vozidel za minutu (více než 72 000 za 24 hodin), dochází k zahuštění dopravního provozu a ke vzniku většího počtu dopravních nehod.

V tabulce 33 používáme též hodnocení založené na kategorizaci průměrných počtů dopravních nehod. Jejich prahové hodnoty za jeden měsíc za posledních deset let byly stanoveny na základě statistiky dopravní nehodovosti, uvedené v [207]. Pokud ve sledovaném úseku dlouhodobě dochází k méně než 10 dopravním nehodám za rok (0.8 nehody za měsíc) lze považovat toto místo za relativně bezpečné, tj. v daném místě je malá kritičnost. V případě počtu 10 – 20 dopravních nehod za rok (0.8 – 1.6 nehody za měsíc) se bezpečnost sledovaného místa zhoršuje, tj. zvyšuje se kritičnost. Pokud je počet dopravních nehod větší než 20 za rok (více než 1.6 nehody za měsíc), místo není bezpečné, tj. má vysokou kritičnost.

Nejprve byla provedena důkladná rekognoskace terénu (horizontální profil, vertikální profil, množství a přehlednost zatáček, významné meteorologické faktory) [207]. Na základě dat získaných rekognoskací terénu [207], aplikací kontrolního seznamu, faktických údajů o intenzitě provozu a faktických údajů o dlouhodobém průměrném počtu dopravních nehod, byly pomocí hodnotové stupnice, uvedené v tabulce 33, všechny zpracované údaje bodově ohodnoceny [207,208] a byla určena kritičnost, tabulka 34 [208].

Tabulka 34. Kritičnost míst na úseku 0-21 km (Praha – Mirošovice) na dálnici D1 v obou směrech **[**208].

Km - Směr Praha	**Počet bodů**	**%**	**Míra kritičnosti**	**Kategorie kritičnosti místa**	**Km - Směr Brno**	**Počet bodů**	**%**	**Míra kritičnosti**	**Kategorie kritičnosti místa**
0-1	7	50.00	Velká	3	0-1	7	50.00	Velká	3
1.01-2	6	42.86	Střední	2	1.01-2	6	42.86	Střední	2
2.01-3	4	28.57	Střední	2	2.01-3	6	42.86	Střední	2
3.01-4	5	35.71	Střední	2	3.01-4	6	42.86	Střední	2
4.01-5	6	42.86	Střední	2	4.01-5	8	57.14	Velká	3
5.01-6	6	42.86	Střední	2	5.01-6	6	42.86	Střední	2
6.01-7	8	57.14	Velká	3	6.01-7	7	50.00	Velká	3
7.01-8	4	28.57	Střední	2	7.01-8	4	28.57	Střední	2
8.01-9	5	35.71	Střední	2	8.01-9	7	50.00	Velká	3
9.01-10	7	50.00	Velká	3	9.01-10	8	57.14	Velká	3
10.01-11	9	64.29	Velká	3	10.01-11	9	64.29	Velká	3
11.01-12	6	42.86	Střední	2	11.01-12	5	35.71	Střední	2
12.01-13	4	28.57	Střední	2	12.01-13	4	28.57	Střední	2
13.01-14	5	35.71	Střední	2	13.01-14	5	35.71	Střední	2
14.01-15	7	50.00	Velká	3	14.01-15	7	50.00	Velká	3
15.01-16	8	57.14	Velká	3	15.01-16	8	57.14	Velká	3
16.01-17	2	14.29	Malá	1	16.01-17	2	14.29	Malá	1
17.01-18	6	42.86	Střední	2	17.01-18	6	42.86	Střední	2
18.01-19	4	28.57	Střední	2	18.01-19	3	21.43	Malá	1
19.01-20	2	14.29	Malá	1	19.01-20	2	14.29	Malá	1
20.01-21	3	21.43	Malá	1	20.01-21	2	14.29	Malá	1

Z tabulky 34 vyplývá, že ve směru jízdy na Prahu patří mezi nejkritičtější následující 3 úseky, u kterých je míra kritičnosti označena jako velká:

- úsek mezi 10 – 11 km, který je ovlivněn vertikálním profilem dálnice, složitostmi na dálnici (most a komplikovaný exit), velkou intenzitou provozu vozidel a hlavně dopravní nehodovostí, která je v tomto místě druhá největší ze sledovaného úseku dálnice mezi Prahou a Mirošovicemi,

- úsek mezi 6 – 7 km, který je ovlivněn především složitostmi na dálnici (most, křižovatka a parkoviště s čerpací stanicí) a velkou intenzitou provozu vozidel,
- úsek 15 – 16 km, který je ovlivněn především horizontálním i vertikálním profilem dálnice.

Ve směru jízdy na Brno patří mezi nejkritičtější místa následující 4 úseky, i u těchto míst je míra kritičnosti označena jako velká:

- úsek mezi 10 – 11 km, který podléhá stejným vlivům jako úsek ve směru jízdy na Prahu a nehodovost je čtvrtá největší ze sledovaného úseku dálnice mezi Prahou a Mirošovicemi,
- úsek mezi 4 – 5 km, kde se na kritičnosti podílejí všechna hodnocená kritéria,
- úsek mezi 9 – 10 km, kde se na kritičnosti podílejí všechna hodnocená kritéria,
- úsek mezi 15 – 16 km, který je ovlivněn horizontálním i vertikálním profilem dálnice a také povětrnostními podmínkami (boční vítr a stékající voda).

Mezi místa, kde je míra kritičnosti malá, byly v obou směrech jízdy vyhodnoceny úseky mezi 16 – 17 km, 19 – 20 km a 20 – 21 km. Tyto úseky patří mezi místa, kde nic nebrání přehlednosti v silničním provozu a vyznačují se menší intenzitou provozu vozidel.

Vyhodnocením kontrolního seznamu bylo zjištěno, že nejkritičtějším místem dálnice D1 v úseku Praha – Mirošovice je v obou směrech jízdy úsek mezi 10 – 11 km. Proto pro něho byl vypracován dlouhodobý plán na zvyšování bezpečnosti [207].

Dopravní nehody s nebezpečnými látkami

Dopravní nehody s přítomností nebezpečných látek jsou velmi nebezpečné pro okolí, jak ukazují čtyři příklady z naší databáze [12], která obsahuje souhrnná data od konce 19. století a detailní data pro 30 274 dopravních nehod s přítomností nebezpečných látek z let 2007-2010:

1. Dne 11. května 1976 v 11:15 vezlo nákladní auto 7 500 galonů (19 tun) bezvodého amoniaku z chemického závodu Tenneco na sever po West Loop do Corpus Christi. Řidič nákladního auta, které vlastnila firma Transport Co of Texas, na výjezdu z dálnice Southwest Freeway, ztratil kontrolu nad vozidlem, narazil na nosný sloup mostu a převrátil vozidlo. Při dopravní nehodě se uvolnil oblak amoniaku, obrázek 37. Na obrázku je vidět bílý oblak výparů bezvodého čpavku při teplotě 83^{o} F [209,210]. Podle zpráv lidí, kteří nemohli odjet, zděšení lidé prchali pěšky z místa nehody. Sedm lidí zemřelo v důsledku dopravní nehody (šest osob bezprostředně, jedna v roce 1979 na zdravotní komplikace vyplývající z nadýchání kontaminovaného ovzduší). Sedmdesát osm lidí bylo hospitalizováno, a více než 100 bylo léčeno pro zranění spojená s poškozením způsobeným amoniakem. Někteří z těchto lidí pravděpodobně stále trpí dlouhodobým onemocněním.

Obr. 37. Dopravní nehoda v Houstonu 11. 5. 1976; bílý oblak v dálce je toxická deka výparů, jako důsledek havárie autocisterny na dálnici [209,210].

2. Dopravní nehoda, která způsobila vážné ztráty a škody v Kemp Los Alfaques (Španělsko, 11. 7. 1978). Z přeplněné automobilové cisterny převážející 23 t zkapalněného propylenu při dopravní nehodě v blízkosti Tarragony unikl propylen, vznítil se a následně cisterna explodovala (BLEVE) [211,212]. San Carlos de la Rápida patří k oblíbeným letoviskům na Costa Blanca, jež tvoří součást španělského pobřeží Středozemního moře. Ještě o něco jižněji ležící Benidorm, který přitahuje každoročně tisíce turistů na prosluněné pláže mezi Tarragonou a Cartagenou. V létě 1978 turisté ze Španělska i z ciziny zaplnili kemp Los Alfaques do posledního místečka. Přímo okolo kempu vedla státní silnice č. 340. Již několikrát se objevil požadavek na zvýšení bezpečnosti silnice, po níž se každý den přepravovalo na 4 000 tun vysoce výbušných nákladů. Jeden takový náklad přinesl 11. července 1978 osazenstvu kempu smrt. Cisternový vůz přepravující zkapalněný propylén sjel ze silnice, narazil do zdi obklopující kemp a explodoval. Během několika sekund se přehnala ohnivá stěna celým kempem. Peklo se šířilo závratným tempem, protože žárem vybuchovaly i plynové láhve vařičů a nádrže aut turistů. Plameny se šířily nejen rychle, ale i nekontrolovatelně. Plameny po sobě zanechaly hrozný obraz zkázy. Stany, vozy a obytné přívěsy shořely až na pár zuhelnatělých zbytků, obrázek 38. 115 osob bylo ihned usmrceno požárem, řada dalších byla v různém stupni zasažení popálena. Konečné údaje: 217 mrtvých, více než šest set osob bylo zraněno, mnozí těžce. Příčiny: přeplněná cisterna neodpovídající bezpečnostním požadavkům, vznik praskliny na cisterně při nárazu na zeď, špatně zvolená trasa přepravy (řidiči bylo nařízeno použít místní silnici místo zpoplatněné dálnice A-7).

Obr. 38. Dopady silniční nehody v kempu [211,212].

3. Dopravní nehoda v Bangkoku (Thajsko) dne 24. 9. 1990. Nákladní auto vezoucí dvě nezajištěné 20.000 litrové nádrže zkapalněného zemního plynu se převrátilo v centru města [213], obrázek 39. Vzniklé exploze a požáry zničily 43 vozidel a mnoho budov v okolí (z toho 38 obchodů) a zabily 90 a zranily 121 osob.

Obr. 39. Ohnivé peklo způsobené dopravní nehodou v Bangkoku dne 24. 9. 1990 [213].

4. Dopravní nehoda u Břestu dne 26. 2. 2008. Došlo k úniku kyseliny dusičné z cisterny u Břestu [214]. Řidič kamionu s cisternovým návěsem uvedl, že na únik kyseliny ho upozornili až další řidiči blikáním a troubením. Po zastavení u krajnice vystoupil a uviděl masivní únik v zadní části cisterny, obrázek 40. Okamžitě nahlásil havárii na tísňovou linku 112 a oznámil únik převážené kyseliny dusičné v 70% koncentraci. Řidič

Obr. 40. Dopravní nehoda u Břestu.

zraněn a kyselinu natankoval ve Vizovicích v objemu 6 tun. Do zastavení za sebou zanechala cisterna znečištěnou vozovku v délce asi 8 kilometrů, a to už z obce Hulín. První čtyři kilometry k obci Břest byla vozovka znečištěna jen drobně, až v Břestu byla vidět stále silnější stopa, která postupně znečistila jednu polovinu vozovky k hranici Zlínského kraje. Odhaduje se, že při havárii došlo k úniku několika set litrů kyseliny dusičné. Kamion byl odstaven uprostřed polí a vlivem čerstvého větru byly vytvořeny dobré rozptylové podmínky. Přímé ohrožení občanů tak bylo sníženo, ale přesto bylo přijato několik preventivních opatření. Celá zóna byla vyhrazena bezpečnostní páskou k zamezení vstupu

nežádoucích osob. Následovala etapa přečerpání kyseliny do náhradního vozu. Na místo havárie přijela i další specializovaná firma, která se postarala o sanaci zasažené půdy.

Dopravní nehody na silnicích byly předmětem samostatného výzkumu, jehož výsledky jsou shrnuty v práci [185]. Z předmětné práce vyplývá:

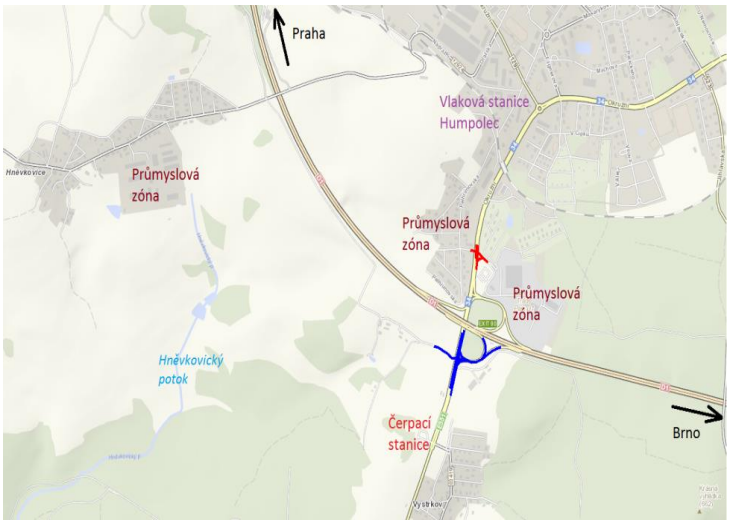
1. Rekognoskací kritických míst na dálnici D1 bylo zjištěno 14 potenciálně kritických míst, tabulka 35.

Tabulka 35. Kritická místa na dálnici D1 [185,191].

	Nehodovost (1/měsíc)	Vertikální profil	Horizontální profil	Podnebí	Šířka vozovky	Kvalita vozovky	Další faktory	Hustota provozu	Celkem
exit1	2.48	a/0	b/1	0	b/1	a/0	2	c/2	8.48
1-2 km	3	b/1	a/0	0	a/0	a/0	0	c/2	6
exit2	4.78	a-b/0.5	a-b/0.5	0	a/0	a/0	2	c/2	9.78
2-4km	1.6	b/1	a/0	0	a/0	a/0	0	c/2	4.6
exit 10	5.37	a-b/0.5	a-b/0.5	0	a/0	a/0	2	c/2	10.37
exit 12	2.53	a-b/0.5	a-b/0.5	0	a/0	a/0	2	b/1	6.53
14 – 15 km	1.57	b/1	b/1	0	a/0	a/0	2	b/1	6.57
18 - 19 km	2.38	b/1	b-c/1.5	0	a/0	a/0	1	b/1	6.88
exit 49	0.12	a-b/0.5	a-b/0.5	0.5	b/1	b/1	2	a/0	7.9
exit 90	0.42	a-b/0.5	a-b/0.5	1	b/1	b/1	2	a/0	5.62
95 - 100 km	2	b/1	c/2	1	a/0	a/0	1	a/0	6.42
exit 190	1.57	a/0	a-b/0.5	0	a/0	a/0	2	b/1	7
exit 194	2.12	a-b/0.5	a-b/0.5	0	a/0	a/0	2	b/1	6.12
exit 196	1.75	b/1	a/0	0	a/0	a/0	2	b/1	5.75

2. Metodou What, I byly provedeny simulace dopravních nehod s nebezpečnými látkami (které se daným místem reálně převážejí) pro více než 100 kritických míst (složité křižovatky, místa častých dopravních nehod a místa nehod, kde již došlo k velkým dopravním nehodám s nebezpečnými látkami) [12,185]. Uvedeme příklad pro D1 - Humpolec – exit 90. Sledovaný úsek, pro který byly simulovány dopady dopravní nehody s přítomností nebezpečných látek, se nachází na 90 km dálnice D1, obrázek 41. Sledovaná oblast se nachází v kraji Vysočina, který je význačný především proměnlivými meteorologickými podmínkami. Po pravé a levé straně ve směru na prahu se nachází průmyslové zóny, které zahrnují především sklady a distribuční centra. U nájezdu ve směru

na Brno je situovaná čerpací stanice pohonných hmot. V okolí celého dopravního uzlu se nachází doprovodná a izolovaná zeleň. V blízkosti se nachází obce Vystrkov a Hněvkovice, mezi nimiž je potok Hněvkovice. Předmětný obrázek také ukazuje místa konkrétních dopravních nehod s přítomností nebezpečných látek. Úsek byl vybrán proto, že zde sjíždějí kamiony z dálnice, jelikož v úseku 49 km – 90 km je průjezd dopravních prostředků s nebezpečnými látkami zakázán z důvodu ochrany vodní nádrže na řece Želivce, která zásobuje pitnou vodou Prahu a okolí.



Obr. 41. Dálnice D1 – exit 90 – Humpolec, červená – místa dopravní nehody s následkem smrti, modrá – místa dopravní nehody se zraněním [12].

Tabulka 36 obsahuje výsledky analýzy „Co se stane, když“ na křižovatce dálnice D1, exit 90 u Humpolce. V tabulce 36 rozlišujeme dva případy, a to dopady obyčejné dopravní nehody, které značíme DN, a dopady, které způsobí dopravní nehoda s přítomností nebezpečné látky, které označujeme NL. Pro simulaci dopravní nehody s přítomností nebezpečné látky jsme vybrali technický benzín. Dle [215] se jedná se o hořlavou kapalinu I. třídy nebezpečnosti. Jde o vysoce hořlavý materiál – páry mohou tvořit se vzduchem výbušnou směs. Vdechnutí do plic může způsobit zánět plic, který může mít fatální následky. Páry působí při vyšší koncentraci narkoticky. Místně odmašťuje a dráždí pokožku a dýchací cesty, způsobuje bolesti hlavy a žaludeční nevolnost. Dráždí sliznice a oči a je toxický pro vodní živočichy [215]. Kontaminace vody vede tudíž k jejich úhynům.

Tabulka 36. Výsledky analýzy „Co se stane, když“ na křižovatce dálnice D1 a exitu 90 u Humpolce. DN – dopady běžné dopravní nehody, NL - další dopady dopravní nehody s přítomností nebezpečné látky (pohonné hmoty - benzin, nafta); dopady jsou uvedeny v časech 0, 3 a 12 hodin a 3 dny, přičemž čas 0 označuje čas vzniku dopravní nehody; symbol *** označuje, že nedošlo k dalšímu novému dopadu [190,191].

Chráněné aktivum	**Dopady na chráněná aktiva**
Životy a zdraví lidí	DN: 0h - úmrtí či zranění účastníků dopravní nehody, 3h***, 12h***, 3 dny ***. NL: 0h - úmrtí či zranění účastníků dopravní nehody; další úmrtí či poškození zdraví v důsledku rozletu úlomků při výbuchu, při požáru či vdechnutí výparů nebo kouře (oxid uhelnatý a oxid uhličitý) do plic

	(dochází k zánětu plic až vzniku rakoviny u osob v dosahu kouře). Vdechování nebezpečných rozkladných produktů i ve větší vzdálenosti působí vážná poškození zdraví, páry působí při vyšší koncentraci narkoticky; 3h – stále dochází k poškození zdraví při vdechnutí hustého černého kouře, 12h***, 3 dny ***.
Bezpečí lidí	DN: 0h - úlek řidičů v koloně, 3h – narůstající stres řidičů; narušení klidu v obytné části Humpolce a na objízdných trasách; narušení městské dopravy, 12h***, 3dny – nepříjemnosti spojené s omezením dopravy vlivem poškození komunikace. NL: 0h – úlek řidičů v koloně a obava z nažloutlého mraku a pronikavého dusivého zápachu; 3h – stres až panika; stres při evakuaci blízkých obytných částí Humpolce; ohrožení lidí přepravujících se městskou dopravou a železniční dopravou, 12h – přetrvávající narušení obytných částí na objízdných trasách, 3dny***.
Majetek	DN: 0h – poškození dopravní komunikace vlivem nehody (povrch vozovky, železnice a pilíře mostů), 3h – ztráta zisku v průmyslových zónách, 12h***, 3 dny ***. NL: 0h – poškození dopravní komunikace vlivem nehody (povrch vozovky, železnice a pilíře mostů) a škody způsobené výbuchem (se vzduchem tvoří páry benzínu i nafty výbušnou směs) a požárem; možný domino efekt - výbuch čerpací stanice v blízkosti postižené komunikace; v případě následného požáru pohonných hmot dochází k dalšímu poškození komunikace a železnice, 3h – další poškození majetku požárem, 12h – ***.
Životní prostředí	DN: 0h – kontaminace povrchové vody (Hněvkovický potok) a půdy uniklými pohonnými hmotami, 3h – uhynutí fauny a flóry v kontaminovaných vodách a půdách, zhoršení ovzduší na objízdných trasách, 12h***, 3 dny – oslabení ekosystému vlivem kontaminace. NL: 0h – kontaminace povrchové vody (Hněvkovický potok), podzemní vody a půdy nebezpečnou látkou; kontaminace ovzduší výpary, 3h - uhynutí fauny a flóry v kontaminovaných vodách a půdách; zhoršení kvality ovzduší v důsledku zplodin z výbuchu směsi pohonných hmot se vzduchem i v širším okolí komunikace, 12h – zhoršení kvality ovzduší na objízdných trasách, zničení ekosystému vlivem úniku ropných látek. 3dny ***.
Infrastruktury a technologie	DN: 0h – výpadek postiženého úseku dálnice D1 (90 km) včetně městské dopravy, železnice, vlakové stanice Humpolec, která se nachází v blízkosti této komunikace, 3h - nefunkčnost postiženého úseku dálnice D1, přetížení objízdných tras, 12h***, 3 dny – poškození postiženého úseku vlivem dopravní nehody, poškození objízdných tras vlivem přetížení. NL: 0h – výpadek postiženého úseku dálnice D1 včetně městské dopravy, železnice, vlakové stanice Humpolec, 3h - nefunkčnost postiženého úseku dálnice D1, městské dopravy, železniční dopravy a přetížení objízdných tras, 12h - nefunkčnost postiženého úseku dálnice D1, přetížení objízdných tras, 3 dny ***. Ztráty zisků průmyslových zón. Poškození dodavatelských řetězců.
Nouzové služby	DN: 0h – snížení dostupnosti složek IZS, 3h – přetrvávající snížení dostupnosti složek IZS, 12h ***, 3 dny ***.

(policie, hasiči, zdravotníci)	NL: 0h – snížení dostupnosti složek IZS, 3h – stálé snížení dostupnosti složek IZS, 12h – dlouhotrvající snížení dostupnosti složek IZS, 3 dny ***.

Část dálnice D1 v uzlu Humpolec exit 90, který je na obrázku 42, vyžaduje objíždění daného úseku po místních komunikacích, což vždy vede ke komplikaci v případě přepravy nebezpečných látek. V úseku exit 49 – exit 90 je přeprava nebezpečných látek po dálnici D1 zakázaná kvůli ochraně vodní nádrže Želivky, která je zdrojem pitné vody pro Prahu a okolí. Proto je zde zavedena stálá objízdná trasa. Ve sledovaném případě je problém s navigací přepravců s nebezpečnými látkami na zavedenou objízdnou trasu; objížďky přes města Humpolec nebo Pelhřimov nejsou vyznačené.

Obr. 42. Dálnice D1 exit 90 u Humpolce.

Z tabulky 36 vyplývá, že v případě velké dopravní nehody s přítomností technického benzínu u Humpolce - exit 90 dojde k významným škodám na chráněných aktivech a k výpadku stálé objízdné trasy, která je důležitá zejména pro vozidla přepravující nebezpečné látky, jelikož na uvedeném sjezdu musí opustit dálnici z důvodu ochrany důsledku vodní nádrže Želivky, která se nachází mezi exit 49 a exit 90 a která zásobuje pitnou vodou Prahu a okolí. Problém je, že náhradní trasa není vyznačena.

3. Při dopravních nehodách s přítomností nebezpečných látek dochází k:
   - úmrtí přítomných osob nebo k poškození jejich zdraví nejen v důsledku dopravní nehody samotné, ale zejména v důsledku působení přítomné chemické látky, tj. v závislosti na jejich vlastnostech (lehčí nebo těžší než vzduch, hořlavá, výbušná, toxická atd.) a množství. Roli hrají též meteorologické podmínky při dané dopravní nehodě (vítr, inverze, déšť, mlha), konfigurace terénu (údolí, kopec, zatáčka), výskyt domino efektů, jejichž zdroje byly nalezeny u téměř všech sledovaných případů,
   - poškození majetku na zúčastněných vozidlech, a to nejen v důsledku dopravní nehody samotné, ale zejména v důsledku působení přítomné chemické látky, tj. v závislosti na jejich vlastnostech a množství. Roli hraje výskyt domino efektů, jejichž zdroje byly nalezeny u téměř všech sledovaných případů,
   - poškození komunikace v místě nehody, a to nejen v důsledku dopravní nehody samotné, ale zejména v důsledku působení přítomné chemické látky, tj. v závislosti na jejich vlastnostech a množství. Roli hraje výskyt domino efektů, jejichž zdroje byly nalezeny u téměř všech sledovaných případů,
   - přerušení dopravy na komunikaci, a to nejen v důsledku dopravní nehody samotné, ale zejména v důsledku působení přítomné chemické látky, tj. v závislosti na jejich vlastnostech a množství. Roli hraje výskyt domino efektů, jejichž zdroje byly nalezeny u téměř všech sledovaných případů,

- poškození okolí místa nehody v důsledku působení přítomné chemické látky, tj. v závislosti na jejich vlastnostech a množství. Určujícími faktory pro velikost škod jsou: vlastnosti podloží (propustné nebo nepropustné, přítomnost zvodní apod.); přítomnost objektů, ve kterých je velké množství lidí (nemocnice, školy, divadla, nákupní střediska apod.); přítomnost objektů zajišťujících např. dodávky vody pro lidi i průmysl (tj. např. podzemní vrty, vodárenské nádrže), potraviny (pole se zemědělskými produkty, ovocné stromy apod.); přítomnost objektů, které mohou být zdrojem domino efektů (čerpací stanice pohonných hmot, sklady nebezpečných látek, zpracovatelské závody s nebezpečnými látkami, obchody s nebezpečnými látkami apod.); přítomnost chráněných přírodních území; a přítomnost skládek nebezpečných odpadů,
- narušení dodavatelských řetězců, jestliže dopravní nehoda s přítomností nebezpečných látek poškodí nebo naruší provoz průmyslových a skladových objektů (průmyslové provozy, sklady kolem silnic). Roli hraje výskyt domino efektů, jejichž zdroje byly nalezeny u téměř všech sledovaných případů,
- Narušení hospodářství. Roli hraje výskyt domino efektů, jejichž zdroje byly nalezeny u téměř všech sledovaných případů.

4. Obnova poškozené komunikace i obnova okolí vyžaduje finance, materiál i personál, a hlavně čas. Někdy obnova trvá léta i desítky let – např. v r. 2004 v obci Kozlov u dálnice D1 byla při dopravní nehodě s přítomností nebezpečné látky kontaminována podzemní voda, což způsobilo kontaminaci studní a dnes, tj. třináct let po události, je voda ve studních v předmětné obci stále kontaminována. Tím je narušeno bezpečí lidí a jsou odčerpávány zdroje, síly a prostředky lidské společnosti, které by jinak bylo možno použít v sociální oblasti a pro rozvoj.
5. Je třeba zdůraznit zjištění uvedené v [191], a to nezájem veřejné správy o řešení dopravních nehod s přítomností nebezpečných látek.
6. Je třeba zdůraznit, že v ČR zatím nebyla tak velká dopravní nehoda s přítomností nebezpečných látek jako ve světě, kde v řadě případů byly postiženy oblasti s poloměrem několika kilometrů až více než desítka kilometrů kolem místa nehody [12, 191]. Přesto je třeba předmětnou problematiku lépe legislativně upravit a zvýšit kulturu bezpečnost v dané oblasti. Předmětný fakt ale to neznamená, že předmětná nehoda by se nemohla vyskytnout.
7. Protože místa dopravních nehod s přítomností nebezpečných látek jsou v zásadě proměnná, i když vykazují jistou kumulaci, která je daná vyšší zranitelností jistých míst na pozemních komunikacích, plány odezvy či krizové plány obsahující odezvu na velké dopravní nehody s přítomností nebezpečných látek, mohou být z důvodu hospodárnosti zpracovány jen pro vybraná místa. Jde především o místa na pozemních komunikacích, ve kterých dochází často k dopravním nehodám s přítomností nebezpečných látek, a zároveň o místa, v jejichž těsném okolí jsou objekty s velkým množstvím lidí nebo zdroje domino efektů, tj. nádraží, křižovatky ve městech aj., které lze identifikovat aplikací kontrolního seznamu [191].
8. S ohledem na zásady krizového řízení [194] plán odezvy musí obsahovat: schéma možného zasaženého území, ve kterém jsou vyznačeny objekty s velkým počtem lidí a objekty, které mohou být zdrojem domino efektů; scénáře dopadů dopravní nehody s přítomností nebezpečné látky v čase 0h a 3h od vzniku události zpracované metodou What, If [15]; konkrétní postupy spolupráce IZS a veřejné správy při odezvě; konkrétní postupy spolupráce s vlastníky a provozovateli objektů, a to s velkým počtem lidí a s těmi, jejichž objekty mohou být zdroji domino efektů; postup a způsob provedení vyhlášení ukrytí, popř. evakuace; a způsob návrtu do normální situace. Vzhledem k tomu, že dopravní nehody představují mobilní zdroj rizik a sestavení konkrétního plánu odezvy není triviální záležitost při požadavku, aby výsledek měl jistou vypovídací schopnost a byl správný), je třeba aplikovat postup: při každé větší dopravní nehodě s přítomností nebezpečné látky zajistit vzájemnou informovanost veřejné správy, která je správcem území, a IZS; zahájit odezvu a

kontinuální monitoring situace; zajistit ukrytí (popř. ve zvlášť kritických situací zajistit evakuaci) obyvatelstva v postiženém území; zajistit informovanost vlastníků a provozovatelů objektů s velkým počtem lidí a objektů, které mohou být zdrojem domino efektů a požádat je o zvýšenou opatrnost při provozu nebo až o odstavení nebezpečných technologií; a zajistit návrat do normální situace.

Zjištěné dopravní nehody s přítomností nebezpečných látek na českých silnicích ukazují, že se přepravují nejrůznější chemické látky: pohonné hmoty, vysoce hořlavé látky, kyselina dusičná, kyselina sírová, kyselina mléčná, kyselina fosforečná, dusičnany, fosforečnany zinku, manganu a niklu, hydroxid draselný, styrén, kapalný chlór, plynný argon, formaldehyd, asfalt, vápno, práškové PVC aj. [12,185]. Celkem je dopravních nehod s přítomností nebezpečných látek stovky ročně a vyčíslené škody na majetku spojené se znehodnocením nebezpečné látky chápané jako zboží s nimi spojené dosahují stovky miliónů. Další náklady souvisí s odezvou (často je nutno nebezpečnou látku přečerpat, což vyžaduje speciální zařízení a technologie), úklidem, obnovou komunikace a s přerušením dodavatelských řetězců a zastavením osobní dopravy [185]. Předmětné dopravní nehody jsou doprovázeny lehčími či těžšími zraněními osob i úmrtími, škodami na komunikacích a majetku v okolí silnic i škodami na životním prostředí.

Selhání objektů silniční dopravní infrastruktury

Mosty a tunely jsou důležitými prvky dopravní infrastruktury, jak silniční, tak železniční, a proto je třeba dbát o jejich bezpečnost a pro případy jejich závažného selhání mít připravena náhradní řešení. Nuselský most je z dopravního hlediska velmi významnou stavbou. Je součástí důležité dopravní tepny hlavního města Prahy spojující Karlov s Pankrácem. Je unikátní nejen svým nadčasovým designem, ale také využitím. Vrchní část mostu využívá automobilová doprava, uvnitř mostu je tubus pro provoz metra. Kvůli velké dopravní vytíženosti a geografické poloze by v případě výskytu velké pohromy došlo k rozsáhlým nepřijatelným dopadům na chráněná aktiva.

Zemětřesení je jedna z pohrom, která často boří mosty [216], a proto byl most podroben hodnocení. Z dostupných pramenů bylo zjištěno, že v době výstavby bylo zvažováno zrychlení spojené se zemětřesením rovné $1.76\ \mathrm{m \cdot s^{-2}}$ a nebyl brán v potaz příspěvek od zemětřesení k celkovému zatížení [217-219].

Pro kontrolu bylo spočteno seismické ohrožení Prahy pomocí katalogu zemětřesení a postupu, který je používán pro jaderná a podobná důležitá technická díla [220-222] v ČR a ve světě. Vyšla hodnota 5.9^{o} MSK-64, které současně platný Eurokód 8 [223] přiřazuje hodnotu zrychlení $3.76\ \mathrm{m \cdot s^{-2}}$, což je hodnota podstatně vyšší, než byla zvažována v době výstavby mostu. Z pohledu dnešního poznání je zřejmé, že most není tak odolný, jak je třeba dle současných normativních požadavků. I když připustíme jisté bezpečnostní rezervy, technické úpravy a modernizace mostu, tak je stejně třeba počítat s příslušným rizikem, a proto je provedena identifikace dopadů silného zemětřesení na most metodou What If, tj. je zváženo silnější zemětřesení než to, na které byl most projektován.

Výsledky rekognoskace území v okolí mostu, které by bylo postiženo prolomením mostu, jsou na obrázku 43. Okamžité dopady velkého zemětřesení jsou uvedeny v tabulce 37.

Z tabulky 37 vyplývá, že zemětřesení způsobí vysoké škody na životech a zdraví lidí nacházejících se na mostě a v jeho bezprostředním okolí. Především pod mostem bude situace kritická. Nejčastějšími příčinami úmrtí budou zasažení uvolněnými částmi mostu a předměty nacházející se na něm. Z pohledu bezpečí lidí a veřejného blaha sehraje velkou roli panika a stres, které postihnou účastníky události. Pod mostem se nachází benzínová pumpa, kde hrozí nebezpečí výbuchu, požáru a rozptylu nebezpečných látek, sídlí zde firmy a restaurace, v provozu jsou dvě větší parkoviště. Ztráty na majetku budou ve vymezené oblasti velmi

vysoké. V přímém poškození v souvislosti s poškozením životního prostředí budou park Folimanka a potok Botič.

Obr. 43. Území postižené prolomením mostu při extrémním zemětřesení s vyznačenými objekty: 1-park Folimanka; 2-potok Botič; 3-sportovní hala Folimanka; 4-dětské hřiště; 5-benzinová pumpa Agip; 6-podchod pod železniční tratí; 7-tramvajová dráha; 8-železniční dráha; 9-GPS center Garmin; 10-kancelářská budova; 11- kancelářská budova; 12-Sport bar Time;14-kancelářská budova Folimanka; 15-penzion Beta; 16-parkoviště 17-parkoviště [224].

Tabulka 37. Dopady způsobené velkým zemětřesením [224].

Chráněné aktivum	**Možné dopady**
Životy a zdraví lidí	- úmrtí nebo vážné zranění osob vyvolané selháním mostu (vážným poškozením až prolomením) - ztráty na životech či poranění v důsledku dopravní havárie v bezprostřední blízkosti mostu - poranění nebo úmrtí obyvatel zasažených uvolněnými částmi mostu, především v místech dětského hřiště, sportovní arény Folimanky a dalších budovách v oblasti pod mostem - úmrtí nebo vážné zranění osob v důsledku výbuchu čerpací stanice nacházející se pod Nuselským mostem
Bezpečí lidí	- panika, stres, šok ze zemětřesení nebo havárie - psychické zhroucení u obyvatel poškozených oblastí
Majetek	- poškození majetku osob nacházejících se na mostě nebo v jeho okolí (auta na přilehlých parkovištích, čerpací stanice, budovy nacházející se pod mostem) - poškození samotného mostu nebo přilehlé silnice - poškození objektů pod mostem zasažených úlomky padajícími z poškozeného až prolomeného mostu
Veřejné blaho	- neklid mezi občany, narušení veřejného pořádku
Životní prostředí	- devastace parku Folimanka nacházejícího se pod mostem - zamoření ovzduší prachem

	- přímé znečištění potoka Botiče v důsledku napadaných úlomků a unikajících látek z blízké čerpací stanice
Infrastruktury a technologie	- přerušení provozu metra a automobilové dopravy na mostě a v přilehlých oblastech - přerušení tramvajové a železniční dopravy nacházející se pod mostem - vznik kongescí přilehlých dopravních obslužností - narušení elektrického vedení, porušení objektů v bezprostřední blízkosti

Vzhledem k tomu, že Nuselský most představuje páteřní dopravní tepnu Prahy, je velmi pravděpodobné, že dojde k omezení hromadné i osobní dopravy v celém městě. Přerušena bude doprava nejen na mostě (metro, automobily), ale také pod ním, kde se nachází tramvajová a železniční trať. Kongesce budou vznikat po celém území hlavního města. Proto byla navržena opatření pro zvládnutí dopadů velkého zemětřesení (tabulka 38) a plán řízení rizik pro případ výskytu velkého zemětřesení (tabulka 39).

Tabulka 38. Obecná opatření pro zvládnutí dopadů extrémního zemětřesení [224,225].

Očekávané nepřijatelné dopady	**Opatření**
Uvolnění částí mostu	- technická opatření ochranného charakteru - včasné varování - rychlá reakce nouzových služeb
Stres a panika	- plán komunikace s veřejností
Výbuch benzinové pumpy	- technická opatření ochranného charakteru - rychlá odezva - zabránění šíření požáru do okolí
Přerušení dopravy	- technická opatření - zajištění náhradní dopravní obslužnosti
Zvýšená kriminalita	- nasazení městské policie pro udržení veřejného pořádku

Z tabulky 38 vyplývá, že v důsledku výskytu silného zemětřesení je velkou hrozbou porušení statiky mostu a pád částí mostu do Nuselského údolí. Je třeba provést technická opatření k zrychlení obnovení stability mostu. Pro snížení ztrát a škod pomůže též včasné varování obyvatel na mostě a pod ním. Proto je nutná příprava veřejné správy na to, že v případě výbuchu benzinové pumpy pod mostem, a s tím spojeného požáru a rozptylu nebezpečných látek je třeba rychle zajistit ukrytí lidí.

Zcela jistě dojde k přerušení dopravy na mostě a v jeho okolí, a to jak dopravy silniční tak železniční. Musí být připraven plán náhradní dopravy a jasně stanovené objízdné trasy. Je třeba počítat s tím, že po výskytu velké pohromy bude zvýšená kriminalita. Plán řízení rizik pro případ výskytu velkého zemětřesení je uveden v tabulce 39.

Tabulka 39. Plán řízení rizik pro případ zemětřesení [224,225].

Oblast rizika	**Popis rizika**	**Pravděpodobnost výskytu Dopady**	**Opatření na zmírnění rizika**
Organizace odezvy	Velké časové zpoždění	Pravděpodobnost: malá Dopady: velké	1. Pravidelné cvičení IZS 2. Příprava a trénink speciálních plánů dle

	nouzových služeb (IZS)		charakteru dopadů zemětřesení
Veřejná správa	Velké časové zpoždění v realizaci varování (selhání veřejného rozhlasu, sirén, apod.)	Pravděpodobnost: malá Dopady: velké	1. Příprava a trénink speciálních plánů pro případ zemětřesení 2. Připravený text k provedení varování 3. Pravidelné testování rozhlasu 4. Varování hluchých obyvatel
Špatná reakce veřejné správy	Zpožděná evakuace	Pravděpodobnost: malá Dopady: velké	1. Zajistit výcvik veřejné správy 2. Pravidelně procvičovat součinnost veřejné správy a IZS 3. Zajistit pravidelné kontroly obecních úřadů, zda jsou připraveny na evakuace, tj. zda mají smlouvy na objekty, do kterých provedou evakuaci nebo autobusy kterými provedou evakuaci. 4. Zajistit informovanost obyvatel.
Personální	Ztráta zkušených pracovníků odchodem do zahraničí	Pravděpodobnost: střední Dopady: velké	1. Nabídka perspektivního zaměstnání 2. Finanční a firemní benefity

Výsledky ukazují, že je třeba se v praxi zabývat řízením bezpečnosti Nuselského mostu a provést opatření a činnosti vedoucí k zajištění objektu. Z dopravního hlediska musí být připraven plán náhradní dopravy a jasně stanovené objízdné trasy.

V práci [224] se autor také zabýval také teroristickým útokem na Nuselský most. Zajímavá je matice odpovědnosti, která je uvedená v tabulce 40, která byla sestavena na základě platné české legislativy.

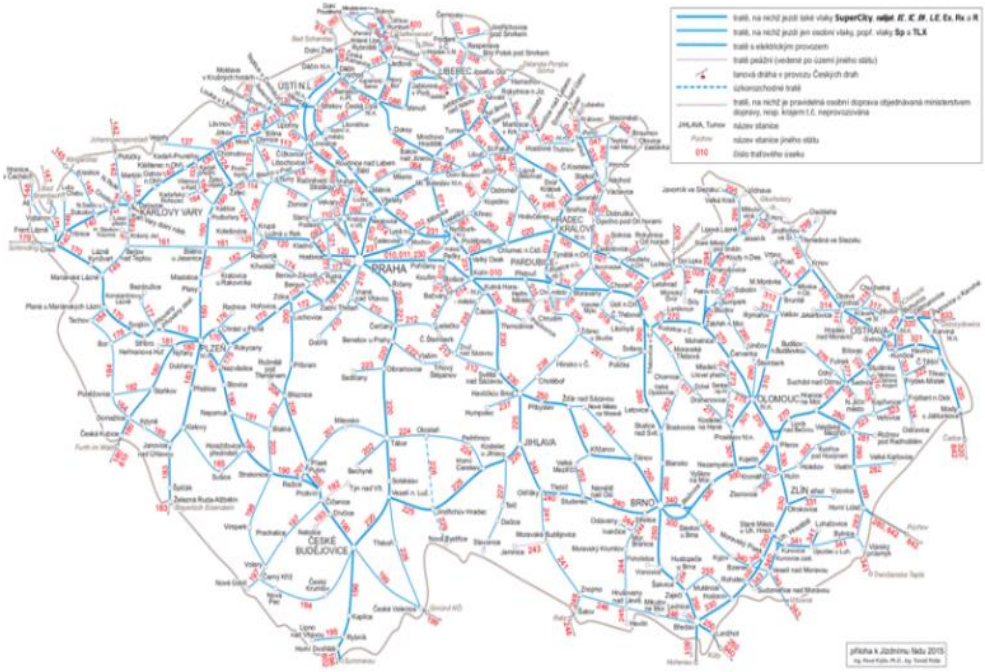
Tabulka 40. Matice odpovědnosti pro odvrácení teroristického útoku [224]. P – primární odpovědnost, Si jsou sekundární odpovědnosti.

Odpovědnost / Činnosti	**Předseda Parlamentu**	**Předseda vlády**	**Primátor hlavního města Prahy**	**Starosta městské části Praha 4 (ORP)**	**Starosta Obce - Nusle**
Systém řízení bezpečnosti zahrnující	P	S1	S2	S3	S4

ochranu důležitých objektů proti teroristickému útoku					
Realizace monitoringu úrovně bezpečnosti	S4	S3	S2	S1	P
Správné rozhodování ve prospěch bezpečí a rozvoje občanů a státu v krátkodobém i dlouhodobém časovém intervalu	P	S1	S2	S3	S4

5.9.4.2. Doprava železniční

Doprava na železnici závisí jak na technické infrastruktuře a vozidlech, tak na napájecí soustavě, a na jejich řízení. Železniční napájecí soustava (trakční soustava) je soubor technických zařízení, která slouží k přenosu elektrické energie ze stabilní soustavy do drážních vozidel. Napájecí soustavy lze rozlišovat podle: technického provedení – trolejové vedení jedno-, dvou- nebo třívodičové, napájecí kolejnice; a napětí a druhu proudu – střídavý jedno- nebo třífázový, stejnosměrný; v případě střídavého proudu se uvádí i jmenovitá frekvence. Obrázek 44 ukazuje rozložení železničních tratí v ČR.



Obr. 44. Železniční tratě v ČR [226].

Běžné dopravní nehody

Na základě posouzení potenciálu působení jednotlivých pohrom náležících do souboru pohrom, který označujeme All-Hazard-Approach [8], na drážní provoz a z údajů v databázi dopravních nehod, která zahrnuje jak údaje z ČR, tak údaje ze světa od r. 1815 (tj. více než 3000 dopravních nehod) [12] jsou odvozeny hlavní příčiny vzniku dopravních nehod a skoro-nehod v provozu drah [227] následující:

1. Technické – spojené s dopravním prostředkem – lokomotiva, vagony:
   - chyba v návrhu nebo při konstrukci drážního vozidla (chybná konstrukce z pohledu stability lokomotivy či vagonů, nevhodné umístění palivové nádrže nebo silového vodiče na svorkovnici v lokomotivě - zřejmé možnosti elektrického zkratu apod.),
   - špatná údržba lokomotivy či vagonů,
   - špatně provedená technická prohlídka drážních vozidel,
   - špatně provedená oprava drážních vozidel (např. lanoví ruční brzdy,
   - nesprávně naložené vagóny,
   - špatně zavřené dveře vagonů (
   - náhlá technická závada lokomotivy či některého z vagonů (poškození ložiska v kole, vysazení pohonu, směrového ovladače nebo jiného důležitého zařízení, výpadek klimatizace apod.),
   - nedostatek paliva nebo výpadek dodávky elektrického proudu,
   - selhání technického vybavení řídicího systému lokomotivy (výpadek přístroje měřícího rychlost, výpadek radiového spojení s dispečinkem apod.),
   - nefunkční zálohovaný systém v případě potřeby.
2. Technické – spojené s dráhou a nádražím:
   - umístění dráhy v území (velké stoupání, nedostatečná únosnost kolejového lože, ostré zatáčky, mnoho nechráněných přejezdů, vysoký a bujný porost snižující viditelnost apod.),
   - konstrukční chyba při stavbě nádraží (příliš krátký provozní prostor, umístění kolejí ve směru, ve kterém je vysoká budova, která snižuje rozhled strojvedoucího a posunovačů při změně směru drážního vozidla, často protivítr apod.),
   - stav kolejí (konstrukční chyba, nepořádek na nádraží, špatná údržba – nerovnosti, led, sníh, vybočení koleje, nalomená výhybka, nepřipevněné kolejnice na pražce apod.),
   - Neprovádění pravidelných prohlídek trati
   - špatně provedená pravidelná technická prohlídka trati (nezjištění nalomené výhybky),
   - neprovedení včasné opravy zjištěných závažných závad na trati či signalizačním zařízení
   - chybí signalizační zařízení nebo má nedostatečný výkon
   - náhlá technická závada přístrojů v dispečinku (špatná údržba, selhání technického vybavení řídicího systému na dispečerském stanovišti apod.)
   - rozmístění techniky pro obsluhu drážních vozidel (tankování paliva, vykládka a nakládka zboží, nástup a výstup lidí apod.),
   - fyzické zničení nádraží nebo kolejí (válka, loupežné přepadení, teroristický útok, …).
   - umístění vlaku na nesprávnou dráhu,
   - překážky na kolejích,
   - nedostatečné radiové vybavení nádraží,
   - nedostatek znalostí a zkušeností obsluhy nádraží (pracovníka navigujícího pohyb drážních vozidel po kolejích v prostoru nádraží),
   - nefunkční varovný systém na nádraží udávající minimální bezpečnou vzdálenost jednoho vlaku od druhého, když jsou na jedné koleji.
3. Řízení drážního provozu – organizační příčiny:
   - špatné postavení vlakové cesty,

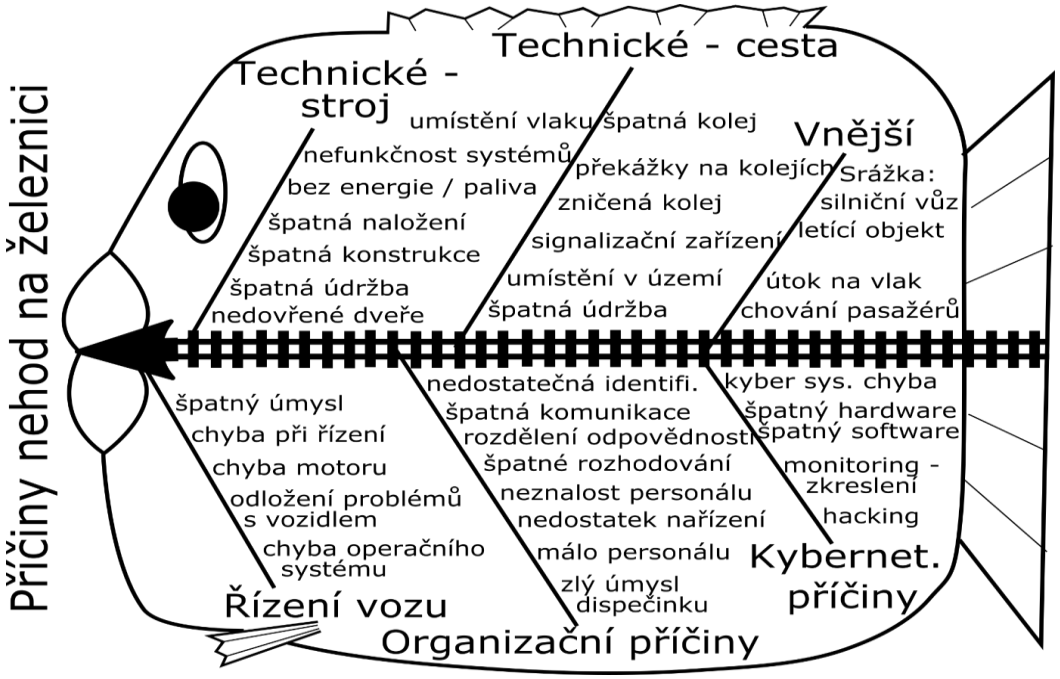
- nespuštění závor či zvukového signálu před příjezdem vlaku ke křížení trati se silnicí či cestou,
- ponechání překážek na trati
- nedostatečné označení tratí,
- nedostatečné označení křížení tratí se silnicí či polní cestou
- navedení vlaku na nesprávnou kolej při vjezdu do nádraží, jízdě i výjezdu z nádraží (kolize vlaků, vykolejení apod.),
- výpravčí vyhodnotil špatně zprávu od policie a zastavil dopravu na jiné trati, než na té, na které byla překážka
- nepředání zprávy o požáru na určité trati strojvedoucím příslušných vlaků
- špatné zvážení meteorologických podmínek (chybné informace pro strojvedoucího),
- odeslání chybných instrukcí vlakům kvůli selhání řídicího systému na dispečerském stanovišti (např. v důsledku výpadku elektrického proudu, výpadku PC apod.),
- odeslání chybných instrukcí vlakům kvůli chybě nebo neznalosti dispečera,
- zmatek na dispečerském stanovišti (špatné informace strojvedoucím, zpožděné informace apod.),
- nedostatek pozemního personálu na nádraží (srážka vlaků apod.),
- špatná údržba či osvětlení nástupišť,
- špatná komunikace mezi výpravčími při stavění cest vlaků
- nezabezpečení jízdy posunovaného dílu
- posunovači nebyli vybaveni červeným světlem
- posunovači nedostatečně vyškolení
- nezajištění střežení křižovatky dráhy a silnice při posunování vlaku
- chyba personálu na nádraží (při navádění vlaků, úklidu nádraží a kolejnic, údržbě nádraží a kolejnic apod.),
- špatná komunikace mezi dispečerským stanovištěm a firmami provádějícími opravu trati,
- špatně rozdělené odpovědností na dispečerském stanovišti,
- nedostatečná komunikace se strojvedoucími v obslužném prostoru,
- nedostatek znalostí a zkušeností obsluhy na dispečerském stanovišti,
- neexistence instrukcí pro podporu strojvedoucích, kteří se dostanou do nenadálých nouzových až kritických situací.

4. Řízení drážního provozu – kybernetické příčiny:
   - zkreslení údajů z monitorovací sítě (chybné instrukce strojvedoucím a od strojvedoucích, zmatek na dispečerském pracovišti apod.),
   - chybný software (nezvažuje všechny možné varianty možných provozních situací, z čehož plynou chybné instrukce pro strojvedoucí i personál),
   - nedostatečný hardware (špatné vyhodnocení dat, odeslání chybných instrukcí strojvedoucím v provozu z důvodu selhání PC, zpoždění zpráv apod.),
   - hackerský útok na řídící centrum vybavení dispečerského stanoviště.
5. Ovládání drážních vozidel:
   - chyba strojvedoucího při ovládání vlaku – např. nezareagování na zákaz jízdy za návěstidlo s návěstí zakazující jízdu, nedodržení rozhledových poměrů při špatné viditelnosti. (kvůli zdravotnímu stavu, únavě, chybné informaci z řízení drážního provozu, selhání kritického zařízení lokomotivy či jiného vozidla v důsledku špatné údržby, chybnému vyhodnocení situace – snížená rychlost a nedodržení časového rozvrhu a z toho plynoucí stress, náraz do překážky, vypnutí funkčního zařízení místo vadného, - výjezd a vjezd do nádraží, vykolejení, nepoužití zarážky při zastavení vlaku při posunování apod.),

- chyba strojvedoucího při hodnocení meteorologických podmínek (námraza, sněhové závěje, překážky na trati apod.),
- Chyba strojvedoucího při výskytu neočekávaných podmínek (kvůli nedostatečné přípravě na zvládnutí nouzových podmínek – vichřice, snížená viditelnost apod.),
- chyba strojvedoucího (nepoužití nouzového volání apod.),
- chyba strojvedoucího při přípravě lokomotivy k jízdě (špatné prostudování instrukcí před jízdou – např. ohledně nákladu, špatně nastavený měřič rychlosti, mylně nastavené výchozí údaje pro jízdu, např. při přepravě drahého zboží apod.),
- chyba strojvedoucího při ovládání radiostanice,
- chybná spolupráce strojvedoucího, vlakvedoucích a dalších členů posádky,
- chyba strojvedoucího při ohlašování (použití chybného volacího znaku vlaku - malý rozestup mezi vlaky),
- požár nebo dým v lokomotivě, vagonech pro cestující, v nákladových prostorech nebo požár motoru,
- špatný úmysl strojvedoucího (změna rychlosti, nereagování na pokyny z dispečerského pracoviště nebo od okolních vlaků apod.),
- neznalost strojvedoucího (neumí postupy pro ovládání vlaku při nenadálých nouzových až kritických situací – překážka na trati aj.).

6. Útok na vlak:
   - raketa / střela z jiného vlaku či z objektu ležícího mimo trať (házení kamenů či jiných těžkých předmětů z mostu nad tratí na vlak aj.),
   - poškození železničního svršku nebo náspu,
   - protiprávní čin ve vlaku,
   - špatný úmysl dispečera,
   - špatný úmysl obsluhy na nádraží (pracovníka navigujícího pohyb vlaku na nádraží),
   - srážka vlaku s letadlem či jiným letícím předmětem.
7. Legislativní:
   - chybí předpisy pro zabránění postavení špatné cesty na nádražích,
   - chybí přesné instrukce pro provádění údržby vlaku, železničního svršku, náspu a okolí tratě,
   - chybí texty srozumitelných a přesných instrukcí pro komunikaci mezi strojvedoucím a dispečerským pracovištěm,
   - postupy pro provádění technické kontroly drážních vozidel – způsob a časový harmonogram
   - absence jednotného systému označení železničních přejezdů, sloužícího k jednotné identifikaci železničních přejezdů z pohledu dráhy železniční a silniční topologie, umožňující přímé informování
   - absence požadavků, podle kterých vozmistr posoudí zatížení kol, zda je úměrné
8. Jiné:
   - nevhodné chování cestujících při nastupování, jízdě či vystupování z vlaku (nerespektování pokynů, nekázeň, špatná péče o pohyb dětí ve vlaku),
   - podmáčení nebo jiné poškození náspu,
   - chování řidičů silničních vozidel na křížení silnice s dráhou (nerespektování značení, zvukového signálu i zábran

Diagram rybí kosti (Fisbone diagram) zobrazující základní kategorie příčin dopravních nehod vlaků je uveden na obrázku 45. Z obrázku 45 je zřejmých šest příčin dopravních nehod, které se v čas opakují. Velice často dochází ke kombinaci technické chyby a lidské chyby, a to zvláště při rozhodování v naléhavých případech a při řízení zásadních činností. Je to způsobeno i tím, že ve vzdělávacím procesu chybí předávání znalostí a výcvik pro zvládání kritických situací.



Obr. 45. Zdroje dopravních nehod na železnici [227].

Dopravní nehody na železnici s nebezpečnými látkami

Dopravní nehody s přítomností nebezpečných látek na železnicích byly předmětem samostatného výzkumu, jehož výsledky jsou shrnuty v práci [185]. Dopravní nehody s přítomností nebezpečných látek jsou velmi nebezpečné pro okolí, jak ukazuje pět příkladů z naší databáze [12], která obsahuje 4080 dopravních nehod s přítomností nebezpečných látek na železnici z let 1996-2010:

1. Dopravní nehoda Langenweddingen (NDR, 6. 7. 1967). V blízkosti Magdeburku, poté co kvůli přetíženému kabelu selhalo fungování železničních závor, se na přejezdu srazil místní vlak s nákladním autem vezoucím 15 000 l lehkého benzinu a vzplanul. 94 osob bylo zabito, z toho 44 byly děti na prázdninách [228], obrázek 46.

Obr. 47. Dopady dopravní nehody v Langenweddingen (Německo 6. 7. 1967) [228].

2. Dopravní nehoda Kingman (Arizona, USA, 5. 7. 1973). Během přečerpávání propanu z vagonu do zásobníku na železniční vlečce se snažil pracovník dotáhnout netěsnící připojení tím, že udeřil na klíč kladivem, což způsobilo jiskru, která vyvolala požár. Požár ohřál cisternu a zvýšil tlak v cisterně. Tlak v cisterně dosáhl mezní hranice a cisterna explodovala (BLEVE). 100 tun propanu, 13 mrtvých, obrázek 48 [229,230].

Obr. 47. Dopady dopravní nehody v Kingman (Arizona, USA, 5. 7. 1973) [229,230].

3. Dopravní nehoda Alberton (Montana, USA, 11. 4. 1996). Při železniční nehodě vlaku, který sestával z 3 lokomotiv, 35 nenaložených a 36 naložených vagonů, z nichž 25 bylo označeno velkými bezpečnostními značkami označujícími přítomnost nebezpečné látky, došlo k vykolejení 19 vagonů, z nichž 6 obsahovalo nebezpečné chemikálie. Čtyři vagony obsahovaly chlór, tři zůstaly neporušeny a z jednoho vagonu podle odhadu uniklo 130 000 liber chlóru. Z dalšího vagonu vyteklo 17 000 galonů draselné soli kyseliny p-hydroxybenzoové a z třetího uniklo něco pevného chlorečnanu sodného. Postiženo bylo nejméně 350 osob, jedno úmrtí a přes 1000 osob bylo evakuováno. Státní silnice byla na 19 dní uzavřena a kamiony musely používat 200 mil dlouhou objížďku, obrázek 48 [231].

Obr. 48. Dopady dopravní nehody v Alberton (Montana, USA, 11. 4. 1996) [231].

4. Dopravní nehoda Graniteville (Severní Karolina, USA, 6. 1. 2005). Vlak s cisternami plnými chlóru se srazil s jiným vlakem a odhadem 11 500 galonů plynného chlóru se okamžitě uvolnilo do ovzduší. Způsobilo smrt 9 osob. Primární příčinou smrti těch, kteří zemřeli na místě, byla asfyxie [232-233]. Tato událost představuje jednu z největších železničních katastrof s únikem nebezpečných látek v historii USA. K úniku chlóru došlo v noci 6. ledna 2005 při srážce dvou vlaků v Graniteville, South Carolina. Příčinou tragédie byla lidská chyba. K výhybce obsluhované vlakovým dispečerem se blížil vlak jedoucí rychlostí 76 km/h a převážející 42 nákladních vagónů a cisteren, z nichž některé byly naplněny nebezpečnými chemickými látkami, mimo jiné chlórem, hydroxidem sodným a kresolem. Obsluha zapomněla přepnout výhybku a nasměrovala tak omylem přijíždějící vlak s cisternami přímo na odstavnou kolej, kde se v tu chvíli nacházel jiný nákladní vlak. Došlo k přímé kolizi, jejímž výsledkem bylo nejen vykolejení obou lokomotiv, šestnácti nákladních vozů z přijíždějícího vlaku a jednoho vozu z odstaveného vlaku, ale též protržení cisterny s chlórem, ze které uniklo 90 tun jedovatého plynu, obrázek 49. Další dvě byly poškozeny. K utěsnění cisterny byla pracovníky

Obr. 49. Dopady dopravní nehody Graniteville (Severní Karolina, USA, 6. 1. 2005) [232-234].

použita dočasná záplata a veškerý její obsah byl přečerpán. V době havárie bylo polojasno, vál jižní až jihozápadní vítr o rychlosti 2 m/s. Teplota vzduchu se pohybovala kolem 12 °C. Při nehodě zemřelo devět lidí. Jeden z nich zemřel na následky svých zranění, zbylých osm zemřelo po nadýchání se jedovatých par chlóru. Téměř 250 lidí se chlóru nadýchalo a muselo být ošetřeno v nemocnici. V okruhu o poloměru jeden kilometr od neštěstí bylo evakuováno 5 400 okolních obyvatel na dobu dvou týdnů, kdy chemické jednotky prováděly dekontaminaci okolí. I během této nehody došlo k několika chybným krokům. Reakce na katastrofu ukázaly rozdíly v připravenosti místních lidí a potřebu zlepšit postupy správních úřadů. Přestože se zde lidé setkávají s chlórem denně, nevědí, jak v případě nehody reagovat. Železnice nahlásila havárii později o více než hodinu po úniku chlóru. Jeden ze zasahujících z místního oddělení dobrovolných hasičů reagoval na vlakové neštěstí a následné uvolnění chlóru bez osobních ochranných prostředků. Systém nouzových telefonů byl aktivován až několik hodin po neštěstí. Zóna určená pro evakuaci byla nedostatečná. Chlór bylo možné cítit i 2.5 kilometru od místa nehody. U jedné ženy, která

se po čtyřech dnech dostavila s dýchacími potížemi k lékaři, byla chybně stanovena diagnóza. Pomocí antibiotik byla léčena na zápal plic. Až po několika dnech její obvodní lékař pochopil, že její problémy jsou způsobeny nadýcháním se chlóru [232-234].

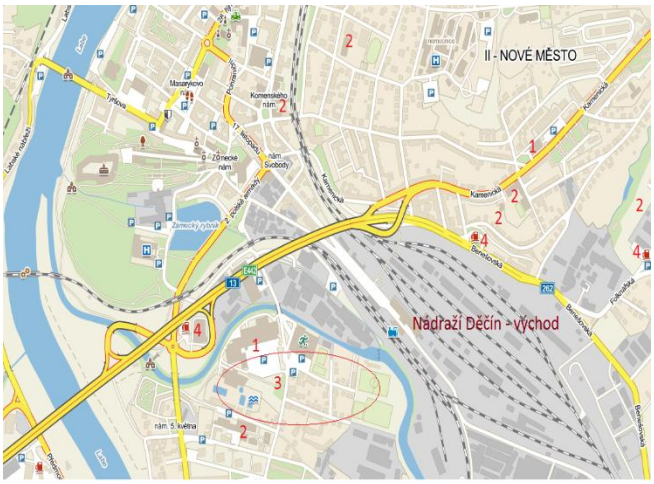
5. Dopravní nehoda ve Lvově (Ukrajina, 16. 7. 2007) [235,236]. Při železniční nehodě vykolejila část cisteren s obsahem bílého fosforu. Převrátilo se 15 vagonů z celkového počtu 58 a 6 z nich začalo hořet s vývinem těžkého dýmu oxidu fosforečného, který se rozšířil na území o ploše 90 km^2. Požár zasáhl 14 okolních vesnic s cca 11 000 obyvateli. Bylo hospitalizováno více než 140 lidí a 815 lidí bylo evakuováno.

Obr. 50. Dopady dopravní nehody ve Lvově (Ukrajina, 16. 7. 2007) [235,236].

Studiem dopravních nehod na železnicích s přítomností nebezpečných látek bylo zjištěno:

1. Dopravní nehody s přítomností nebezpečných látek na českých železnicích ukazují, že se přepravují nejrůznější chemické látky: hořlavé tuhé látky, samozápalné látky, žíravé látky, jedovaté látky a jiné nebezpečné látky a předměty. Z databáze [12] vyplývá, že nejčastěji přepravované nebezpečné látky jsou látky kapalné, kterých se nejvíce převáželo v roce 2007, a to 131 druhů. Následují látky plynné, kterých se v roce 2007 převáželo 24 druhů, a na třetím místě jsou látky pevné, kterých se nejvíce převáželo v roce 2008, a to 25 druhů. Celkem se během let 2007 až 2010 převezlo 402 druhů látek kapalných, 71 druhů látek plynných a 54 druhů pevných látek. Z procentuálního hlediska je: 76% látek kapalných, 14% plynných a 10% pevných látek. První analýzy obsahu databáze ukázaly shodu s výsledky získanými ve vyspělých zemích, a to, že k dopravním nehodám s přítomností nebezpečných látek dochází i tehdy, když strojvedoucí dodržují dopravní předpisy. Na jejich vzniku se podílí: stav vozidla, stav komunikace, způsob řízení přepravy na komunikaci, technická závada na vozidle, meteorologické podmínky, jiné vozidlo, chodec nebo zvíře a řidič vozidla.
2. Dopravní nehody s přítomností nebezpečných látek na železnicích se udály většinou na nádražích. Nebezpečné látky zjištěné při těchto dopravních nehodách byly jak ropné produkty, tak i další nebezpečné látky jako benzen, formaldehyd a další hořlavé látky,

samozápalné látky, žíravé i jedovaté látky [185]. Proto uvádíme příklad simulace dopadů dopravní nehody pomocí metody What, If na nádraží. Analýza databáze [12] ukazuje, že na nádraží Děčín - východ, obrázek 51 došlo k několika dopravním nehodám s přítomností nebezpečných látek. Hodnocení ukázalo, že nejčastěji šlo o dusičnan draselný (téměř 200 krát), močovinu (150 krát), chlorečnan sodný (více než 100 krát), aromatické uhlovodíky (téměř 60 krát), formaldehyd (více než 30 krát), dusičnan amonný (30 krát)a kyselina fosforečná (téměř 30 krát). Mezi hlavní ropné produkty patří benzín, motorová nafta, topný olej, LPG (Liquefi ed Petroleum Gas), petrolej, parafín, mazut, asfalt a dehet. Jednotlivé produkty se významně liší svými vlastnostmi. Z podrobnějšího rozboru databáze je počet dopravních nehod s ropnými produkty následující: benzin více než 50 krát, nafta více než 60 krát, topný olej téměř 80 krát, LPG více než 50 krát, parafin více než 100 krát, dehet více než 20 krát a ropné produkty bez rozlišení více než 40 krát. Pro benzíny je vypracována celá řada bezpečnostních listů, které se liší tím, zda jde o tzv. technický benzín, bezolovnaté automobilové benzíny (Čepro, Česká rafinérská, Slovnaft, OMV), lakový benzín, lékařský benzín či benzínové rozpouštědlo. Pro analýzu What, If jsme vybrali technický benzín.



Obr. 51. Nádraží Děčín – východ a jeho okolí. Na obrázku jsou vyznačeny objekty s velkým množstvím lidí; nákupní zóna – 1; školy – 2; obytné a rekreační objekty 3; a nemocnice H, tj. místa, ve kterých jsou základní veřejná aktiva, tj. lidé. Kromě toho jsou vyznačeny i zdroje možných domino efektů, kterým jsou ve sledované oblasti čerpací stanice pohonných hmot – 4.

Na základě bezpečnostního listu zpracovaného podle nařízení (ES) č. 1907/2006 (REACH) technický benzín je: kapalná látka, barvy bezbarvé až nažloutlé, benzínová frakce (ropná), rozpouštědlová rafinovaná, lehká, nízkovroucí a modifikovaná frakce (číslo CAS: 92045-57-3, číslo EINECS: 295-438-4, UN: 3295, Kemlerův kód: 33, přepravní název - uhlovodíky kapalné) s příměsí benzenu (méně než 0.1 %, CAS: 71-43-2, EINECS: 200-753-7), která se v průmyslu používá jako rozpouštědlo. Podle směrnice 1999/45/ES jde o nebezpečnou látku, jejíž klasifikace je daná symboly: F; R11, Xn; R65, Xi; R36/38, N; R51, R53, R67. Rizikové věty: R11 Vysoce hořlavý. R 36/38 Dráždí oči a kůži. R 51/53 Toxický pro vodní organismy, může vyvolat dlouhodobé nepříznivé účinky ve vodním prostředí. R 65 Zdraví škodlivý: při požití může vyvolat poškození plic. R 67 Vdechování par může způsobit ospalost a závratě. Bezpečnostní věty: S 9 Uchovávejte obal na dobře větraném místě. S 16 Uchovávejte mimo dosah zdrojů zapálení – Zákaz kouření. S 33 Proveďte preventivní opatření proti výbojům statické elektřiny. S 45 V případě nehody nebo necítíte-li se dobře, okamžitě vyhledejte lékařskou pomoc (je-li možno, ukažte toto označení). S 53 Zamezte expozici - před použitím si obstarejte speciální instrukce. S 61

Zabraňte uvolnění do životního prostředí. Viz speciální pokyny nebo Bezpečnostní listy S 62 Při požití nevyvolávejte zvracení: okamžitě vyhledejte lékařskou pomoc a ukažte tento obal nebo označení. Látka je vysoce hořlavá a zdraví škodlivá: při požití může vyvolat poškození plic. Dráždí oči a kůži. Je toxická pro vodní organismy, může vyvolat dlouhodobé nepříznivé účinky ve vodním prostředí. Působí dlouhodobé a nepříznivé dopady na životní prostředí. Vdechování par může způsobit ospalost a závratě. Látka má omamné účinky a její páry tvoří se vzduchem při pokojové teplotě výbušné směsi. Výpary jsou těžší než vzduch. Když se dostane do kanalizace, tak tam způsobí škody výbuchy. Jde o karcinogenní látku, na kterou se vztahují R-věty 45 - 65, 11-45-46-48/23/24/25-65-36/38. Při každé větší dopravní nehodě s přítomností technického benzínu na nádraží Děčín - východ dojde ke kontaminaci ovzduší, vody a půdy v okolí nádraží, dojde k explozím v ovzduší a v kanalizaci. Jsou postižení zaměstnanci nádraží, přítomní na nádraží a občané nacházející se v okolí nádraží. Tlakovou vlnou, rozletem úlomků spojených s výbuchy a požárem jsou zasaženy vlaky na nádraží, budovy na nádraží a okolí nádraží. Čerpací stanice pohonných hmot v těsné blízkosti jsou zasaženy jak výbuchy, tak požáry a následně na nich může dojít i k explozi. Výsledky analýzy metodou What, If v první hodině po velké dopravní nehodě s technickým benzínem jsou v tabulce 41.

Tabulka 41. Dopady velké dopravní nehody s přítomností technického benzínu na aktiva v okolí nádraží Děčín – východ.

Chráněné aktivum	**Dopady na chráněná aktiva**
Životy a zdraví lidí	U zaměstnanců, lidí přítomných na nádraží a občanů nacházejících se v okolí nádraží usmrcení rozletem úlomků nebo velmi vážné poškození zdraví při vdechování, styku s kůží a při požití. Ve vzdálenějším okolí lidé utrpí šok po explozích doprovázených tlakovou vlnou doprovázenou zvukovými projevy. Velké množství lidí bude zasaženo v nákupních centrech, školách a nemocnici. Při požáru a výbuchu na čerpací stanici pohonných hmot úmrtí lidí v těsném okolí v důsledku rozletu úlomků, požáru a zadýmení okolí. Kvůli hustému černému dýmu bude nutná evakuace lidí až do vzdálenosti 5 km od nádraží, tj. ve sledovaném případě až nemocnice a školy.
Bezpečí lidí	Obavy a panika mezi lidmi na nádraží (stres z hustého černého dýmu, ze zmatku v okolí, z výbuchu na čerpací stanici pohonných hmot, ze zpoždění z důvodu výluky) a v okolí (z výbuchů, požárů a z hustého černého dýmu).
Majetek	Poškození železniční tratě (kolejiště, nástupiště, nádražní budova), poškození vlakových souprav, poškození okolních budov, i obytných. Další poškození při požáru a výbuchu na čerpací stanici pohonných hmot na nádraží a v okolí čerpací stanice pohonných hmot.
Životní prostředí	Kontaminace ovzduší, vody a půdy, a poškození fauny a flóry v těsném okolí. Další poškození při požáru a výbuchu na čerpací stanici pohonných hmot.
Infrastruktury a technologie	Výpadek elektřiny, postiženého úseku železnice a okolních komunikací. Snížení dostupnosti složek IZS v důsledku odezvy na dopravní nehodu na nádraží, požár a výbuch čerpací stanice pohonných hmot, dopravní nehody v okolí nádraží.

	Snížení obslužnosti obyvatel v širším okolí nádraží. Zastavení dodávek vody pro občany a služby kvůli zvýšené spotřebě vody na hašení požárů. Snížení dostupnosti zdravotní péče a dalších veřejných služeb. Zatížení obecního úřadu a dopravních služeb, které musí zajistit evakuaci občanů a hlavně lidí z nemocnic, škol a nákupních center. Nutnost zavedení speciálních opatření ve školách, nemocnici a veřejných budovách (nevětrat, utěsnit okna) dokud se neprovede evakuace. Ztráta zisku vlakových společností vlivem omezení železniční dopravy.

Z tabulky 41 vyplývá, že extrémně velké dopady nastanou, když na čerpací stanici pohonných hmot nacházející se severně od nádraží (číslo 4 na obrázku 46) dojde k požáru a výbuchu. Dopady postihnou objekty s velkým počtem lidí – školy, nemocnice a nákupní centra. Místní šetření provedené v objektech s velkým počtem lidí kolem nádraží Děčín východ [237], při kterém byly položeny tři otázky - Co budete dělat při dopravní nehodě na nádraží s přítomností velmi nebezpečné látky? - Víte, jak se ochráníte a jak ochráníte osoby, za něž jste odpovědní? - Máte plán evakuace nebo plán ukrytí? – Z odpovědí bylo zjištěno, že objekty s předmětnou nouzovou situací nepočítají, tj. nemají plány ukrytí, ani plány evakuace; spoléhají, že ochranu lidí zajistí IZS.

3. Z vyhodnocení výše uvedených výsledků simulací a z výsledků simulací vyplynuly stejné závěry, jako jsou uvedené u dopravních nehod s nebezpečnými látkami na silnicích.
4. V rámci výzkumu, popsaného v práci [185] byla provedena inspekce na nádraží v Lovosicích, kde se dopravní nehody s nebezpečnými látkami vyskytují. Její výsledek je velmi varující: podle dokumentace na nádraží si provozovatel nádraží a jeho nadřízené útvary existenci velké dopravní nehody sledovaného typu nepřipouští, a proto nemají ani představu o jejím rozsahu, dopadech, a krocích, které vyžaduje v daném případě odezva; nebyly nalezeny postupy pro varování zaměstnanců a cestujících nacházejících se v době předmětné nehody na nádraží; nebyl nalezen postup zásahu, který začnou ihned provádět zaměstnanci, ani plán evakuace cestujících z nádraží; byl nalezen pouze plán pro zdolávání požáru; nebyly nalezeny nutné ochranné pomůcky pro zaměstnance pro práci za podmínek ztížených přítomností nebezpečné látky; nebyly nalezeny pokyny pro informování veřejné správy atd. Byla nalezena pouze instrukce, že v případě mimořádné události na nádraží je třeba volat IZS na linku 112. Na základě následného místního šetření na obecním úřadu, provedeného autorkou této práce ve spolupráci s autorkou práce [2386], bylo zjištěno, že veřejná správa se problematikou ochrany obyvatel v případě velké dopravní nehody s přítomností agresivní nebezpečné látky na nádraží Lovosice nezabývá a spoléhá na IZS, a to i při evakuaci obyvatel v okolí nádraží. ***Proto je třeba zvýšit kulturu bezpečnosti na nádražích a mít k dispozici alespoň plán řízení rizik.***

Na základě uvedených příkladů i závěrů práce [185] je zřejmé, že důsledky velké dopravní nehody na železnici s přítomností nebezpečné látky mohou být fatální. Z analýzy české i evropské legislativy, která je provedena v předmětné souvislosti, vyplývá velká chaotičnost. Příkladem je paradox, dle kterého u podniků spadajících pod direktivu SEVESO se v podniku hodnotí přítomnost jednotlivých vagonů či kamionů s nebezpečnou látkou, ale jakmile opustí území podniku, tak mohou stát na seřaďovacím nádraží v libovolném počtu a z nich vagony tvořený vlak se pak může pohybovat kudy libo; a stejné je to u kamionů. Jediným případem, kdy je plošně kontrolován transport nebezpečných látek je transport odpadů (zákon č. 185/2001 Sb.).

Řízení bezpečnosti v železniční dopravě

V rámci železniční dopravy je základním dokumentem účely bezpečnosti Směrnice Evropského parlamentu a Rady 2004/49/EC (Směrnice o bezpečnosti železnic) [239]. Uvedená

směrnice vedle systému řízení bezpečnosti zavádí i společné bezpečnostní cíle (CST – Common Safety Targets) a společné bezpečnostní metody dle Prováděcího nařízení Komise (EU) 402/2013 (CSM – Common Safety Methods) [240]. Při jakékoliv technické, provozní a organizační změně je nutné změnu zdokumentovat, posoudit a odůvodnit její vliv na bezpečnost dle metodiky Drážního úřadu, jakožto drážní autority v ČR stanovené Ministerstvem dopravy, metodika je založená na CSM [240], tj. jde o analýzu rizik.

Část výše uvedené směrnice vztahující se k systému řízení bezpečnosti [241] byla v CŘ transponována do Vyhlášky číslo 376/2006 Sb., o systému bezpečnosti provozování dráhy a železniční dopravy a postupech při vzniku mimořádných událostí na dráhách [241]. Systém řízení bezpečnosti má dle této vyhlášky povinnost zavádět pouze provozovatel dráhy. Systém předpokládá pouze normální podmínky. Při tzv. mimořádných událostech se provede zastavení provozu. Mimořádné události (tj. nouzové situace v rizikovém inženýrství) se ohlašují Drážnímu úřadu, který události vyšetřuje a je-li potřeba, navrhuje bezpečnostní opatření.

Systém řízení bezpečnosti, který je provozovatel dráhy povinen zavádět, má následující požadavky [242]:

1. Provozovatel dráhy a dopravce vede průběžně dokumentaci o všech důležitých částech systému zajišťujícího bezpečné provozování dráhy celostátní a regionální a drážní dopravy na těchto dráhách. Ve vnitřních předpisech provozovatele dráhy nebo dopravce musí být stanoveno rozdělení povinností v rámci organizace ve vztahu k zajišťování bezpečnosti provozování dráhy a drážní dopravy a stanoven způsob řízení v organizaci na různých úrovních, způsob zapojeni zaměstnanců na všech úrovních řízení do systému zajišťováni bezpečného provozování dráhy nebo drážní dopravy a způsob zajištění soustavného zlepšování systému bezpečnosti.
2. Systém zajišťování bezpečnosti provozování dráhy celostátní a regionální a drážní dopravy na těchto dráhách musí stanovovat:
   - bezpečnostní zásady a způsob jejich sdělování všem zaměstnancům,
   - kvalitativní a kvantitativní cíle organizace v oblasti zachování a zvyšování bezpečnosti a plány a postupy pro dosažení těchto cílů,
   - postupy zajišťující dodržování existujících, nových a změněných technických a provozních norem nebo jiných závazných podmínek stanovených: v technických specifikacích pro interoperabilitu; ve vnitrostátních právních předpisech; v jiných vnitřních předpisech provozovatele dráhy nebo dopravce, nebo v rozhodnutích úřadů státní správy,
   - postupy pro zajištění souladu stavu zařízení s požadavky technických nebo provozních norem a jinými závaznými podmínkami po dobu životnosti zařízení a po dobu jeho provozu,
   - postupy a metody posuzování rizika a zavádění opatření pro usměrňování rizika v případě, že změna provozních podmínek nebo materiály představují nová rizika pro dopravní cestu dráhy nebo provozováni drážní dopravy,
   - programy školení zaměstnanců a systémy, které zajišťují udržování kvalifikace zaměstnanců a odpovídající úroveň plnění úkolů,
   - opatřeni zajišťující dostatečnou informovanost v rámci provozovatele dráhy nebo dopravce a podle potřeby mezi dopravci používajícími tutéž dopravní cestu dráhy
   - postupy a vzory pro dokumentování bezpečnostních informací a stanovení postupu pro kontrolu předávání nejdůležitějších bezpečnostních informaci,
   - postupy zajišťující, že jsou závažné nehody, nehody, ohrožení a jiné události ovlivňující bezpečné provozováni dráhy a drážní dopravy oznamovány, jsou zjišťovány jejich příčiny a jsou analyzovány, a že jsou přijímána nezbytná preventivní opatření,
   - plány zásahu, varováni a předávání informací v případě mimořádné situace, jež jsou dohodnuty s příslušnými orgány veřejné správy,

- ustanovení o provádění periodických vnitřních kontrol systému zajišťování bezpečnosti.

Drážní průmysl není vždy povinen, ale je konkurenčním prostředím stimulován k zavedení drážního standardu IRIS [243], který je integrován do stávajícího systému řízení. IRIS rozšiřuje požadavky systému řízení jakosti dle ISO 9001 [242] s důrazem na kvalitu a bezpečnost vyvíjených a instalovaných systémů v jejich celém životním cyklu, tj. mimo jiné implementuje požadavky EN 50126 [244] pro prokázání bezporuchovosti, dostupnosti, udržovatelnosti a bezpečnosti systému (RAMS). Principy funkční bezpečnosti jsou dále rozšířené normou EN 50129 [245] pro bezpečnostně relevantní systémy (zabezpečovací zařízení) a EN 50128 [246] pro jakýkoliv software aplikovaný na drahách. Uvedené evropské normy jsou založené na funkční bezpečnosti dle IEC 61508 [247]. Bližší informace o požadavcích standardu IRIS a jemu příbuzných norem jsou uvedeny v práci [248].

Metodika normy EN 50126 [244] zavádí pojem integrita bezpečnosti a stupeň integrity bezpečnosti (dále jen SIL – Safety Integrity Level) pro bezpečnostně relevantní systémy. SIL přiřazuje provozovatel dráhy pro dané funkce či určité systémy plnící tyto funkce na základě analýzy nebo vlastního posouzení. Metody a opatření definované v uvedené normě jsou určené k identifikaci a vypořádání se s náhodnými a systematickými chybami elektronického systému. Příkladem jedné z metod zvýšení bezpečnosti (kupříkladu zabezpečovacího zařízení) je jednoduchá architektura s vlastní bezpečností (tzv. inherentní bezpečnost), kdy při neschopnosti systému vykonat požadovanou funkci v požadované době a požadované kvalitě, systém akci neprovede, selže bezpečně (například návěstní hodnota „stůj“ apod.). Bezpečnou architekturu vytváří také zálohovaný (redundantní) systém s porovnáním výsledků (systémy 2 z 3, porovnávání výsledků 3 systémů, kde se musí alespoň dva shodovat apod.).

Pro software bezpečnostně relevantního drážního systému je dle drážních předpisů známá pouze systematická chyba způsobená zavedením chyby v návrhu software, chyby programátora či zvolených metod programování. Pro eliminaci systémové chyby vývoje softwaru jsou v normě EN 50 128 [246] definované požadavky pro vývoj softwaru pro bezpečnostně relevantní drážní systémy s příslušnou integritou bezpečnosti (SIL 0 až 4).

Komunikace mezi bezpečnostně relevantními systémy je řízena normou EN 50159 [245]. Komunikace se může uskutečňovat skrze uzavřené nebo otevřené komunikační prostředí (radiová komunikace, Wi-Fi, různé technologické sítě). Uzavřené přenosové prostředí je přístupné pouze tvůrci systému popřípadě autorizovaným osobám. Otevřené komunikační prostředí je přístupné i neoprávněným a neautorizovaným subjektům. Bezpečnostně relevantní data v otevřeném prostředí mohou být zachycena útočníkem, který má možnost provést chybné operace a způsobit tak nehodu nebo i destrukci systému.

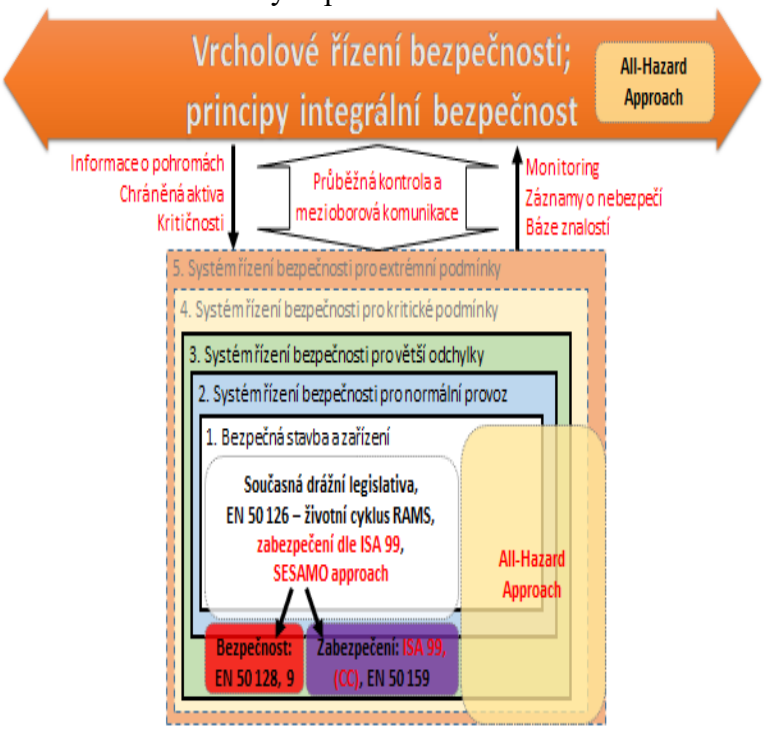
Předpisy spojené s řízením rizika na dráhách v České republice [249] nestanoví jasně stupnici pro určení míry rizika; použité slovní výrazy nejsou jasně vymezeny, což dovoluje nejednotné posuzování. Mají rozlišené 4 kategorie rizika a matici rizika (tabulka 42) i pokyn, jak s rizikem nakládat [249]. Předmětný pokyn stanoví: je-li riziko zanedbatelné, není třeba provádět žádnou činnost, či opatření; je-li riziko přípustné, je třeba ho prověřit a projednat s provozovatelem dráhy; je-li riziko nežádoucí, tak provést opatření ke snížení rizika, a když snížení rizika není prakticky dosažitelné, tak rozhoduje provozovatel; a když je riziko nepřípustné, tak jeho příčina musí být odstraněna.

Tabulka 42. Matice rizik používaná v drážní dopravě [249].

Četnost výskytu nebezpečné události	**Úroveň rizika**			
Častá	Nežádoucí	Nepřípustné	Nepřípustné	Nepřípustné
Pravděpodobná	Přípustné	Nežádoucí	Nepřípustné	Nepřípustné

Občasná	Přípustné	Nežádoucí	Nežádoucí	Nepřípustné
Malá	Zanedbatelné	Přípustné	Nežádoucí	Nežádoucí
Nepravděpodobná	Zanedbatelné	Zanedbatelné	Přípustné	Přípustné
Vysoce nepravděpodobná	Zanedbatelné	Zanedbatelné	Zanedbatelné	Zanedbatelné
	Nevýznamné	Okrajové	Kritické	Katastrofické
	Úrovně závažnosti následků nebezpečí			

Posouzení shody řízení bezpečnosti mezi modelem založeným na integrální bezpečnosti a realitou [250], obrázek 52, ukazuje, že v realitě nejsou plně zohledněny přístupy All- Hazard-Approach a pětistupňový Defence-In-Depth, ze kterých vychází princip řízení bezpečnosti [1,10]. Je použit pouze třístupňový model ochrany do hloubky a výslovně se nepožaduje zohlednění všech možných pohrom v daném místě.



Obr. 52. Porovnání reálného systému řízení bezpečnosti s požadavky modelu, založeném na přístupech All- Hazard-Approach a pětistupňovém Defence-In-Depth [250].

Na základě hodnocení provedených v pracích [250,251] jsou odvozeny dále uvedené nedostatky:

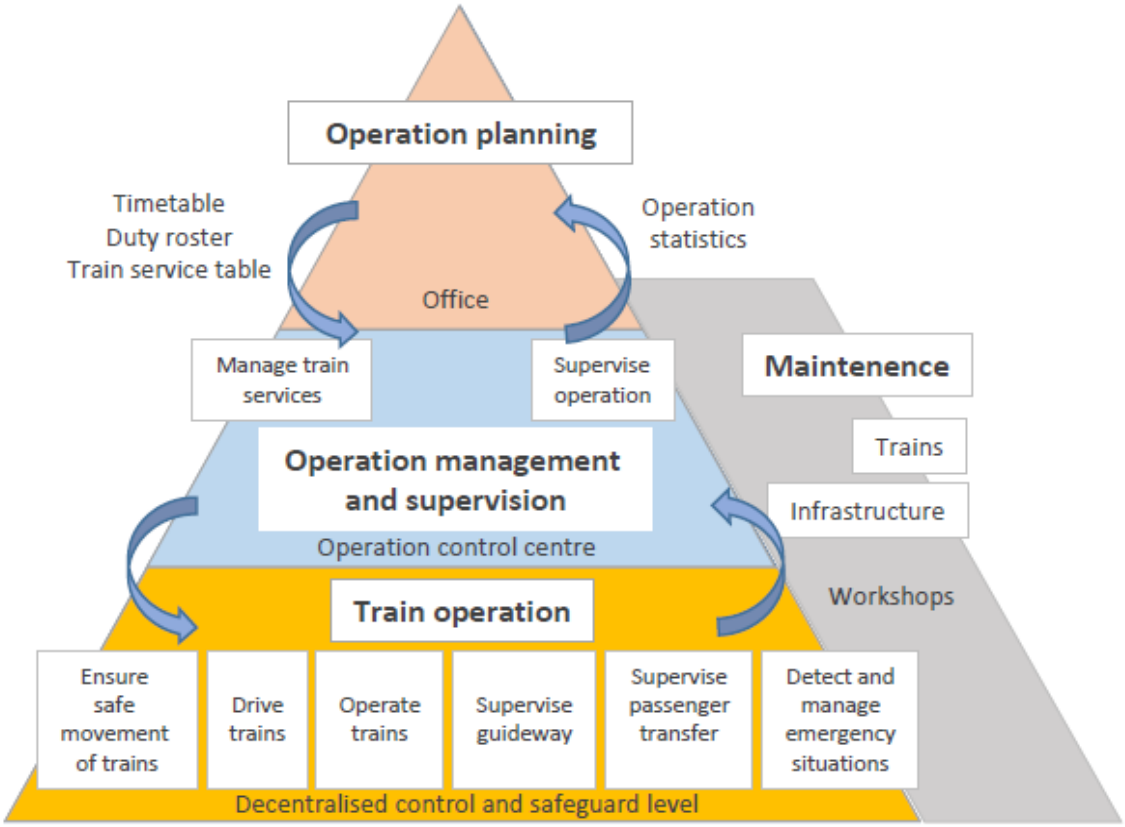
- není řádně zavedeno vrcholové řízení založené na proaktivním přístupu a na integrálním riziku,
- chybí mezioborová komunikace a vazba mezi jednotlivými vrstvami řízení bezpečnosti,
- požadavky na bezpečnost nejsou řešeny komplexně; nemusí být identifikována všechna rizika,
- neřeší se otázka selhání lidského faktoru,
- ve všech vrstvách řízení bezpečnosti chybí aplikace konceptu All-Hazard-Approach,
- absence konceptu Defence-In-Depth pro kritické položky ve sledované síti,
- přístup k bezpečnosti a zabezpečení je v české i evropské legislativě pojat odděleně a neřeší vzájemné závislosti, které mohou ovlivnit bezpečnost,
- drážní předpisy a normy dosud dostatečně neřeší zabezpečení všech drážních zařízení,
- neuvažují se vazby a toky přes hranice systému a za hranicemi systému.

5.9.4.3. Metro

Provoz metra v Praze byl zahájen v roce 1974 na lince C v úseku Kačerov – Sokolovská (Florenc). V roce 1978 byl zahájen provoz na lince A v úseku Leninova (Dejvická) – Náměstí míru. V roce 1985 byl zahájen provoz na lince B v úseku Smíchovské nádraží – Sokolovská (Florenc). V současné době je v pražském metru v provozu 61 stanic. Na linkách A a B jsou provozovány soupravy s typovým označením 81-71M, které jsou modernizovanou verzí původních sovětských souprav 81-71. Na lince C jsou provozovány soupravy typu M1, které byly vyrobeny konsorciem společností ČKD Praha, ADtranz a Siemens.

Dle dokumentace [252] pražské metro pracuje ve dvou režimech, a to: dopravní systém metra (DSM); a ochranný systém metra (OSM). Režim DSM je základním režimem metra plnícím funkci dopravně obslužní. Jednotlivé subsystémy a zařízení pražského metra (DSM a OSM) se mohou dle daných situací nacházet v různých stavech a režimech provozu. Pro oblast řízení bezpečnosti je nutné uvedené režimy detailně znát.

Metro je důležitou součástí městského dopravního systému v Praze. Zabezpečit provoz metra znamená zabezpečit provoz každé stanice metra, a na ní aplikovat několika vrstevnatý model pro řízení bezpečnosti. Pro systém řízení městské a příměstské kolejové dopravy je dle [253] použít model (obrázek 53), který rozděluje systém řízení do tří úrovní:



Obr. 53. Model řízení metra dle [253]. Základní části jsou: plánování provozu; řízení provozu a dohledu; a provoz vlaků.

1. Úroveň operačního plánování. Zde jsou vytvářeny plány přepravy pro běžný provoz i pro případ větších odchylek (tzv. mimořádností) v dopravě. Výstupy (jízdní řády) směřují do úrovně řízení. Informace o odchylkách od předmětného plánu přicházejí zpět do úrovně operačního plánování a tvoří základ pro vyhodnocení kvality provozu. Pro část systému, zabývajícího se údržbou poskytují podklady pro zpracování plánu oprav; z nich se pak

získávají informace o poruchách a požadavcích na obnovu vozového parku a technologií. Informace jsou důležité pro analýzu kritických komponent systému, protože se z nich predikují místa a četnosti výskytu poruch.

2. Úroveň operačního řízení. Jde o dispečerské řízení, které zajišťuje dohled nad provozem vlaků, tj. koordinuje dopravu v navazujících úsecích a řeší odchylky v dopravě nebo komplikace při pohybu osob. Centrum operačního řízení je klíčovým prvkem systému řízení. V případě jeho výpadku přebírají část pravomocí lokální pracoviště ve stanicích. Přepravní kapacita je v případě poloautomatického systému značně omezena, v případě výpadku automatického nebo bezobslužného systému dochází k zastavení provozu.
3. Úroveň provozu vlaků zastřešuje kompletní dopravní infrastrukturu, tj. vlaky, trať, stanice, napájecí soustavu, dále staniční informační a dohledové systémy, systémy sdělovací, zabezpečovací zařízení. Každá stanice je samostatným systémem, závislým na výše uvedených subsystémech, tzn., že výpadek kteréhokoli z nich vede k nezpůsobilosti stanice k provozu. Vlaky, byť jsou samostatnými celky, bez součinnosti s traťovou částí rovněž nejsou schopny samostatného provozu.

Údržba navazuje na všechny tři úrovně systému. Odpovídá za funkčnost všech jeho částí od vlaků přes signalizační a akční členy až po systém řízení. V případě výpadku údržby je systém schopen plně funkce pouze po omezenou dobu. Kromě operativních zásahů provádí údržba průběžnou kontrolu klíčových prvků systému a předchází tím závadám, které mohou vést od ohrožení plynulosti provozu až ke ztrátám na lidských životech. Použité standardy zajišťují, aby systém splňoval funkční požadavky, byl dostatečně flexibilní pro případná budoucí rozšíření a byl schopen integrace do vyšších celků [253].

Aby dopady selhání metra na životy a zdraví cestujících a zaměstnanců, majetek a obslužnost města nebyly závažné, je třeba zajistit metro jako bezpečný systém. Jak bylo dříve uvedeno, člověk je schopen vytvořit zabezpečený systém, který je bezpečný v jistém rozsahu podmínek, a pro podmínky, které jsou mimo daný interval, musí vytvořit specifické nástroje, které sníží ztráty na veřejných aktivech i aktivech systému na přijatelnou úroveň. Proto je nutno se orientovat na bezpečnost všech aktiv systému, tj. z oblasti technické, organizační i lidských zdrojů.

Stanice metra společně s jejími technologiemi a návaznými stanicemi tvoří dopravní infrastrukturu městské kolejové dopravy v Praze. Jedná se o složitý systém, který je součástí nadřazeného systému, tj. stanice je podřízena centrálnímu dispečinku řízení dopravy a je propojena s okolními systémy po celé trase metra. Centrální dispečink i jednotlivé stanice metra jsou provozovány provozovatelem, v případě pražského metra se jedná o Dopravní podnik hl. m. Prahy.

Systém řízení bezpečnosti sledovaného systému odpovídá systému řízení kvality, ve kterém jsou integrované požadavky mezinárodních standardů ISO 9001 [240] a EN 13816 [254] určující jakost služby, cíle a měření veřejné přepravy osob, tj. bezpečnost celého systému a jeho okolí. Jeho hlavní cíle jsou dle [10]: spolehlivost; informovanost; dostupnost; zabezpečení; a komfort při cestování.

Každá stanice metra propojuje různé typy systémů, které mají povahu technologickou, kybernetickou, ekonomickou a sociální. Stanice jsou konstruovány na základě legislativních požadavků, které jsou platné v České republice (např. jsou respektovány jen jisté pohromy, jednotlivé systémy jsou projektovány a řízeny samostatně, tj. bez ohledu na systémy ostatní, nezvažují se nadprojektové pohromy [1,11,253]). To znamená, že při výstavbě i provozu není důsledně brán ohled na propojení jednotlivých systémů, a tudíž není zavedena ochrana proti průřezovým rizikům [1,5,11], což vede k identifikaci neshod mezi ideálem a skutečností, tj. normativem, který odpovídá požadavkům normativu, který respektuje přístupy Defence-In-Depth a All-Hazard-Approach [1].

Při stanovení rizik pro modelovou stanici metra byla zvážena aktiva [255]:

- chráněná veřejná aktiva v okolí (občané, parkoviště, autobusová zastávka, křižovatky, benzínové pumpy, městské sídliště),
- chráněná aktiva modelové stanice metra (lidé a majetek):
    - lidé (životy a zdraví cestujících, zaměstnanců) a životní prostředí,
    - objekty (tj. veřejná místa – vestibuly, nástupiště, soupravy vlaků; shromažďovací místa, technologické místnosti, stanoviště dozorčí stanice),
    - energetická zařízení (měnírny a distribuční transformovny),
    - sdělovací zařízení (sdělovací kabely, VKV spojení s vlaky, automatické odbavování cestujících, zařízení průmyslové televise, telefonní zřízení, rozhlasové zařízení, hodinové zařízení, elektrická požární signalizace, elektrická zabezpečovací signalizace),
    - strojní zařízení (pohyblivé schody ve stanicích, čerpací stanice ve stanicích a mezistaničních úsecích, výtahy ve stanicích, dílny a sklady údržby ve stanicích),
    - vzduchotechnická zařízení (hlavní větrání, staniční vzduchotechnika),
    - mobilní stroje a zařízení (vozový park, zařízení a prostředky pro čištění odpadu zahrnují mycí a zametací vozíky, kontejnery na odpad a soustavu žebříků a lešení pro čištění osvětlovací techniky, prostředky požární ochrany umístěné ve stanicích, které umožňují rychlý zásah při požáru v podzemních prostorách),
    - ostatní důležitá zařízení (bezpečnostní a poplachová tlačítka, zařízení pro vyhlášení požárního poplachu, trakční zařízení a osvětlení, traťová zařízení, hlavní uzávěr vody, pohyblivé schody, plošiny, signální panel strojního zařízení, uzavírací zařízení - elektrické rolety),
    - staniční jednotky řídicího systému (staniční uzel ASDŘ-D – automatický systém dopravního řízení, staniční jednotka automatického stavění jízdních cest, staniční uzly s návazností na energetický a technologický dispečink, staniční uzly systému centrálního ovládání osvětlení, staniční uzly s návazností na dispečink sdělovací, zabezpečovací a dispečink hasičů),
    - zabezpečovací zařízení (staniční, traťová a vlaková),
    - toky (energetické, informační, materiálové).

Kritičnost aktiv s ohledem na možné pohromy je oceněna podle úrovně jejich zabezpečení vůči možným pohromám [256], přičemž byla použita stupnice: - pohroma nemá přímý dopad; 1 – jsou provedena preventivní opatření; 2 – jsou provedena částečná ochranná opatření; 3 – zabezpečení nezajištěno. Výsledek hodnocení kritičnosti je v tabulce 43.

Tabulka 43. Úroveň zabezpečení aktiv vůči možným pohromám: 1 – zajištěno; 2 – zajištěno částečně; 3 – nezajištěno; - nemá přímý dopad.

Pohromy / Aktiva	Povodeň	Zemětřesení	Ztekucení podloží	Výstup plynu na	Epidemie	Pandemie	Narušení blaha	Kriminalita	Útok	Teroristický útok	Útok CBRNE	Ozbrojený konflikt	Válka	Průmyslová nehoda	Nehoda s neb. látkou	Dopravní nehoda	Selhání dodávek	Pohroma v ekonomice
Lidé	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	1	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Objekty	1	1	1	2	-	-	-	2	3	3	3	3	3	1	3	2	2	-
	1	1	1	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
	2	1	1	2	-	-	-	2	3	3	3	3	3	2	3	3	3	-
	1	1	1	2	-	-	-	2	3	3	3	3	3	1	3	2	2	-

Energetická zařízení	1	1	1	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
	2	1	1	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
Sdělovací zařízení	2	2	2	2	-	-	-	2	3	3	3	3	3	1	3	2	3	-
	2	2	2	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
	2	2	2	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
Strojní zařízení	1	1	1	2	-	-	-	2	3	3	3	3	3	1	3	2	2	-
	2	2	2	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
	3	3	3	3	-	-	-	3	3	3	3	3	3	3	3	3	2	-
Vzduchotechnická zařízení	1	1	1	2	-	-	-	2	3	3	3	3	3	2	3	2	2	-
	2	2	2	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
	3	3	3	3	-	-	-	3	3	3	3	3	3	3	3	3	3	-
Mobilní stroje a zařízení	1	1	1	1	-	-	-	3	3	3	3	3	3	3	3	3	3	-
	1	1	1	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
	2	1	1	3	-	-	-	3	3	3	3	3	3	3	3	3	-	-
Ostatní důležitá zařízení	1	1	1	1	-	-	-	3	3	3	3	3	3	3	3	3	3	-
	1	1	1	2	-	-	-	2	3	3	3	3	3	2	3	3	2	-
	2	1	1	3	-	-	-	3	3	3	3	3	3	3	3	3	-	-
Staniční jednotky řídicího systému	1	1	1	-	-	-	1	1	1	1	1	1	1	1	3	1	1	-
	1	1	1	-	-	-	2	1	1	2	1	1	2	1	3	1	1	-
	3	2	2	-	-	-	3	2	2	3	3	2	2	2	3	2	2	-
Zabezpečovací zařízení	1	1	1	-	-	-	1	1	1	1	1	1	1	1	3	1	1	-
	1	1	1	-	-	-	2	1	1	2	1	1	2	2	3	1	1	-
	3	2	2	-	-	-	3	2	2	3	3	2	3	3	3	2	2	-
Toky	1	1	1	-	-	-	1	1	1	3	3	3	3	3	3	3	3	3
	1	1	1	-	-	-	2	1	1	3	3	3	3	3	3	3	3	3
	3	2	2	-	-	-	3	2	2	3	3	3	3	3	3	3	3	3

Na základě údajů v tabulce 43 lze pomocí součtů údajů v řádcích a sloupcích určit aktiva, která jsou nejméně zabezpečená i pohromy, vůči kterým chybí preventivní, zmírňující a reaktivní opatření, když se vyskytne předmětná pohroma o velikosti větší než projektová. Z tabulky 43 vyplývá, že nejméně jsou zabezpečení lidé, následují řídící, energetické a informační toky, vzduchotechnická, strojní, sdělovací a další zařízení a teprve po nich mobilní stroje, jiná důležitá zařízení, konstrukce a objekty. Z tabulky je též zřejmé, že v ochranném dopravním systému metra chybí opatření proti nehodě s nebezpečnou látkou, teroristickému útoku, válce, útoku s látkami CBRNE, ozbrojeného konfliktu, dopravní nehodě, útokům, průmyslové nehodě, a v řadě případů i proti selhání dodávek elektřiny či kriminalitě; mnohdy i v konceptu entity, tj. na první úrovni zabezpečení.

Pro zajištění bezpečnosti stanice metra byl proto zpracován plán řízení rizik [254] pro prioritní rizika dle [1] a jeho úroveň byla posouzena podle kontrolního seznamu, tabulka 44, zpracovaného podle zásad strategického řízení [257] s tím, že je použita hodnotová stupnice – tabulka 2 v kapitole 4.2.

Tabulka 44. Kontrolní seznam pro posuzování plánu řízení rizik.

Otázka	**Hodnocení**
Je plán pro zvládnutí rizik veden jasnou představou a sledovanými cíli?	
Uplatňuje se v plánu pro zvládnutí rizik princip celistvosti (tj. uvážení prosperity sociálního, ekologického a ekonomického subsystému;	

vyjádření nákladů a užitků; dopadů a přínosů ekonomické aktivity pomocí peněžních i nepeněžních hodnot)?	
Jsou v plánu pro zvládnutí rizik zváženy podstatné elementy (např. spravedlivá dělba využívání zdrojů mezi současnou generací a generacemi budoucími; nadměrná spotřeba a chudoba; lidská práva; ekologické poměry podmiňující život; prosperita umožněná ekonomickým rozvojem a mimotržními činnostmi)?	
Má plán pro zvládnutí rizik přiměřený rozsah (např. vhodné měřítko času a prostoru)?	
Je plán pro zvládnutí rizik prakticky zaměřen (např. explicitně definované kategorie, které spojují vytyčenou představu s indikátory a kritérii; omezený počet klíčových cílů; omezený počet indikátorů; standardizovaný způsob měření a porovnávání; referenční hodnoty indikátorů, prahové hodnoty, vývojové trendy)?	
Je plán pro zvládnutí rizik otevřený (např. všeobecně přijaté metody a databáze; explicitní věrohodnost, vyloučení nejistoty)?	
Je v plánu pro zvládnutí rizik zahrnuta efektivní komunikace v zájmové společnosti?	
Podílí se na plánu pro zvládnutí rizik široká veřejnost?	
Počítá se v plánu pro zvládnutí rizik s následným posuzováním (např. upřesňování postupných cílů vlivem vývoje systému)?	
Jsou v plánu pro zvládnutí rizik zabezpečeny kapacity institucí (např. určení odpovědnosti za dodržení cílů rozhodovacího procesu, sběr a uchovávání údajů, dokumentace)?	
CELKEM	

Konkrétní plán řízení rizik vybrané stanice metra pro rizika spojená s technickými a organizačními systémy je vypracován v tabulce 45, která uvádí relevantní oblasti rizik, popis rizik, jejich pravděpodobnosti výskytu, jejich dopady a návrh možných opatření na zmírnění rizika. Nejsou uvedena opatření spojená s bezpečností lidí, protože jak ukazuje tabulka 43, rizika spojená s lidmi, kromě úzké oblasti BOZP nejsou v konceptu bezpečnosti stanic metra sledovány. Při aplikaci opatření jsou zváženy naplněné požadavky standardů ISO 9001 [244], IRIS [243] a zavedený přístup SIL na všechna zařízení z kategorie E/E/PE [247],

Tabulka 45. Plán řízení prioritních rizik pro stanici metra; SMS – systém řízení bezpečnosti; v případech, kde není uvedena odpovědnost, tak je stanovena v předpisech Dopravního podniku [256].

Oblast rizika	**Popis rizika**	**Pravděpodobnost výskytu a dopady rizika**	**Opatření na zmírnění či zvládnutí rizika**
Jednotlivé	Slabiny v zabezpečení vůči vnějším vlivům.	Pravděpodobnost: střední Dopady: mírné až vysoké	Aplikovat opatření technická či organizační opatření uvedená v bezpečnostním plánu založeném na konceptu bezpečnost systému systémů a aplikaci principů All-Hazard-Approach a Defence-In-Depth.

			Provede: generální ředitel Dopravního podniku.
	Výskyt vnitřních náhodných poruch systému.	Pravděpodobnost: nízká dle SIL; Dopady: vysoké	Aplikovat opatření ze systému řízení kvality ISO 9001 [242], IRIS [243], zavedení alespoň SIL 0 na všechny E/E/PE [247]. Provede: vedoucí jednotky provozu metra za pomoci vedoucího jednotky správy vozidel metra, vedoucího jednotky dopravní cesty metra, ředitele bezpečnostního úseku, vlakového dispečera a dozorčího stanice.
	Výskyt vnitřních systémových poruch v systému.	Pravděpodobnost: nízká dle SIL; Dopady: vysoké	Aplikovat opatření systému řízení kvality ISO 9001 [242], IRIS [243], zavedení alespoň SIL 0 na všechny E/E/PE [247]. Provede: vedoucí technické správy objektů a podpory provozu metra za spolupráce vedoucího odboru řízení provozu jednotky metra, vlakového dispečera a dozorčího stanice.
	Poruchy v procesech, lidská chyba.	Pravděpodobnost: velmi vysoká; Dopady: vysoké	Aplikovat opatření systému řízení kvality ISO 9001 [242], IRIS [243], školení, přezkoušení, cvičení, potvrzovací funkce E/E/PE [247], zavedení zpětných vazeb. Provede: vedoucí odboru vzdělávání a rozvoje zaměstnanců za spolupráce s ředitelem úseku bezpečnostní kontroly a vedoucím odboru řízení provozu jednotky metra.
	Omezené zdroje	Pravděpodobnost: nízká Dopady: střední	Aplikovat opatření požadované systémem řízení kvality ISO 9001 [242], IRIS [243], zachování rezerv pro provedení kritických činností. Provede: generální ředitel ve spolupráci s celým top managementem.
	Vzájemné vlivy požadavků na bezpečnost a zabezpečení	Pravděpodobnost: vysoká; Dopady: střední	Aplikovat opatření pro hledání kompromisů navržených v projektu SESAMO [258]. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím jednotky provozu metra, vedoucím jednotky dopravní cesty metra, vedoucím jednotky pro správu vozidel metro a vedoucím technické správy objektů a podpory provozu.

	Chybná nebo nedostatečná identifikace ovlivňujících činitelů.	Pravděpodobnost: střední Dopady: vysoké	Aplikovat opatření EN 50126 [244], tj. provést nezávislé posouzení selhání, monitoring a nalézt vhodné řešení. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím jednotky provozu metra, vedoucím jednotky dopravní cesty metro, vedoucím jednotky správa vozidel metro, vedoucím technické správy objektů a podpory provozu a dozorčího stanice.
	Chybná práce s riziky, volba metody, definice stupnic, ohodnocení rizik.	Pravděpodobnost: nízká Dopady: vysoké	Aplikovat opatření EN 50126 [244], tj. provést nezávislé posouzení selhání, monitoring a nalézt vhodné řešení, ověřování a hodnocení metodiky. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím jednotky provozu metra, vedoucím jednotky dopravní cesty metra, vedoucím jednotky správa vozidel metro a vedoucím technické správy objektů a podpory provozu.
	Odpovědnosti, kompetence, nezávislost a důvěrnost řešitelských subjektů.	Pravděpodobnost: nízká Dopady: vysoké	Provést nezávislé posouzení selhání a aplikovat opatření EN 50126 [244] a systému řízení kvality ISO 9001 [242]. Provede: ředitel bezpečnostního úseku ve spolupráci s ředitelem personálního úseku.
	Přenos chybných a matoucích informací, tj. chyby na vstupu nebo na výstupu systémů.	Pravděpodobnost: střední Dopady: velmi vysoké	Provést nezávislé posouzení selhání a aplikovat opatření v monitoringu a mezioborové komunikaci, tj. zavést jednotnou terminologii. Provede: vedoucí jednotky řízení provozu metra ve spolupráci s vlakovými dispečery a dozorčím stanice.
	Přerušení informačních a materiálových toků.	Pravděpodobnost: nízká Dopady: vysoké	Kontinuálně zajišťovat vytváření záloh a redundantních systémů. Provede: ředitel technické správy objektů a podpory provozu ve spolupráci s vedoucím odboru řízení provozu jednotky metra, vlakovými dispečery a dozorčím stanice.
	Vykonávání navzájem se ovlivňujících funkcí.	Pravděpodobnost: vysoká; Dopady: vysoké	Zajistit monitoring a pravidla pro mezioborovou komunikaci. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím

			odboru technické správy objektů a podpory provozu.
	Poruchy okolních systémů a realizace relevantních pohrom.	Pravděpodobnost: střední Dopady: velmi vysoké	Zajistit monitoring a pravidla pro mezioborovou komunikaci. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím odboru technické správy objektů a podpory provozu.
Vazby mezi jednotlivými vrstvami SMS	Chybná metodika identifikace nebezpečí a analýzy rizik z vyšších úrovní SMS.	Pravděpodobnost: vysoká; Dopady: velmi vysoké	Zajistit monitoring a pravidla pro mezioborovou komunikaci. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím odboru technické správy objektů a podpory provozu a vedoucím jednotky provoz Metra.
	Neporozumění požadavkům a informacím z jiné vrstvy SMS.	Pravděpodobnost: vysoké; Dopady: vysoké	Zajistit monitoring a pravidla pro mezioborovou komunikaci, vzdělávání a přerozdělit kompetence. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím odboru technické správy objektů a podpory provozu a vedoucím jednotky provoz Metra.
	Přenos poruchových stavů v případě jejich výskytů z jedné vrstvy do druhé.	Pravděpodobnost: střední Dopady: střední	Zajistit přiměřenou nezávislost vrstev, fyzické oddělení vrstev a diverzní sběr informací. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím odboru technické správy objektů a podpory provozu a vedoucím jednotky provoz Metra.
	Chybějící vstupní informace.	Pravděpodobnost: vysoká; Dopady: velmi vysoké	Zkvalitnit vrcholové řízení bezpečnosti, vzdělávání a výzkum. Provede: ředitel bezpečnostního úseku ve spolupráci s vedoucím odboru technické správy objektů a podpory provozu a ředitelem personálního úseku.
Jiné nepředvídatelné události a lidský faktor	Vnější faktory	Pravděpodobnost: vysoké; Dopady: střední	Zajistit zlepšení systému řízení kvality ISO 9001 [242] , IRIS [243], školení, přezkoušení, cvičení, kompetence, systémy řízení bezpečnosti informací ISA/IEC 27000 [259], zabezpečení dle ISA 99 [247] a CC [258], monitoring. Provede: ředitel bezpečnostního úseku ve spolupráci s řídícími pracovníky všech úseků.

	Vnitřní faktory	Pravděpodobnost: střední Dopady: vysoké	Zajistit zlepšení systému řízení kvality ISO 9001 [242] , IRIS [243], školení, přezkoušení, cvičení, kompetence, systémy řízení bezpečnosti informací ISO/IEC 27000 [259], zabezpečení dle ISA 99 [247] a CC [258], monitoring. Provede: ředitel bezpečnostního úseku ve spolupráci s řídícími pracovníky všech úseků.
	Úmyslná poškození	Pravděpodobnost: nízká Dopady: velmi vysoké	Zajistit zlepšení systému řízení kvality ISO 9001 [242], IRIS [243], školení, přezkoušení, cvičení, kompetence, systémy řízení bezpečnosti informací ISA/IEC 27000[259], zabezpečení dle ISA 99 [260] a CC [261], monitoring. Provede: ředitel bezpečnostního úseku ve spolupráci s řídícími pracovníky všech úseků.

Z tabulky 45 vyplývá, že v metru je třeba:

1. Mít zavedené kvalitní / bezpečné a monitorované procesy údržby a provozu, které jsou zavedené v provozním řádu stanice.
2. Aplikovat bezpečnostní plán při návrhu, výstavbě a při řízení změn, který je zacílený na eliminaci systémových poruch a mít připraven plán pro zvládání systémových poruch v provozu.
3. Zavést pravidelná školení, přezkoušení a cvičení zaměstnanců; potvrzovací funkce E/E/PE dle [247] a zpětné vazby.
4. Zajistit bezpečnost vysokou kvalitou instalovaných systémů dle požadavků [41,262-264].
5. Provádět pravidelné audity, hodnocení kompetencí, zajištění nezávislosti řešitelských týmů apod.

Výše uvedená tabulka 45 zachycuje několik základních skupin rizik, se kterými je v rámci SMS stanice metra jako objektu kritické infrastruktury potřeba pracovat.

Výsledek posouzení kritičnosti plánu řízení rizik je uveden v tabulce 46; bodové hodnocení je provedeno odhadem na základě zkušeností z inspekcí v provozu metra [258], a logických úvah ohledně stability bezpečnostního plánu pro metro z pohledu dynamického vývoje planety, technologií a lidské společnosti (na základě současných dat a zkušeností opatření proti pohromám mají řádově platnost: živelní - stovky let; technologické - desítky let; sociální – roky.

Tabulka 46. Posouzení kritičnosti plánu řízení rizik.

Otázka	**Hodnocení**
Je plán pro zvládnutí rizik veden jasnou představou a sledovanými cíli?	0
Uplatňuje se v plánu pro zvládnutí rizik princip celistvosti (tj. uvážení prosperity sociálního, ekologického a ekonomického subsystému; vyjádření nákladů a užitků; dopadů a přínosů ekonomické aktivity pomocí peněžních i nepeněžních hodnot)?	2

Jsou v plánu pro zvládnutí rizik zváženy podstatné elementy (např. spravedlivá dělba využívání zdrojů mezi současnou generací a generacemi budoucími; nadměrná spotřeba a chudoba; lidská práva; ekologické poměry podmiňující život; prosperita umožněná ekonomickým rozvojem a mimotržními činnostmi)?	3
Má plán pro zvládnutí rizik přiměřený rozsah (např. vhodné měřítko času a prostoru)?	1
Je plán pro zvládnutí rizik prakticky zaměřen (např. explicitně definované kategorie, které spojují vytyčenou představu s indikátory a kritérii; omezený počet klíčových cílů; omezený počet indikátorů; standardizovaný způsob měření a porovnávání; referenční hodnoty indikátorů, prahové hodnoty, vývojové trendy)?	1
Je plán pro zvládnutí rizik otevřený (např. všeobecně přijaté metody a databáze; explicitní věrohodnost, vyloučení nejistoty)?	1
Je v plánu pro zvládnutí rizik zahrnuta efektivní komunikace v zájmové společnosti?	2
Podílí se na plánu pro zvládnutí rizik široká veřejnost?	4
Počítá se v plánu pro zvládnutí rizik s následným posuzováním (např. upřesňování postupných cílů vlivem vývoje systému)?	1
Jsou v plánu pro zvládnutí rizik zabezpečeny kapacity institucí (např. určení odpovědnosti za dodržení cílů rozhodovacího procesu, sběr a uchovávání údajů, dokumentace)?	1
CELKEM	16

Z porovnání tabulky 46 se stupnicí tabulce 1 (kapitola 4.2) vyplývá, že plán řízení rizik má střední kritičnost, což znamená, že existují úseky, ve kterých rizika jsou ošetřena jen z dílčího pohledu, tj. jsou řešena jen známá rizika. Uvedený fakt je v souladu s výsledkem expertního šetření [257], dle kterého řízení a vypořádání rizik založené na integrální bezpečnosti pro model systém systémů má též jistou kritičnost, protože neznáme všechna možná propojení mezi aktivy a jejich možné proměny v důsledku dynamického vývoje světa. Při zvážení vztahu mezi mírou bezpečnosti b a mírou kritičnosti k ve tvaru b = 1 - k, dostaneme míru bezpečnosti střední, což odpovídá realitě, protože znalosti a disponibilní možnosti člověka jsou omezené.

Vážným nedostatkem reálné situace je skutečnost, že stanice metra mají sloužit dle krizového plánu Prahy k přežití lidí v případě nepřátelského napadení (dle zákona č. 240/2000 Sb., o krizovém řízení a souvisejících předpisů Dopravní podnik hl. m. Prahy zpracovává plán krizové připravenosti), že systémy řízení bezpečnosti reálných stanic metra se nezabývají bezpečím lidí ve stanici metra a jejím okolí při kritických podmínkách ve stanicích. Protože nic není absolutně bezpečné, je třeba možnost vzniku kritických podmínek připustit, a připravit plán řízení možných realizovaných rizik i s ohledem na cestující a zaměstnance stanice metra a na obyvatele nacházející se v okolí. Proto je velmi důležité zavést sestavený plán řízení rizik do praxe a rozšířit ho na zbývající části metra [256] .

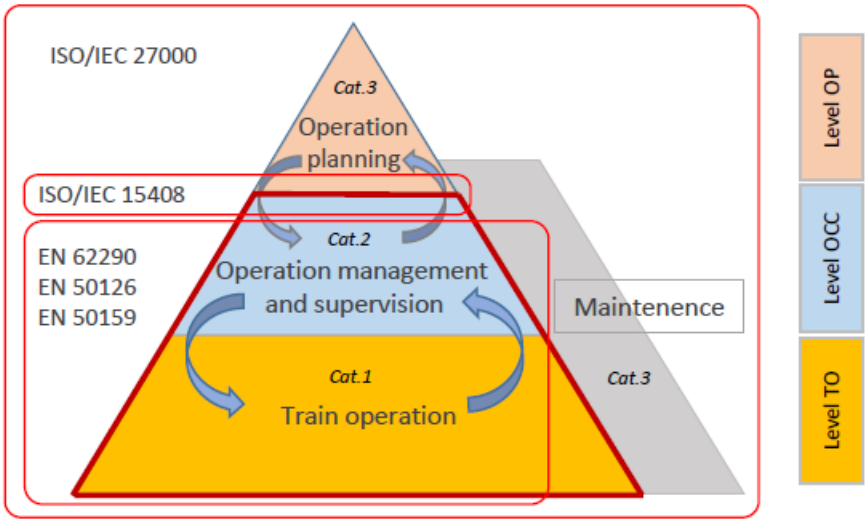
V oblasti řízení jde o způsob organizace procesů a jejich činností řízení a o jejich zabezpečení. Protože jde o řízení složitého systému, tak je prováděno pomocí záznamů z automatických technických prostředků (sonary, radary, termokamery, infradalekohledy či jiná speciální čidla; čidla jsou napojená na obrazovkové displeje, které zobrazují momentální situaci přehledovým způsobem, a na počítače, které mají programy pro mapování přehledové situace). K tomu je potřeba mít jak spolehlivé a robustní technické prostředky, tak spolehlivou a robustní komunikační infrastrukturu.

Práce [255] uvádí třívrstvý model řízení komunikační drážní infrastruktury (obrázek 54) a ukazuje, že největší dopady na aktiva veřejná i podniková mají selhání na nejnižší vrstvě, a

proto jim musí být věnována největší pozornost.

Obecný popis systému řízení metra vychází z popisu systému řízení pražského metra ASDŘ [253], a evropského standardu pro definici funkcí a parametrů řídicího systému pro řízení městské kolejové dopravy [263], tj. systém UGTMS.

Z technického úhlu pohledu můžeme systém metra rozdělit na systémy řídicí, řízené a ochranné či zabezpečovací, které mají vzájemné vazby a některé společné vstupy a výstupy. Vstupem systému jsou informace z procesu plánování provozu, tj. plánované jízdní řády, rozpisy služeb a podobně. Výstupem systému je zajištění dopravního výkonu v požadované kvalitě a v režimu dopravním a snížení dopadů pohrom v případě režimu ochranném [253].



Obr. 54. Model řízení drážní infrastruktury [254].

Podle vykonávaných funkcí je dle [263] systém řízení (UGTMS) členěn do několika úrovní dle úrovně řešení problému (provozní plánování, řízení provozu, řízení vlaků) a dle stupně automatizace (GOA 0 až GOA 5, provozování vlaků na rozhled a neautomatizovaný provoz až po plně automatický provoz vlaků bez obsluhy) [263].

Tabulka 47 obsahuje obecný popis systému metra dle [253] s přiřazenými bloky a rozhraní systému (technickými a funkčními) dle UGTMS [263].

Tabulka 47. Obecný model systému metra dle dat v pracích [253,263].

Aktiva	**Přiřazení bloků a rozhraní UGTMS**	**Vstupy**	**Výstupy**
Řídicí systém	Jádro systému UGTMS (provozní řídicí zařízení, traťové zařízení, vlakové zařízení, systém datové komunikace), Řízení (ústřední rozhraní s personálem, místní rozhraní s personálem, traťová zařízení, stávající uzávorování, plánování provozu), Informační systémy komunikace (např. zvuková komunikace, komunikace s personálem, s cestujícími), Stanice (monitorování pomocí CCTV, informace pro cestující na trati, zvuková komunikace),	vnější vlivy, plánování provozu, řízený systém METRO	zabezpečovací zařízení, řízený systém METRO

	Vlak (rozhraní s personálem obsluhy vlaku, diagnostika vlaku (pro údržbu), stav vlaku (z hlediska způsobilosti k provozu), vybírání jízdného (informace o lokalizaci), monitorování pomocí CTTV, zvuková komunikace), Údržba (systém údržby), Trakční napájení (řízení trakčního napájení)		
Zabezpečovací systém	Stanice (detekce ohně/ochrana proti ohni, detekce narušení nástupiště/tratě (např. cestující na kolejích), dveře nástupiště a/nebo dveře na konci nástupiště, rozhraní s jinými zařízeními (např. nouzové rukojeti, zařízení nouzového volání, zařízení pro detekce/uzavření nechtěného prostoru, odbavovací tlačítko/vlak připraven k odjezdu), Vlak (zařízení pro detekci překážek, vykolejení, ohně/kouře detekce nechráněného prostoru, zařízení pro uzavření nechráněného prostoru, rukojeť pro nouzové zastavení, uvolnění dveří/nouzové tlačítko), Infrastruktura (např. detekce zlomené kolejnice, detekce ohně a kouře, systém detekce narušení)	vnější vlivy, řídicí systém,	Řízený systém
Řízený systém METRO	Informační systémy, Stanice (pomocná zařízení (např. výtahy/eskalátory)), Vlak (dveře, pohon, brzdy, zařízení propojující vlak (např. elektrické mezi vozidlové propojky), rozhraní s jinými zařízeními (např. s osvětlením, vytápěním, větráním, klimatizací (HVAC), baterií), informace pro cestující ve vlaku), Infrastruktura (kolej, větrání tunelu, rozhraní s jinými zařízeními (např. tlakovými uzávěry)), Trakční napájení (vysokonapěťový vypínač)	vnější vlivy, zabezpečovací systém, řídicí systém	řídicí systém, kvalita provozu a dopravní výkon, snížení dopadů pohrom (OSM)

Specifické vlastnosti systému pražského metra jsou podrobněji popsané v práci [253]. Funkce, funkční vazby a obecné požadavky na vykonávání funkcí systému UGTMS jsou definované v normě [263]. Požadavky jsou označené pro každou úroveň automatizace zvlášť jako povinné, podmíněné anebo volitelné.

Uvedené funkce a členění slouží pro vysokoúrovňové zadávací požadavky na systém. Neposkytují však detailní popis vazeb funkcí, parametrů jednotlivých subsystémů, nároků na bezpečnost dílčích systému a celého systému (tj. integrální bezpečnost – kvalitu). Zmíněné vlastnosti je nutné vždy specifikovat dle lokálních požadavků a podmínek návazných a nadřazených systémů, včetně vazeb na povrchovou dopravu, geologických a klimatických podmínek, míry ohrožení všech relevantních pohrom apod.

Protože v předložené práci nás zajímají otázky kybernetické bezpečnosti, tak se vymezíme na požadavky a vlastnosti jádra systému UGTMS, které tvoří kritickou část systému řízení a jeho rozhraní, tj. zvažujeme:

- provozní řídící zařízení,

- traťové zařízení (zahrnuje bodový přenos mezi kolejí a vlakem),
- vlakové zařízení (zahrnuje lokalizaci, měření rychlosti a času),
- systém datové komunikace (zahrnuje datovou komunikaci traťového zařízení s provozním řídicím zařízením, komunikaci mezi traťovým zařízením a vlakovým zařízením).

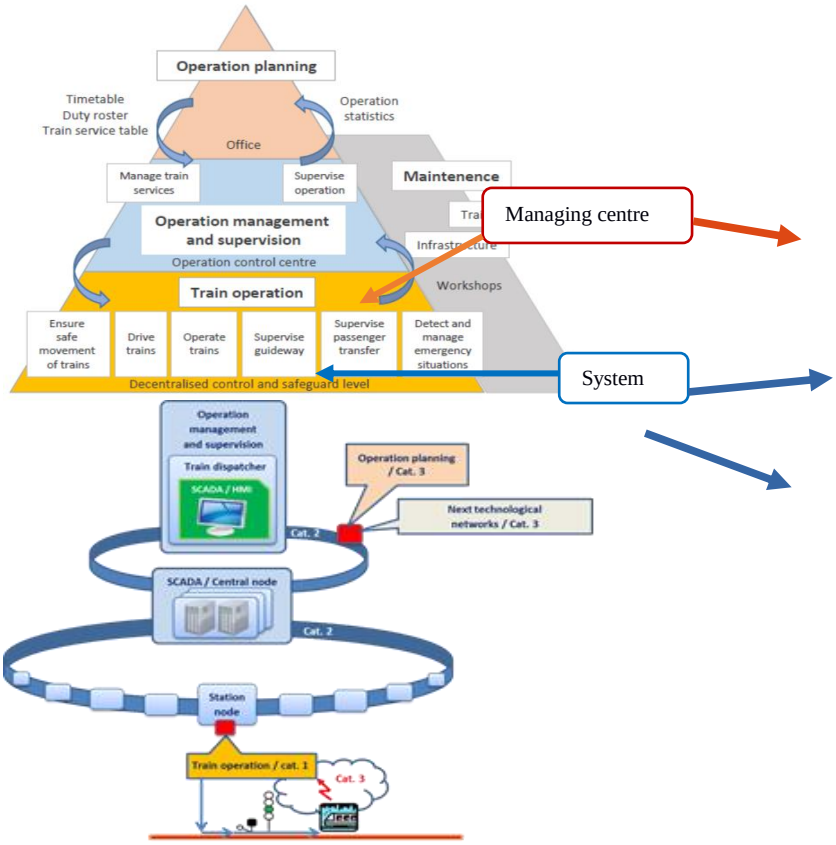
Obrázek 55 popisuje vztah mezi teorií, obecným popisem systému a reálným stavem.

V horní části obrázku 55 je znázorněno členění systému UGTMS dle úrovně řízení (provozní plánování, řízení provozu, řízení vlaků), na pravé straně reálné uspořádání systému ASDŘ-D pro řízení dopravy pražského metra, tj. dispečerská pracoviště spojení komunikačním kanálem s centrálními uzly systému (na této vrstvě jsou znázorněné i rozhraní na další technologické či podnikové systémy), centrální uzly jsou propojené vlastní komunikační infrastrukturou se staničními, traťovými subsystémy. Červené body na pravé straně obrázku 55 značí kritická komunikační rozhraní a přenosové prostředí dle [41]. Označení Cat. 1-3 znamená kategorii přenosového prostření (systému) dle drážního standardu EN 50159 [245].

Při jisté míře abstrakce lze ke klasifikaci kyber-fyzického systému dle obrázku 55 přiřadit bloky systému UGTMS a reálné prvky řídicího systému ASDŘ-D pražského metra:

- řídicí centrum – provozní řídicí zařízení – centrální uzly systému ASDŘ-D (respektive staniční řídicí uzly),
- systém – traťové a vlakové zařízení – staniční systémy a rozhraní, traťové přístupové body, vlakové komunikační jednotky, vlakové počítače,
- přenosové prostředí A, B dle obrázku 55 – systémy datové komunikace – síť dispečerského centra, síť staničních a traťových uzlů, rádiové přenosové prostředí.

Kritickou analýzou výše popsaného systému řízení se zjistí místa, ve kterých lze narušit kybernetickou bezpečnost.



Obrázek 55. Model pro řízení kybernetické bezpečnosti systému dle EN 62290 a reálný stav v metru [41] – červeně jsou označena nedostatečně zabezpečená místa.

Podle [265] jsou nejvyšší rizika (tj. velké dopady a vysoká pravděpodobnost jejich výskytu) spojena s:

- selháními procesů a lidskými chybami na všech úrovních systému řízení bezpečnosti,
- vzájemným propojením funkcí,
- chybami systému řízení bezpečnosti (SMS): chybná metodika pro identifikaci ohrožení a analýzu rizik na vyšší úrovni SMS; nepochopení požadavků a informací z jiné úrovně SMS; chybějící vstupní informace,
- jiné nepředvídatelné události a lidské faktory (vnitřní, vnější faktory nebo nebezpečné útoky).

Doporučená generická opatření dle [266] jsou:

- zavést kvalitní / bezpečné a monitorované procesy údržby a provozu do provozních předpisů stanice,
- použít bezpečnostní plán při návrhu, konstrukci a řízení změn, který je zaměřen na odstranění selhání systému a mít plán pro zvládání selhání systému při provozu,
- zavést pravidelná školení, zkoušení a cvičení zaměstnanců; potvrzení funkce E/E/PE [247] a zpětné vazby,
- zajistit bezpečnost, vysokou kvalitou nainstalovaných systémů dle požadavků [266, 267],
- pravidelné audity, hodnocení schopností a zajistit nezávislost řešených týmy, atd.

Selhání kybernetického systému

Řídící a řízené systémy v metru se tvoří distribuovanou strukturu s řadou uzlů systému a většina příkazů nebo akcí dispečera je podmíněna správnými informacemi a sadou potvrzení zpráv, jsou zde možností narušení provázanosti. Zvážíme tři původce kybernetických rizik, které jsme odhalily na základě údajů v provozní dokumentaci [41,152] (obrázek 55 a tři nedostatečně zabezpečená místa) a pro ně metodou What, If stanovíme dopady. V prvním případě jde o dopady, když dojde k průniku rozhraní, které je označeno na obrázku 55 jako "provozní plánování (operation planning)“. V druhém případě jde o dopady, když dojde k průniku rozhraní, které je na obrázku 55 označeno jako "provoz vlaku (train operation)“. Ve třetím případě jde o dopady proniku ve volném prostoru, kterým probíhá radiová komunikace mezi řidičem a dispečinkem, označeném na obrázku 55 jako „cat 3“.

Každý z případů má specifické rysy. V prvním případě jde o rozhraní mezi systémem dohledu a systémem řízení. V druhém případě jde o rozhraní mezi různými úrovněmi integrity bezpečnosti (SIL). Ve třetím případě jde o otevřené prostředí, a útočník může přenášené zprávy pozměnit anebo pomocí nich proniknout do uzavřeného systému. Tabulka 48 ukazuje výsledky aplikace metody What, If. Hodnocení provedli 4 experti pomocí stupnice pro dopady: nevýznamné; okrajové; významné; kritické; a katastrofální, která je podrobně charakterizována v dokumentaci [41] a vychází z normy EN 50126 [244].

Tabulka 48. Dopady narušení systému kybernetické bezpečnosti na veřejné a metra aktiv [41].

Aktiva	**Dopady**
Případová studie 1 – *(hrozby: narušení systému, ztráta integrity systému, ztráta ovládání)*	
Lidské životy, zdraví a bezpečí	Zaměstnanci: okrajové; pouze nepřímé dopady způsobené zmatením dispečera a jeho špatným rozhodnutím. Cestující: okrajové; pouze nepřímé dopady způsobené zmatením dispečera a jeho špatným rozhodnutím. Lidé mimo metro: nevýznamné; katastrofální pouze u složitějšího teroristického útoku, sérii příkazů (nepravděpodobné).

Majetek	Metro: okrajové. Veřejný: okrajové; škody způsobené panikou a drobnými krádežemi.
Životní prostředí	Nevýznamné.
Veřejné blaho	Okrajové; panika a možné poškození dobrého jména.
Metro – doprava	Významné; přímé dopady na pohyb vlaku, zhoršení dopravy a zpoždění.
Finance a jiné ztráty	Metro: významné; ztráty zisku kvůli zastavení provozu metra, poškození na dobré vůli. Veřejné: kritický; ztráta možnosti přepravy
Případová studie 2 *(hrozby: přerušení dopravy, ztráta ovládání)*	
Lidské životy, zdraví a bezpečí	Zaměstnanci: kritický; jednotlivá úmrtí nebo vážná zranění. Cestující: katastrofální; mnoho úmrtí nebo více těžkých zranění. Lidé mimo metro: kritický; způsobené panikou a pohybem mnoha lidí.
Majetek	Metro: Kritická – ztráta důležitých komodit. Veřejný: Okrajové; způsobené panickým pohybem lidí a rabováním.
Životní prostředí	Nevýznamné.
Veřejné blaho	Okrajové; panika a možné poškození dobrého jména.
Metro – doprava	Významné – přímé dopady na pohyb vlaku, zhoršení dopravní situace a zpoždění.
Finance a jiné ztráty	Metro: významné; ztráty zisku kvůli zastavení provozu metra, poškození dobrého jména. Veřejné: kritické; ztráta možnosti přepravy
Případová studie 3 – *(hrozby: narušení systému, ztráta integrity systému, ztráta ovládání)*	
Lidské životy, zdraví a bezpečí	Zaměstnanci: okrajové; pouze nepřímé dopady způsobené zmatením dispečera a jeho špatným rozhodnutím. Cestující: okrajové; pouze nepřímé dopady způsobené zmateným dispečerem a jeho špatným rozhodnutím. Lidé mimo metro: nevýznamné; katastrofální u složitějšího teroristického útoku.
Majetek	Metro: okrajové. Veřejné: okrajové; způsobené panikou a drobnými krádežemi.
Životní prostředí	Nevýznamné.
Veřejné blaho	Okrajové; panika a možné poškození dobrého jména.
Metro – doprava	Významné; přímé dopady na vlaku, zhoršení dopravní situace a zpoždění.
Finance a jiné ztráty	Metro: významné; ztráty zisku kvůli zastavení provozu metra, poškození dobrého jména. Veřejné: kritický; ztráta možnosti dopravy.

Kritické hodnocení výsledků v [41,152] ukazuje zranitelná místa metra v oblasti kybernetické bezpečnosti. Pro snížení odhalených zranitelností a zlepšení kybernetické bezpečnosti je třeba upravit legislativu. Jde především o opatření na rozhraní systému dohledu a systému řízení metra. To znamená zavést účinné řízení rizik – na všech úrovních. Je rovněž

nezbytné zavést jednotnou terminologii do řízení bezpečnosti a správně definované stupnice pro hodnocení kritičnosti aktiv, kritičnosti interdependences a rizik v systémovém pojetí.

Proto vlastníci a provozovatelé systémů jako je metro a systémy řízení musí zajistit přinejmenším následující úkoly:

- aplikovat řízení rizik zacílenou na integrální bezpečnost,
- systémy řízení a dohledu musí zahrnovat všechny zainteresované strany (subdodavatele, dodavatele atd.) - dostupnost, odpovědnost, spolehlivost (uplatňování standardů IT z oblasti bezpečnosti a zabezpečení jako jsou TQM například COBIT, ITIL, ISMS, ICS) [152],
- zavést proces pro řízení bezpečnosti PSM (proces of safety management), tj. definovat nejdůležitější funkce, jejich parametry a řídit je (včetně spolehlivosti, dostupnosti, udržovatelnosti a bezpečnosti a / nebo zabezpečení; RAMS), analyzovat chyby, především na rozhraní se systémy různé podstaty; tj. zvažovat nejen technické parametry, ale i ostatní související se změnami prostředí a lidským faktorem,
- posuzovat všechny důležité monitorované aktivity a provádět případné korekce,
- sledovat a posuzovat kvalitu informačního výkonu a identifikovat položky, které jsou zvláště citlivé z pohledu úrovně celkové bezpečnosti, anebo zabezpečení,
- provádět audit systému řízení z hlediska efektivity nákladů.

Výše uvedené požadavky přesahují legislativní požadavky, protože jsou multidisciplinární a zahrnují více subjektů.

Dopady selhání elektrické energie na provoz metra

Jak již bylo uvedeno dříve, elektrická přenosová soustava je systém zařízení zajišťující přenos elektrické energie od výrobců k odběratelům (spotřebitelům). Výroba i spotřeba elektrické energie musí být v každém okamžiku vyvážená, jelikož v současné době a za využití stávajících technologií, nedokáže lidstvo elektrickou energii efektivně skladovat. Výkyvy ve výrobě či odběru mohou mít za následek nestabilitu elektrické přenosové soustavy a její výpadky. Obecně lze výpadky kategorizovat dle dvou parametrů: času (tj. doby, po kterou trvají) a prostoru (tj. oblasti, kterou zasáhnou) [268].

Na základě dat [252,269,270] a znalostí uvedených již výše je pražské metro složitý systém systémů skládající se z mnoha subsystémů. Jednotlivé subsystémy jsou mezi sebou propojeny prostřednictvím vazeb a toků. Provoz pražského metra je plně závislý na elektrické energii (pohyb souprav, osvětlení, vzduchotechnika, sdělovací zařízení, zabezpečovací zařízení, strojní zařízení atd. Elektrickou energii lze z hlediska systémového inženýrství definovat jako tok energie zajišťující spolehlivost a funkčnost jednotlivých subsystémů. Pro ocenění rizik byla použita data a poznatky z prací [269,270] a metody rizikového inženýrství, především What, If [15].

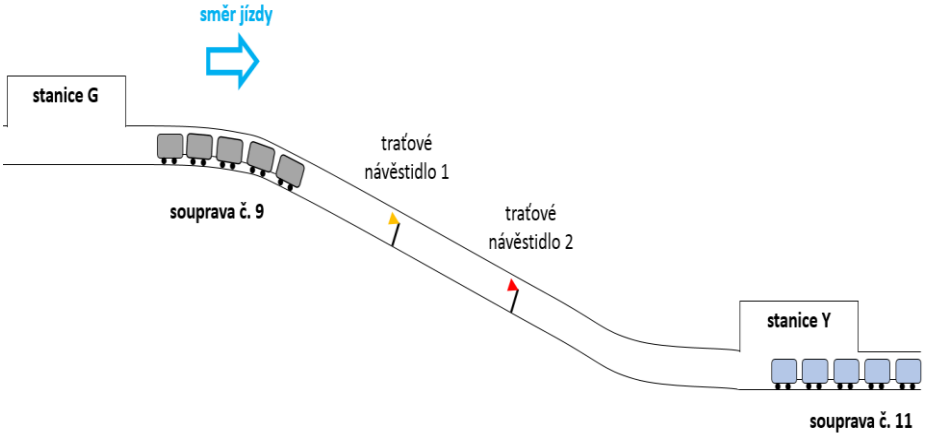
Vazby v systému metra jsou povahy technické „stroj-stroj“, povahy smíšené „člověk-stroj“ a s rozvojem počítačů také povahy „stroj-počítač“ a „člověk-počítač“. Propojení mezi provázanými systémy vedou k existenci vzájemných závislostí, které musí být zohledněny při všech fázích řízení bezpečnosti technologických systémů. Cílem řízení technologických systémů je zajistit bezpečí za podmínek normálních, abnormálních a kritických.

Provoz metra využívá poznatky z mnoha oblastí fyziky např. mechaniky (statika, dynamika), vlastností gravitačního pole Země, elektrického i magnetického pole. Pro zajištění bezpečí lidí jsou velmi důležité poznatky ohledně dynamiky pohybu soupravy metra, elektrodynamického brzdění se stejnosměrným trakčním motorem s cizím buzením, elektrodynamického brzdění s asynchronním trakčním motorem a magnetizačních proudů [270].

Při stanovení dopadů výpadku elektrické energie na metro byla použita data [12,252,270]. Je třeba uvést, že selhání dodávek elektrické energie do pražského metra má dopady na veškeré systémy metra, které ke své činnosti elektrickou energii využívají. Pro analýzu a ocenění rizik

vzniklých při výpadku elektrické energie je nutné předem pochopit a popsat chování všech systémů pražského metra a podrobně analyzovat veškeré probíhající procesy, vazby a toky mezi jednotlivými systémy. V práci [270] jsou důkladně rozebrány 4 případové studie; zde uvedeme pro ukázku jednu.

Zvažujeme situaci znázorněnou na obrázku 56, tj. dvě stanice G a Y propojené traťovými tunely, které se nachází v různých nadmořských výškách. Pro jednoduchost je zde zvážen pouze jeden z traťových tunelů sloužící pro jízdu ve směru ze stanice G do stanice Y. V případové studii se nacházejí soupravy č. 9 a č. 11 (obě soupravy jsou typu M1). Stanice G se nachází v hloubce 38 metrů. Vstup do stanice G je zajištěn prostřednictvím dvou vestibulů. Oba vestibuly jsou s nástupištěm spojeny spojovacími tunely. V každém spojovacím tunelu jsou instalovány dva eskalátory. Nadmořská výška nástupiště stanice G činí 371 m.n.m.



Obr. 56. Rozmístění souprav v tunelu v době výpadku elektrické energie [270].

Stanice Y se nachází v hloubce 36 metrů. Vstup do stanice Y je zajištěn prostřednictvím dvou vestibulů. Oba vestibuly jsou s nástupištěm propojeny spojovacími tunely. V každém spojovacím tunelu jsou instalovány dva eskalátory. Nadmořská výška stanice činí 330 m.n.m.

Délka traťového tunelu mezi stanicí G a stanicí Y činí 1100 metrů. Rozdíl nadmořských výšek stanic je 41 metrů. Podélný sklon v traťovém tunelu je 37.2 ‰.

K výpadku elektrické energie dochází v pondělí v 7:36 (SEČ). V čase výpadku se souprava č. 9 nachází v traťovém tunelu - jede do stanice Y. Souprava č. 11 jede ze stanice Y. Z obrázku 56 je zřejmé, že souprava č. 9 se v době výpadku nachází v pohybu zrychleném. Po ztrátě napájení trakčních motorů pokračuje souprava v pohybu, který závisí na: jízdních odporech soupravy, hmotových sil setrvačnosti, odporu stoupání, přídavném odporu oblouku a odporu brzdícím. Brzdící odpor je ovlivněn zásahem vlakového zabezpečovacího zařízení Matra, které zastaví soupravu před traťovým návěstidlem číslo 2. Souprava č. 11 se v době výpadku nachází též v pohybu zrychleném v tunelu, zastaví pomocí brzdného zařízení (ve sledovaném případě jede do kopce, a proto po zastavení se použije pneumatická brzda, a když výpadek elektrické energie trvá dlouho, tak po vyčerpání vzduchu nouzové mechanické zařízení (podrobnosti jsou v technické dokumentaci [252]). Tím vznikne nouzová situace, ve které je třeba řešit ochranu cestujících i ochranu majetku.

Při analýze dopadů předmětné nouzové situace zvažujeme chráněná aktiva: životy a zdraví; majetek soupravy metra kabina strojvedoucího, trakční výzbroj, brzdné systémy, osvětlení prostoru pro cestující, ventilace prostoru pro cestující, dveřní systémy, sdělovací zařízení, zabezpečovací zařízení, EPS, náhradní zdroje elektrické energie, traťový tunel a energetické toky. Předmětná chráněná aktiva jsou:

- životy a zdraví cestujících a životy a zdraví strojvedoucího,
- majetek (technologie, infrastruktura, objekty, zařízení), tj. soupravy metra; traťový tunel; kabina strojvedoucího a řídící pult strojvedoucího; trakční motor DK 117V; brzdné systémy - elektrodynamická brzda, pneumatická brzda, střídačová brzda, kompresorové jednotky,

vzduchové potrubí, zásobníky stlačeného vzduchu; osvětlení prostoru pro cestující - hlavní osvětlení prostoru pro cestující, nouzové osvětlení prostoru pro cestující; ventilace prostoru pro cestující - hlavní ventilátory, pomocné ventilátory; dveřní systémy - boční dveřní systémy, čelní dveřní systémy; sdělovací zařízení - vlaková část radiostanice VKV, vlakový rozhlas, nouzové telefonní spoje v traťovém tunelu; zabezpečovací zařízení - mobilní část vlakového zabezpečovače Matra; elektrická požární signalizace (EPS) - teplotní čidla v trakčních kontejnerech a skříních rozvaděčů, optická kouřová čidla v prostorách pro cestující; náhradní zdroje elektrické energie - vozidlové baterie, statické měniče určené pro dobíjecí vozidlových baterií; traťový tunel - hlavní osvětlení traťového tunelu, nouzové osvětlení traťového tunelu, návěstidlo traťového zabezpečovacího zařízení ESA 11 M, přívodní (napájecí) kolejnice,

- toky - energetické - napájení soupravy z přívodní kolejnice, palubní síť 400 V, palubní síť 110 V.

Dopady výpadku elektrické energie na soupravu č. 9 a soupravu č. 11 jsou v tabulce 49.

Tabulka 49. Dopady výpadku elektrické energie zjištěné metodou What, If [270,271].

Chráněná aktiva		**Dopady**
Životy a zdraví cestujících		možné úmrtí přítomných lidí možné zranění přítomných lidi
Život a zdraví strojvedoucího		možné úmrtí strojvedoucího možné zranění strojvedoucího
Majetek	soupravy metra	výskyt velkého množství osob, vznik paniky, možnost ušlapání, výpadek všech nezálohovaných systémů
	traťový tunel	výpadek napájení přívodní kolejnice, výpadek traťového zabezpečovacího zařízení, výpadek nouzových telefonních spojů Kabina
Kabina strojvedoucího	řídící pult strojvedoucího výpadek zařízení, ztráta ovládání a řízení	výpadek zařízení, ztráta ovládání a řízení soupravy, znemožnění sledování zobrazovaných informací na displeji řídícího pultu
Trakční výzbroj	trakční motor DK 117V	výpadek zařízení, ztráta pohonu soupravy
Brzdné systémy	elektrodynamická brzda	výpadek napájení trakčního motoru, brzdný účinek není ovlivněn
	pneumatická brzda	výpadek zdroje stačeného vzduchu, brzda v provozu v závislosti na množství stlačeného vzduchu v zásobnících
	střídačová brzda	výpadek zdroje stačeného vzduchu, brzda v provozu v závislosti na množství stlačeného vzduchu v zásobnících

	kompresorové jednotky	výpadek zařízení, znemožní výroby stačeného vzduchu pro brzdové ústrojí
	vzduchové potrubí	ztráta zdroje stlačeného vzduchu
	zásobníky stlačeného vzduchu	ztráta zdroje stlačeného vzduchu
Osvětlení prostoru pro cestující	hlavní osvětlení	výpadek zařízení, ztížená prostorová orientace cestujících
	nouzové osvětlení	výpadek zařízení, ztížená prostorová orientace cestujících
Ventilace prostoru pro cestující	hlavní ventilátory	výpadek zařízení a problémy lidí s dýcháním
	pomocné ventilátory	výpadek zařízení a problémy lidí s dýcháním
Dveřní systémy	boční dveřní systémy	výpadek zařízení, znemožnění automatického otvírání bočních dveří
	čelní dveřní systémy	výpadek magnetických zámků bočních dveří, odemknutí bočních dveří Sdělovací
Sdělovací zařízení	vlaková část radiostanice VKV	výpadek zařízení, znemožnění komunikace strojvůdce s vlakovým dispečinkem
	vlakový rozhlas	výpadek zařízení, znemožnění komunikace strojvůdce s cestujícími
Zabezpečovací zařízení	mobilní část vlakového zabezpečovacího zařízení Matra	výpadek zařízení, znemožnění zabezpečení jízdy soupravy
Elektrická požární signalizace (EPS)	teplotní čidla v trakčních kontejnerech a skříních rozvaděčů	výpadek zařízení, znemožnění automatické detekce vzniklého požáru
	optická kouřová čidla v prostorách pro cestující	výpadek zařízení, znemožnění automatické detekce vzniklého požáru
Náhradní zdroje elektrické energie	vozidlové baterie	znemožnění dobíjení
	statické měniče určené pro dobíjení vozidlové baterie	výpadek zařízení, znemožnění dobíjení vozidlové baterie
Energetické toky	napájení soupravy z přívodní kolejnice	výpadek napájení soupravy
	palubní síť 400 V	výpadek napájení kompresorů vzduchového potrubí, ventilátorů prostoru oddílu pro cestující a strojvedoucího
	palubní síť 110 V	výpadek osvětlení prostor pro cestující a kabiny strojvedoucího, výpadek elektronických přístrojů a dobíjecích jednotek pro vozidlové baterie

Z tabulky 49 vyplývá, že selhání elektrické energie má dopady na všechna chráněná aktiva. Za účelem zmírnění dopadů se dle technické dokumentace [253] využívá technologických zmírňujících opatření v podobě záložních zdrojů elektrické energie. Předmětné záložní zdroje jsou určeny pro: napájení vybraných elektronických zařízení v palubní síti 110 V (řídící pult strojvedoucího, nouzové osvětlení, pomocné ventilátory, mobilní část vlakového zabezpečovacího zařízení, systém EPS, magnetické zámky čelních dveří souprav). Dále je z vlastního zdroje zálohována mobilní část vlakového VKV rozhlasu. V traťovém tunelu je zálohováno nouzové osvětlení a nouzové telefonní spoje.

Z výše uvedeného vyplývá, že:

- při výstavbě metra nebyly zváženy požadavky přístupu All Hazard Approach (např. vypuknutí požáru v prostorách soupravy během výpadku elektrické energie),
- při ukončení pohonu soupravy je nouzové řešení nejisté a neodzkoušené, jde o přerušení výkonu kompresorů brzdových ústrojí a přerušení dobíjení vozidlových baterií,
- nejsou připraveny scénáře řešení pro možné selhání vozidlových baterií, staničních baterií a UPS.

Proto je třeba při výpadku elektrické energie provést evakuaci. Evakuace cestujících ze soupravy č. 9 je závislá na charakteru místa, v jakém se souprava č. 9 bude nacházet. V případě, že souprava č. 9 dojede do stanice, cestujícím bude umožněno vystoupit na nástupní plochu stanice. V případě, že souprava č. 9 nedojede do stanice, bude provedena evakuace cestujících traťovým tunelem. Postup evakuace bude probíhat dle technické dokumentace [272]. Dojezd soupravy č. 9 od traťového návěstidla číslo 2 do stanice je závislý: na odporu stoupání (podélném sklonu, ve kterém se souprava nachází), hmotnosti soupravy, jízdních odporů soupravy, hmotových sil setrvačnosti, přídavném odporu oblouku a zásobách stačeného vzduchu pro brzdové systémy. Pokud zásoby stlačeného vzduchu poklesnou pod předem stanovenou hodnotu, dojde k zabrzdění soupravy.

Evakuace cestujících ze soupravy č. 11 je závislá na konečné poloze soupravy. V případě rychlé reakce strojvedoucího a zabrzdění soupravy bude evakuace probíhat z posledního vozu soupravy na nástupištní plochu. V případě, že souprava stihne opustit prostory stanice, bude evakuace cestujících provedena z traťového tunelu. Z uvedeného vyplývá, že při evakuaci cestujících se spoléhá na reakci strojvedoucího a na obecný postup evakuace tunelem, který dle [272] dosud nebyl odzkoušen.

Metro je důležitá část dopravní infrastruktury, a proto je třeba na základě simulace dopadů vybraných možných selhání [271] připravit a procvičit postupy pro:

1. Vyproštění souprav uvázlých v tunelu metra.
2. Zvládnutí selhání záložních zdrojů.
3. Aktivaci dieselagregátů.
4. Evakuaci cestujících, a to zvláště ve 2 stanicích, kdy souprava nedojede do stanice.
5. Odezvu na blackout, včetně konkrétních odpovědností zaměstnanců Dopravního podniku hl. m. Prahy.

5.9.4.4. Doprava letecká

Vzdušný prostor kolem nás je využíván mnoha různými subjekty, které mají rozdílné možnosti a požadavky. Zatímco rekreační a sportovní letci preferují volnost pohybu a co nejnižší nároky na finančně náročné přístrojové vybavení letadla, osobní obchodní letecká doprava vyžaduje nejvyšší úroveň bezpečnosti, spolehlivosti a přesnosti poskytovaných služeb.

V důsledku rozvoje mezinárodních aktivit se neustále zvyšují požadavky na propustnost vzdušného prostoru. Tím nevyhnutelně narůstají rizika spojená s letovým provozem. Ačkoliv je v letectví na bezpečnost kladen maximální důraz za všech okolností, dochází ve vzdušném prostoru k událostem, které jsou na hraně nebo i za hranou stanovených bezpečnostních limitů

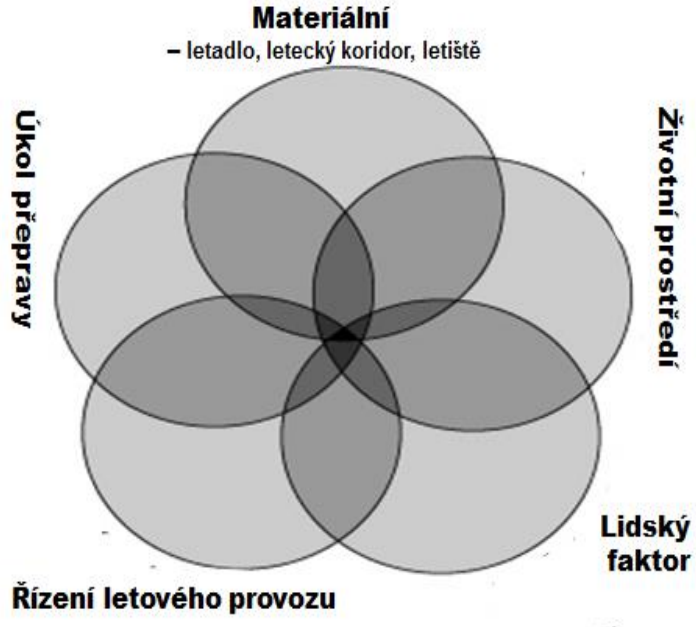
[273]. Může se jednat o výskyt přírodních pohrom, selhání lidského faktoru, technických zařízení na zemi i na palubách letadel, a také systému řízení letového provozu jako takového. Posledně zmíněná skutečnost je považována za velmi zásadní v posledních cca 25 letech, a proto je jí věnována velká pozornost při vzdělávání, výcviku i praxi. Cílem odstavce je pro vybrané letecké nehody uvést případové studie a vyhodnotit jejich dopady.

Systém řízení letového provozu musí být připraven na situace, které narušují letový provoz, ať už pocházejí zevnitř nebo z jeho okolí. V krajním případě může jít o letecké nehody bezprostředně ohrožující velké množství lidských životů. Za všech okolností musí být uděláno maximum pro zajištění bezpečného letového provozu v daném vzdušném prostoru. Jestliže má být rizikům pro letecký provoz rozumně předcházeno, je rozhodujícím prvkem pochopení příčin a plánování řešení možných nenadálých nebezpečných situací předem. Včasné uvedení postupů pro nenadálé situace vyžaduje rozhodnou iniciativu a kvalitní, včasné a rychlé provedení správných opatření.

Systém letecké dopravy tvoří několik vzájemně propojených otevřených systémů, obrázek 57, tj. jde o SoS. Jeho řízení tak, jako každé jiné představuje kulturu, procesy a struktury zaměřené na efektivní řízení potenciálních příležitostí a možných nežádoucích důsledků.

Letecký provoz je řazen do 4 základních kategorií [274], přičemž nejvíce markantní jsou obchodní letecká doprava a letecké práce a všeobecné letectví. Zmíněné kategorie mají svou specifickou povahu a není možné využívat stejné principy pro udržení bezpečnosti na určité úrovni pro obě zmíněné skupiny. Obchodní letecká doprava (OLD) je skupina provozovatelů letadel, kteří jsou oprávněni provádět dopravu osob, zvířat, věcí a pošty za úplatu. OLD je dále dělena na pravidelnou a nepravidelnou, vnitrostátní a mezinárodní [275].

Všeobecné letectví je dle [275] děleno do skupin: letecké práce - letecké činnosti, při nichž letecký provozovatel využívá letadlo k pracovní činnosti za úplatu (mimo jiné vyhlídkové lety, letecké školy); letecké činnosti pro potřeby státu – tj. lety pro potřebu státních činitelů, pro výkon státní správy; rekreační a sportovní létání, které není prováděno za účelem zisku; a letecká veřejná vystoupení a soutěže.



Obr. 57. Systémy tvořící systém letecké dopravy.

Legislativa rozlišuje 3 základní kategorie leteckých událostí z pohledu závažnosti nehody [275], a to: letecká nehoda (LN); vážný incident (VI); a incident (I). Definice pojmů jsou uvedeny v leteckém předpise L13 [275]. Letecká nehoda je událost spjatá s provozem letadla, které se, v případě pilotovaného letadla, stala mezi dobou, kdy jakákoli osoba nastoupila do

letadla s úmyslem vykonat let a dobou, kdy všechny takové osoby letadlo opustily a při které byla některá osoba smrtelně, nebo těžce zraněna nebo bylo letadlo zničeno či poškozeno tak, že poškození nepříznivě ovlivnilo pevnost konstrukce, výkon nebo letové charakteristiky. Incident je událost jiná než letecká nehoda, spojená s provozem letadla, která ovlivňuje nebo by mohla ovlivnit bezpečnost provozu. Zpravidla se jedná o chybnou činnost osob, či nesprávnou činnost leteckých a pozemních zařízení, jejíž důsledky však zpravidla nevyžadují předčasné ukončení letu [276].

Základní kámen právních předpisů České Republiky v oblasti civilního letectví je zákon č. 49/1997 Sb., o civilním letectví. Kromě základního vymezení pojmů, zřizuje zákon Úřad pro civilní letectví a popisuje tvorbu a vedení leteckého rejstříku. Další část národního leteckého práva tvoří vyhlášky ministerstva dopravy. Posledním pilířem české legislativy ve zmíněné oblasti jsou právní předpisy vycházející ICAO (Mezinárodní organizace pro civilní letectví).

Definici letecké nehody uvádí předpis L13 - o odborném zjišťování příčin leteckých nehod [275], dle kterého letecká nehoda je událost spojená s provozem letadla, která se, v případě pilotovaného letadla, stala mezi dobou, kdy jakákoliv osoba nastoupila do letadla s úmyslem vykonat let a dobou, kdy všechny takové osoby letadlo opustily, nebo při které:

- některá osoba byla smrtelně nebo těžce zraněna následkem přítomnosti v letadle, nebo · přímého kontaktu s kteroukoli částí letadla, včetně částí, které se od letadla oddělily, nebo přímým působením proudu plynů (vytvořených letadlem), s výjimkou případů, kdy ke zranění došlo přirozeným způsobem, nebo způsobila-li si je osoba sama nebo bylo způsobeno druhou osobou, nebo jestliže šlo o černého pasažéra ukrývajícího se mimo prostory normálně používané pro cestující a posádku,
- letadlo bylo zničeno, nebo poškozeno tak, že poškození: nepříznivě ovlivnilo pevnost konstrukce, výkon nebo letové charakteristiky letadla, a · vyžádá si větší opravu nebo výměnu postižených částí,
- letadlo je nezvěstné, nebo je na zcela nepřístupném místě.

Prvním krokem k zavedení systematického vyšetřování nehod v oblastech letectví byla ratifikace Chicagské úmluvy o mezinárodním civilním letectví v roce 1944, jejíž součástí bylo zavedení a provádění odborného zjišťování příčin leteckých nehod. Zmíněného úkolu se od počátku ujímá ministerstvo dopravy ČR, které ve své funkci působí dva roky. Následně přebírají jeho úkol následující organizace: státní letecká správa; ústřední správa civilního letectví; a státní letecká inspekce. V roce 1997 přebírá funkci úřad pro civilní letectví [275], který v roce 2003 zahajuje činnost ústavu pro odborné zjišťování příčin leteckých nehod, který společně s leteckou amatérskou asociací České Republiky (LAA ČR) působí na tomto poli dodnes.

V průběhu vývoje letectví docházelo k postupnému zvyšování bezpečnosti mechanické konstrukce letounů. To mělo za následek celkové snížení počtu leteckých nehod, jejichž hlavní příčinou byla mechanická porucha stroje [276].

Dále uvedeme výsledky studia ze dvou oblastí, a to civilní letecké dopravy a z oblasti malých letadel.

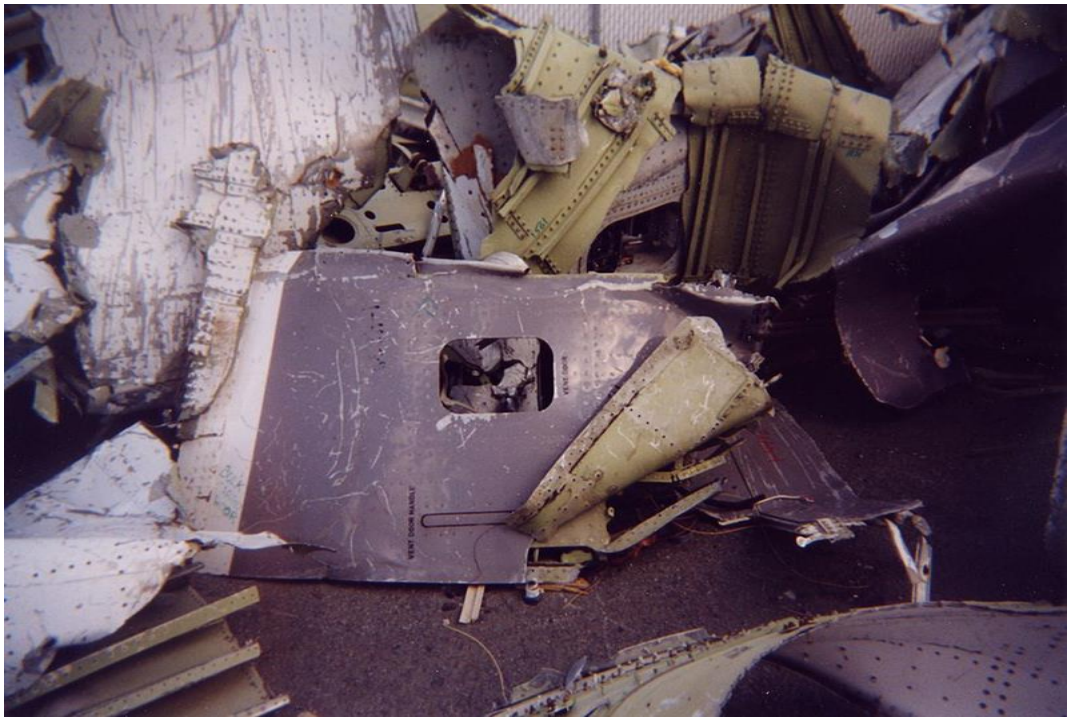
Letecké nehody velkých civilních letadel

Letecké nehody se nevyhýbají žádnému státu, jak ukazuje obrázek 58. Jen malá část z nich (cca 15%) byla bez lidských obětí. Letecké nehody jsou rekonstruovány na základě: úředních dokumentů; výpovědi účastníků; záznamů z černých skříněk; a z názorů odborníků. Pro názornost uvedeme několik příkladů leteckých nehod z [12], které byly získány z [277,278]:

1. Let Swissair 111, obrázek 59. Šlo o pravidelný letecký spoj společnosti Swissair mezi New Yorkem a Ženevou. Dne 2. září 1998 se stroj McDonnell Douglas MD-11, který na něm létal, zřítil poblíž Nového Skotska do Atlantského oceánu. Zemřelo všech 229 osob na palubě, což dělá z této nehody největší havárii, v níž účinkoval daný typ letadla, a druhou

největší leteckou havárii v historii Kanady. ***Příčinou havárie byl požár na palubě,*** který zachvátil elektrické rozvody, tvořené vysoce hořlavými materiály.

Obr. 58. Letecké nehody civilních letadel v Evropě v posledních 30 letech [279].



Obr. 59. Důsledek letecké nehody Swissair 111 dne 2. 9. 1998.

2. Let Aeroperú 603. Šlo o pravidelný spoj peruánských aerolinek z Limy do Santiaga de Chile. Krátce po startu dne 2. října 1996 po půlnoci vyslal Boeing 757-23A (reg. N52AW), který jej obsluhoval, nouzové volání a žádal letovou kontrolu o povolení k návratu do Limy pro rozsáhlé selhání základních přístrojů. Během návratu se však zřítil do Tichého oceánu.

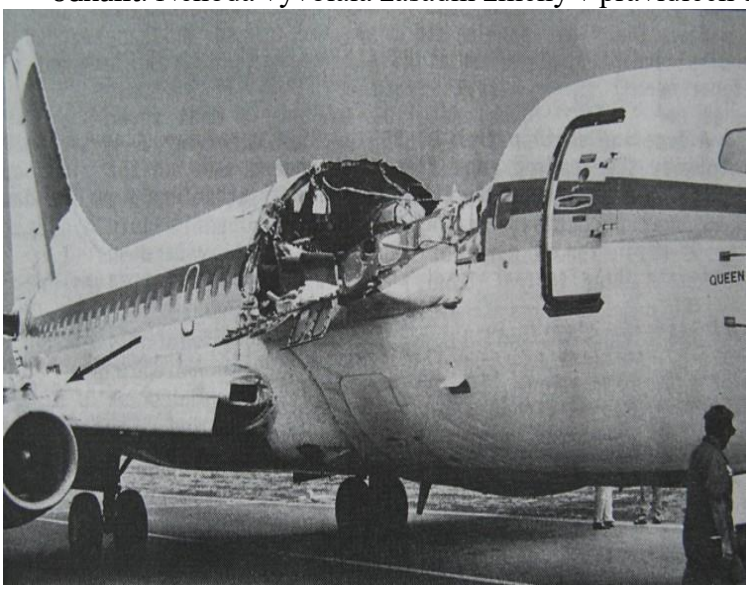
Zemřelo všech 70 osob na palubě. Vyšetřování prokázalo, že prvotní příčinou havárie bylo hrubé selhání údržby: její pracovník zapomněl odstranit pásku chránící během omývání letadla statické porty, což vedlo k selhání základních přístrojů (výškoměru a ukazatele rychlosti) a v důsledku toho k deaktivaci autopilota a zmatečným hlášením počítače. Ve tmě nad oceánem, kde nebyly k dispozici žádné orientační body, zavaleni desítkami falešných poplachů, protichůdných hlášení a nesmyslných údajů, se piloti nedokázali zorientovat v tom, kde letoun je a co dělá. K nehodě přispěl letecký dispečer, který pilotům na žádost o pomoc udal údaje o výšce ze své obrazovky – ne o výšce letadla. Dezorientovaný letoun klesl příliš nízko a roztříštil se o hladinu.

3. Letecké neštěstí na ostrově Tenerife. Dne 27. března 1997 se srazily se 2 boeingy uprostřed vzletové a přistávací dráhy na bývalém vojenském letišti Los Rodeos v horách na ostrově Tenerife, obrázek 60. a 61. Vyšetřování ukázalo, že letadlo PanAm: Boeing 747-121, vzlétlo bez povolení a KLM: Boeing 747-206B, popojížděl po ranveji. Situaci zkomplikovala mlha, nepřesné informace od dispečerů, neoznačené dráhy, spěch pilotů (v obou případech šlo o odkloněné lety). Zemřelo 583 lidí, tj. jde o největší leteckou katastrofu

Obr. 60. Důsledek letecké nehody na Tenerife dne 27. 3. 1997.

4. Let Aloha Airlines 243, obrázek 61. Při pravidelném spoji havajských aerolinek Aloha Airlines, létajícím z Hilo do Honolulu došlu dne 28. dubna 1988 u Boeingu 737-297 k explozivní dekompresi doprovázené dezintegrací stěn a stropu trupu za pilotní kabinou. Posádka nouzově přistála na 43 km vzdáleném letišti Kahului na ostrově Maui. Během nehody zahynula vrchní letuška, která byla během dekomprese vymrštěna z letounu, a osm osob utrpělo těžká zranění při explozi či po ní v důsledku zásahu létajícími předměty.

Dalších 57 osob utrpělo zranění lehká. Vyšetřování určilo za příčinu havárie kombinaci koroze a únavy materiálu a selhání údržby, která nebyla schopna riziko při kontrolách odhalit. Nehoda vyvolala zásadní změny v pravidlech údržby a kontroly opotřebení letadel.



Obr. 61. Letecká nehoda Aloha Airlines 243 dne 28. 4. 1988.

Civilní letecká doprava

Letecká doprava je nejbezpečnější formou přepravy, ve srovnání s jinými druhy přepravy je malý počet dopravních nehod, avšak jejich dopady v případě zničení letounu jsou fatální. Podle údajů IATA (International Air Transport Association - Mezinárodní asociace leteckých dopravců) např. v roce 2006 celosvětově došlo k 0.65 dopravním nehodám s fatálními následky na 1 milion letů. V počtu dopravních nehod existují značné rozdíly mezi regiony - nejbezpečnější jsou střední a západní Evropa, Severní Amerika a Austrálie, nejméně bezpečná je Afrika. Každý rok se také vyskytuje řada jevů, které v terminologii zabývající se nehodami a haváriemi označujeme jako skoro-nehody, tj. jevy, kde fatálním následkům zabránila rychlá reakce člověka, např. pilota, který nouzově přistál, když motory přestaly pracovat v důsledku nasátí ptáků do motoru.

Civilní letecká doprava ve světě v roce 2015 měla jen 16 fatálních nehod, což je doposud nejlepší výsledek v její historii [280]. Při těchto nehodách zahynulo 560 osob (pro srovnání s jinými druhy dopravy - jen v ČR za rok 2015 zahynulo na silnicích 660 osob). Uvedená statistika se vztahuje na letadla s minimální kapacitou 14 cestujících, přičemž celkový počet letů za uvedený rok dosáhl hodnoty asi 34 milionů, tj. úmrtí jednoho cestujícího při letecké nehodě připadá na asi 4 857 000 letů [280].

Pro specifický výzkum příčin civilních letadel s počtem cestujících 15 a více, jehož výsledky budou dále uvedeny, byla zpracována specifická databáze z dostupných informací z let 1909-2015 [12], která obsahuje více než 1900 událostí. Pomocí nástrojů rizikového inženýrství jsou roztříděny příčiny nehod a jsou přehledně podle příbuznosti zobrazeny pomocí diagramu rybí kosti (Fishbone diagram) [15], obrázek 62.

Analýzou předmětné databáze jsou rozlišeny následující příčiny:

- technické – spojené s letounem,
- technické – spojené s letištěm,
- řízení letového provozu – fyzické příčiny,
- řízení letového provozu – organizační příčiny,
- řízení letového provozu – kybernetické příčiny,

- útok na letadlo,
- útok na řízení letového provozu nebo letiště.

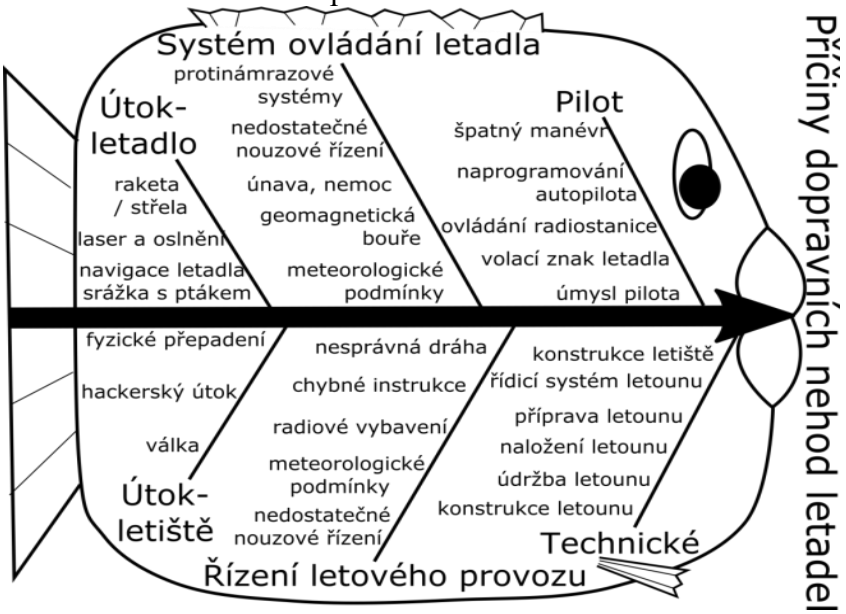
Dále uvedeme jejich podrobnější členění:

1. Technické – spojené s letounem:
    - konstrukční chyba letounu (chybná konstrukce a umístění palivové nádrže, chybná konstrukce výměníků, zřejmé možnosti elektrického zkratu, stabilita,...)
    - špatná údržba letounu
    - nesprávně naložený letoun
    - náhlá technická závada letounu (vysazení motoru, směrového kormidla nebo jiného důležitého zařízení)
    - selhání technického vybavení řídicího systému letadla (výpadek přístroje měřícího výšku letounu, výpadek radiového spojení s letištěm, …)
2. Technické – spojené s letištěm:
    - umístění letiště v území (moře, hory, vysoké stavby…)
    - konstrukční chyba při stavbě letiště (příliš krátká runway, runway ve směru, ve kterém je často protivítr ……)
    - stav runway (konstrukční chyba, nepořádek na letištní ploše, špatná údržba – nerovnosti, led, sníh, …)
    - chybí pozemní radar
    - náhlá technická závada přístrojů na řídící věži (špatná údržba, selhání technického vybavení řídicího systému na dispečerském stanovišti)
    - rozmístění techniky pro obsluhu letounu (tankování, vykládka a nakládka zboží, nástup a výstup lidí, ….)
    - fyzické zničení letiště (válka, loupežné přepadení, teroristický útok, …)
3. Řízení letového provozu – fyzické příčiny
    - umístění letounu na nesprávnou runway
    - překážky na runway
    - nedostatečné radiové vybavení letiště
    - nedostatek znalostí a zkušeností obsluhy letiště (pracovníka navigujícího pohyb letadla po letištní ploše)
    - nefunkční pozemní varovný systém udávající minimální bezpečnou nadmořskou výšku letounu u letiště
4. Řízení letového provozu – organizační příčiny
    - navedení letounu na nesprávnou dráhu při startu, letu i přistání (kolize letadel)
    - špatné zvážení meteorologických podmínek
    - odeslání chybných instrukcí letadlům kvůli selhání řídicího systému na dispečerském stanovišti (např. v důsledku výpadku elektrického proudu)
    - odeslání chybných instrukcí letadlu kvůli chybě dispečera
    - zmatek na dispečerském stanovišti
    - nedostatek pozemního personálu
    - chyba pozemního personálu
    - špatně rozdělené odpovědnosti
    - nedostatečná komunikace s piloty
    - nedostatek znalostí a zkušeností obsluhy na řídící věži
    - neexistence instrukcí pro podporu pilotů, kteří se dostanou do nenadálých nouzových až kritických situací
5. Řízení letového provozu – kybernetické příčiny
    - chybná monitorovací síť
    - chybný software

- nedostatečný hardware (špatné vyhodnocení dat, odeslání chybných instrukcí letadlům z důvodu selhání PC, zpoždění zpráv
- hackerský útok na řídící centrum vybavení dispečerské věže

6. Ovládání letadla
   - chyba pilota při ovládání letadla (kvůli zdravotnímu stavu, únavě, chybné informaci z řízení letového provozu, selhání kritického zařízení letadla v důsledku špatné údržby, chybnému vyhodnocení situace - úhel a rychlost pro vzlétnutí a přistání, náraz na plochu, vypnutí funkčního motoru místo vadného, - start, přistávání – požáry, vyjetí z dráhy, vyřazení přístrojů z činnosti v důsledku solární bouře, geomagnetické bouře apod.)
   - chyba pilota při vyhodnocení meteorologických podmínek
   - chyba pilota kvůli nedostatečné přípravě na zvládnutí nouzových podmínek (turbulence, snížená viditelnost, …)
   - chyba pilota - nepoužití protinámrazových systémů
   - chyba pilota při přípravě stroje k letu (špatné naprogramování autopilota před letem, špatně nastavený výškoměr, mylně nastavené výchozí údaje, např. u přetlakového systému)
   - chyba pilota při ovládání radiostanice
   - chybná spolupráce pilota a posádky
   - chyba pilota při ohlašování (použití chybného volacího znaku letadla - malý rozestup mezi letadly)
   - špatný úmysl pilota (změna kurzu, nereagování na pokyny z řídící věže nebo doprovodných letounů
   - neznalost pilota (neučí se postupy ovládání letadla při nenadálých nouzových až kritických situací - předcházení a zvládnutí vývrtky aj.)

7. Útok na letadlo
   - raketa / střela z jiného letadla či z pozemního cíle
   - zacílení laseru a oslnění pilota
   - špatný úmysl dispečera
   - špatný úmysl obsluhy na letišti (pracovníka navigujícího pohyb letadla po letištní ploše)
   - srážka letadla s ptákem.



Obr. 62. Roztřídění příčin dopravních nehod civilních letadel.

Z výčtu příčin dopravních nehod civilních letadel i z obrázku 62 je zřejmé, že příčin je mnoho a mají rozmanitý původ. Je třeba zdůraznit, že letectví je jedním z mála odvětví, které za zdroj rizika považují geomagnetické bouře vyvolané procesy na Slunci a mají k tomu uzpůsobené technické předpisy.

Jelikož se ukazuje, že u řady havárií se uplatňuje lidský faktor, a to nejen manuálně, ale i při rozhodování a řízení procesů, tj. jde o tzv. organizační havárie, je třeba na každém pracovišti pro řízení letového provozu je třeba mít zpracován plán [279], ve kterém:

- jsou řešena opatření pro zmírnění dopadů dopravní nehody způsobené chybou v řízení a zvládnutí odezvy,
- jsou stanoveny jasné odpovědnosti a je zajištěn důsledný důraz na jejich dodržování v provozu,
- je zvláštní pozornost věnována opatřením, která sníží dopady protiprávních činů,
- je uloženo pilotům letadel, která se stanou předmětem protiprávního činu, že musí vyvinout maximální úsilí, aby uvědomili o dané skutečnosti příslušné stanoviště Řízení letového provozu a oznámili mu jakékoli důležité okolnosti spojené s předmětným činem a jakoukoli odchylku od platného letového plánu vynucenou okolnostmi.

Opatření pro zmírnění dopadů dopravní nehody způsobené chybou v řízení a zvládnutí odezvy dle [281] jsou:

1. Přesměrování provozu pro vyhnutí se danému vzdušnému prostoru.
2. Zavedení zjednodušené struktury tratí daného prostoru.
3. Zajištění a provoz dostačujícího spojení „letadlo - země“, včetně předání odpovědnosti.
4. Zvláštní opatření k soustřeďování a rozšiřování letových a poletových hlášení z letadel.
5. Požadavek na letadla udržovat nepřetržitý poslech na zvláštních VHF kmitočtu „pilot - pilot“ ve stanovených prostorech.
6. Požadavek všem letadlům ve stanovených prostorech, aby měla stále rozsvícená navigační a proti srážková světla.
7. Požadavek a postupy pro letadla udržovat zvýšené podélné rozstupy, které mohou být stanoveny mezi letadly ve stejné cestovní hladině.
8. Požadavek na stoupání a klesání dostatečně vpravo od osy specificky stanovených tratí.
9. Stanovení postupů pro řízený vstup do prostoru, kde jsou uplatňovány postupy pro řešení nouzových situací, k zamezení jeho přetížení.
10. Požadavek, aby veškerý provoz v prostoru, kde jsou uplatňovány postupy pro řešení nenadálých situací, byl prováděn podle pravidel pro lety podle přístrojů (IFR), včetně přidělování IFR letových hladin.

Nástroje pro snížení výskytu dopravních nehod civilních letadel a pro zvládnutí odezvy

Pro odstranění řady příčin dopravních nehod civilních a pro jejich kvalitní zvládnutí se používají nástroje rizikového inženýrství, např. kontrolní seznamy, bezpečnostní audity, bezpečnostní plány, plány pro řízení rizik, operativní krizové plány apod. [1].

Příklad plánu řízení rizik pro letadlo je uveden v tabulce 50. V tabulce 51 je pak uveden plán pro letiště. Plán řízení rizik obsahuje čtyři základní položky, a to:

- oblast příčin rizika (technická, organizační, vnitřní příčiny, vnější příčiny, kybernetická)
- popis příčin rizika,
- pravděpodobnost výskytu a ocenění dopadů rizika,
- opatření pro zmírnění rizika a odpovědnosti.

Při ocenění dopadů a pravděpodobností nehod civilních letadel byla použity údaje ze sestavené databáze [12] a stupnice pro hodnocení velikosti ztrát a četnosti výskytu, kterou použilo 5 expertů z oblasti letového provozu: Malá – 5-20%, střední 20-45%, vysoká – 45-70%, velmi vysoká 70-95%.

Tabulka 50. Plán řízení rizik pro letadlo [281,282]. Opatření vydaly: IATA, NTSB = National Transportation Safety Board; ŘLP = Řízení letového provozu; SAS = Skybrary aviation safety.

Oblast rizika	Popis příčin rizika	Pravděpodobnost výskytu a dopady rizika	Opatření pro zmírnění rizika a odpovědnosti
Organizační	Ztráta orientace	Pravděpodobnost: malá Dopady: velké	Opatření: použití náhradních způsobů orientace - dle reliéfu terénu a požádání o pomoc řízení letového provozu [283] Odpovědnost: pilot [283]
	Chybné vyhodnocení situace	Pravděpodobnost: střední Dopady: velké	Opatření: provedení opravného manévru [283] Odpovědnost: pilot [283]
	Špatná spolupráce posádky	Pravděpodobnost: malá Dopady: střední	Opatření: okamžité zavedení pořádku a později změna posádky [284] Odpovědnost: velitel letadla [284]
	Nezvladatelný cestující	Pravděpodobnost: střední Dopady: střední	Opatření: pohovor, přikurtování k sedadlu, popř. oddělení od ostatních, přistání na vhodném letišti [284] Odpovědnost: velitel letadla [284]
Technické	Výpadek motoru	Pravděpodobnost: malá Dopady: střední	Opatření: zahájit nouzové klesání a vyslání zprávy na řízení letového provozu [285-287] Odpovědnost: pilot „letící" [285-287]
	Nefunkční výškoměr	Pravděpodobnost: malá Dopady: střední	Opatření: použití záložních systémů určení polohy [286] Odpovědnost: pilot [286]
	Úbytek kyslíku na palubě	Pravděpodobnost: malá Dopady: vysoká	Opatření: spuštění kyslíkových masek, vyslání zpráva na řízení letového provozu [288] Odpovědnost: pilot [288]
Narušení bezpečnosti z vnějších příčin	Požár v kabině	Pravděpodobnost: malá Dopady: velmi vysoké	Opatření: použití hasicích přístrojů na palubě, vyslání zprávy na řízení letového provozu, snaha o rychlé přistání [289] Odpovědnost: velitel letadla [289]
	Požár v zavazadlovém prostoru	Pravděpodobnost: malá Dopady: velmi vysoké	Opatření: nouzové přistání na nejbližším vhodném letišti [283] Odpovědnost: velitel letadla [283]
Narušení bezpečnosti z vnějších příčin	Velké propadnutí letounu	Pravděpodobnost: malá Dopady: střední	Opatření: opravný zásah v řízení letadla [290] Odpovědnost: pilot „letící" [290]
	Velký elektrický výboj	Pravděpodobnost: malá Dopady: vysoké	Opatření: okamžité převzetí manuálního řízení [289] Odpovědnost: pilot [289]
	Útok cizího letadla	Pravděpodobnost: malá Dopady: velmi vysoké	Opatření: nouzové přistání na nejbližším vhodném letišti [291] Odpovědnost: pilot „letící" [291]
Ky be	Ztráta spojení	Pravděpodobnost: střední	Opatření: nastavení nouzového kódu odpovídače letadla [292,293]

		Dopady: střední	Odpovědnost: pilot „letící” [292,293]
	Hackerský útok na systém řízení letadla	Pravděpodobnost: malá Dopady: velmi vysoké	Opatření: aplikace manuálního řízení [284] Odpovědnost: pilot „letící” [284]
	Podivné hlášení – neobvyklá aktivace senzorů	Pravděpodobnost: malá Dopady: velmi vysoké	Opatření: prověření varovných systémů, vyslání zpráva na řízení letového provozu [287] Odpovědnost: velitel letadla [287]

Tabulka 51. Plán řízení rizik pro letadlo [281,282]. Opatření vydaly: IATA, NTSB = National Transportation Safety Board; ŘLP = Řízen í letového provozu; SAS = Skybrary aviation safety.

Oblast rizika	**Popis příčin rizika**	**Pravděpodobnost výskytu a dopady rizika**	**Opatření pro zmírnění rizika a odpovědnosti**
Organizační	Neposkytnutí informací nebo poskytnutí špatných informací letadlu	Pravděpodobnost: nízká Dopady: velmi vysoké	Opatření: provést urychleně opravné hlášení [285] Odpovědnost: vedoucí směny na řízení letového provozu [285]
	Umístění letadla na nesprávnou dráhu	Pravděpodobnost: nízká Dopady: vysoké	Opatření: urychlené uvolnění dráhy a vyzvání pilota přistávajícího letadla k posečkání a opatrnosti [295] Odpovědnost: vedoucí směny na řízení letového provozu [295]
	Neschopnost pomoci letadlu v nouzové situaci	Pravděpodobnost: nízká Dopady: velmi vysoké	Opatření: okamžité odstartování nouzových opatření a činnosti nouzových služeb; později zajistit kvalitní výcvik řídících letového provozu [294] Odpovědnost: vedoucí směny na řízení letového provozu; později ředitel výcviku řízení letového provozu [294]
	Chaos na pracovišti v důsledku vnější pohromy, např. požár, špatná údržba letové dráhy	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 [294] Odpovědnost: vedoucí směny na řízení letového provozu [294]
Technická	Špatný stav letových drah na letišti	Pravděpodobnost: nízká Dopady: velmi vysoké	Opatření: okamžitě uzavřít poškozené dráhy [285] Odpovědnost: ředitel letiště [285]
	Špatné rozmístění techniky na letišti	Pravděpodobnost: nízká Dopady: střední až vysoké	Opatření: provést nápravná opatření a zajistit vydání výstražných zpráv NOTAM o stavu letiště [295] Odpovědnost: provozní ředitel letiště [295]
	Nefunkční varovný systém	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 [285] Odpovědnost: vedoucí směny na řízení letového provozu; později ředitel výcviku řízení letového provozu [285]
Vnější podmínky	Mlha	Pravděpodobnost: střední Dopady: vysoké	Opatření: uvést v činnost všechny pozemní radary a pomocná zařízení pro orientaci na letišti [296] Odpovědnost: technický ředitel letiště [296]
	Zaplavení / zasněžení plochy letiště	Pravděpodobnost: nízká Dopady: vysoké	Opatření: provést okamžité uzavření letiště, varovat letadla v přímém řízení a zahájit odklízecí práce [295] Odpovědnost: vedoucí směny na řízení letového provozu, za odklízení ředitel údržby letiště [295]
	Fyzický útok na letiště nebo dispečerské stanoviště	Pravděpodobnost: střední Dopady: vysoké	Opatření: nařídit okamžitý zásah bezpečnostních složek [285] Odpovědnost: vedoucí směny na řízení letového provozu [285]
Kybernetická	Ztráta spojení	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 [289, 293] Odpovědnost: vedoucí směny na řízení letového provozu; později ředitel výcviku řízení letového provozu [289,293]
	Hackerský útok na systém řízení letového provozu	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 [285] Odpovědnost: vedoucí směny na řízení letového provozu; později technický ředitel řízení letového provozu [285]

Pro případ velmi kritických situací je třeba mít připraveny specifické plány odezvy, zpracované ve smyslu krizových plánů. V pracích [279,280] byly speciálně sledovány dva případy, a to nouzové přistání na letišti a požár v objektu řízení letového provozu. Plány byly zpracovány ve formě karet [297].

Nouzové přistání na letišti

Popis situace: v čase T1 přijde žádost o povolení nouzového přistání civilního letadla plného cestujících z důvodu technické závady na letadle; v čase T1 + dT probíhá rozhodování na stanovišti řízení letového provozu; přistání je povoleno a jsou zahájeny přípravy na pomoc, kdyby došlo k nebezpečné situaci. Postup činností dle [298] je:

1. *Zahájení kontinuálního monitoringu na provozní ploše letiště* - provede vedoucí směny letištní řídící věže.
2. *Svolání krizového štábu letiště* - odpovídá ředitel letiště.

3. Velitelé nouzových složek zajistí, aby na místo nouzového přistání byly poslány základní jednotky, aby se zabránilo časovému zpoždění odezvy, bude-li třeba, protože včasným zásahem se sníží ztráty na lidských životech i ztráty ekonomické.
4. Při letecké nehodě při nouzovém přistání zajistí vedoucí řídící věže letiště *vyrozumění letištního personálu* telefonem nebo prostřednictvím pověřeného pracovníka, který bude zajišťovat nezbytné činnosti a provádět ochranná opatření; jde především o pracovníky na letištní ploše. Text: Vážení kolegové, na runway X5 přistává nouzově velké civilní letadlo, proveďte činnosti dle pokynu [298] a dbejte o své bezpečí.
5. Informace pro osoby přítomné na letišti. Text: vážení cestující na letišti, na runway X5 přistává nouzově velké civilní letadlo, dbejte o své bezpečí, uposlechněte pokyny bezpečnostních složek a personálu letiště.
6. Výpomoc letadlu v nouzi.
7. Obnova běžného provozu.

Požár v objektu řízení letového provozu

Popis situace: v čase T1 vypukne požár v provozním objektu řízení letového provozu. V čase T1 + dT rozhodování na stanovišti řízení letového provozu a jsou zahájeny přípravy na vyklizení oblohy a evakuaci objektu. Postup činností dle [298] je:

1. *Zahájení kontinuálního monitoringu situace* – provede vedoucí směny na sále letových provozních služeb.
2. *Svolání krizového štábu* - provede ředitel řízení letového provozu.
3. *Velitelé nouzových složek zajistí, aby do objektu ŘLP byly poslány základní jednotky*, aby se zabránilo časovému zpoždění odezvy, bude-li třeba, protože včasným zásahem se sníží ztráty na lidských životech i ztráty ekonomické.
4. *Vyrozumění osob v objektu ŘLP s výjimkou personálu na sále letových provozních služeb*. Text: Vážení kolegové, došlo k požáru, proveďte činnosti dle pokynu [298] a dbejte o své bezpečí.
5. *Varování řídících letového provozu a provozního personálu na sále letových provozních služeb provede vedoucí směny.* Text: „Vážení kolegové, v objektu je vyhlášena evakuace z důvodu požáru. Okamžitě zahajte postup pro nouzové vyklizení oblohy, aby mohla být zahájena evakuace stanoviště."

   Velmi důležité je zajištění vyklizení oblohy. Od doby rozhodnutí o nutné evakuaci stanoviště je nutno dokončit činnosti související s poskytováním letových provozních služeb co nejdříve, nejpozději však v takovou dobu, aby byli pracovníci schopni opustit objekt do 30 minut od doby vyhlášení evakuace nebo do jiného časového limitu, byl-li stanoven.
6. *Evakuace osob:*
   a) Osoby nacházející se mimo sál letových provozních služeb opustí objekt řízení letového provozu okamžitě po vyhlášení evakuace rozhlasem některou z nechráněných únikových cest a soustředí se na evakuační místo před objektem.
   b) Osoby nacházející se na sále letových provozních služeb, včetně těch, které nemají přímou účast na „vyklízení oblohy", vyčkají na pokyn vedoucího směny, aby zahájili evakuaci chráněnou únikovou cestou. Ta by měla poskytnout bezpečnou únikovou cestu z objektu po dobu několika desítek minut. V celém objektu jsou instalovány informační tabulky s vyznačením směru na místo evakuace osob. Postup evakuace osob je popsán v [298].
7. *Přechod na záložní pracoviště*. V případě, že výpadek pracoviště řízení letového provozu bude delší než 30 minut, tak službu převezme záložní pracoviště řízení letového provozu na letištní řídící věži nejbližšího mezinárodního letiště. Toto pracoviště shromažďuje dotazy a

předává ostatním služebnám známé informace do doby, než dojde k obnovení služeb z normálního pracoviště.

8. *Přechod ze záložního pracoviště do obnoveného normálního pracoviště*. Za urychlené odstranění škod v zájmu obnovení poskytování letových provozních služeb z běžného pracoviště odpovídá provozovatel objektu řízení letového provozu. Doba odstranění závisí na rozsahu poškození objektu. Návrat do objektu je z důvodu bezpečnosti poskytovaných služeb možný až po zkušebním provozu.
9. Obnova provozu ve vzdušném prostoru z normálního pracoviště. V rámci zkušebního provozu obnoveného objektu budou letové provozní služby poskytovány částečně ze záložního a částečně z běžného pracoviště. *Po přechodu na obnovené normální pracoviště zůstane záložní pracoviště v pohotovostním provozu po nezbytně nutnou dobu.*

Dopravní nehody malých letadel

Bezpečnost v letecké dopravě s letouny o maximální vzletové hmotnosti nad 2 250 kg, je značně odlišným systémem z pohledu bezpečnosti, než je tomu ve všeobecném letectví. V České republice je průměrně 300 případů leteckých nehod či incidentů ročně [275]. Zpravidla se jedná o chybnou činnost osob, či nesprávnou činnost leteckých a pozemních zařízení, jejíž důsledky však zpravidla nevyžadují předčasné ukončení letu [276].

V práci [299] je zpracována originální databáze nehod malých letadel v České republice v letech 2003-2014, která je součástí archivu [12]. Na základě těchto dat jsou získány dále uvedené výsledky. Tabulka 52 uvádí roční počty leteckých nehod.

Tabulka 52. Počty leteckých událostí v letech 2003-2014 [299].

Rok	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**
Počet hlášených událostí	540	557	639	683	623	763	686	764	685	640	689	645
Letecké nehody	92	105	81	105	106	106	68	90	79	72	82	58
Sportovní létání	354	301	384	391	517	429	257	672	383	319	503	319
Počet úmrtí	17	7	15	13	22	19	15	6	14	12	8	11

Z tabulky 52 vyplývá mírně vzrůstající trend v počtu leteckých incidentů oproti stabilním počtům leteckých nehod. Statistické vyhodnocení sestavené databáze [299] ukazuje současný trend vývoje bezpečnosti, tj. v hodnoceném období je počet leteckých nehod poměrně stabilní. Každým rokem je evidováno okolo 90 leteckých nehod, přičemž ročně si vyžádají v průměru 12 lidských životů. Stabilně je větší počet leteckých nehod v kategorii SLZ (sportovní létající zařízení), což je dáno především početností této skupiny oproti pilotům letounů. Výsledky popisující jednotlivé příčiny leteckých nehod jsou uvedeny v tabulce 53.

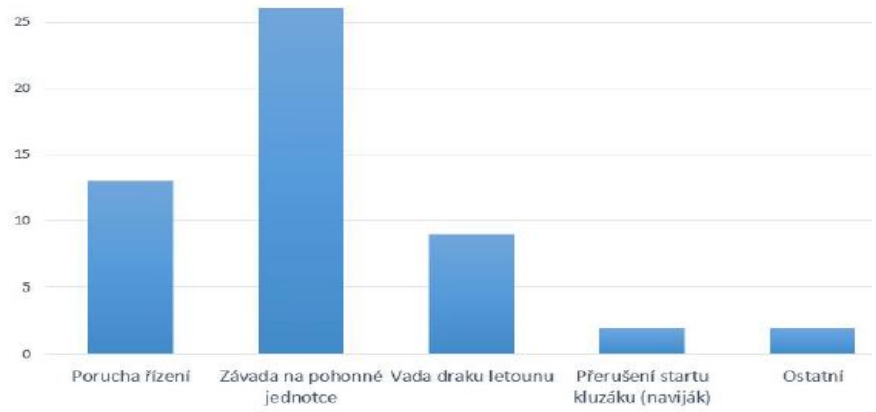
Tabulka 53. Procentuální rozdělení příčin leteckých nehod [299].

Příčina letecké nehody	**Počet**	**%**
Lidská chyba	151	61.38211
Meteorologické podmínky	15	6.097561
Technická	52	21.13821
Technická/Lidská chyba	11	4.471545
Meteorologické podmínky / Lidská chyba	8	3.252033

Ovlivnění okolím	1	0.406504
Ostatní	2	0.813008
Nelze určit	5	2.032520
Celkový počet sledovaných případů	246	100

Z tabulky 53 vyplývá, že lidská chyba, jako příčina vzniku letecké nehody, se vyskytuje ve více než 60 % případech. Zmíněné číslo však není absolutní. Je nutné si uvědomit, že databáze byla zpracována tak, aby ověřila především míru zavinění jednotlivých faktorů. Z uvedeného důvodu jsou zahrnuty kategorie „smíšené příčiny“, tedy kategorie technická / lidská chyba a meteo / lidská chyba, kde je podíl lidského konání značný, ale zpravidla mu předchází řetězec událostí, které pilot ovlivnit nemohl, a které vedly ke zvýšení zátěže pilota, čímž byl náchylnější k chybování. Pokud bychom započítali i zmíněné kategorie do společného součtu, vychází procentuální zastoupení lidského faktoru na 69.1%. Můžeme tedy tvrdit na základě dat, že udávaná hodnota procentuálního zastoupení 70-80% je v zásadě správná a Česká republika se svým rozložením příčin nijak nevymyká celosvětovému průměru, který je uveden v práci [297].

Druhé místo zaujímá technická chyba s 21% ze všech nehod obsažených v databázi. Na základě údajů z databáze je nejčastějším problematickým místem porucha pohonné jednotky letadla. Rozdělení typu letecké nehody s příčinou technické chyby je znázorněno na obrázku 63.



Obr. 63. Četnostní rozdělení událostí dle typu technických chyb [300].

Z obrázku 63 vyplývá, že nejčastější technickou chybou je závada na pohonné jednotce. Uvedená závada je současně nejčastější příčinou letecké nehody, ve které spolupůsobí chyba techniky s chybou pilota. Kvůli poruše motoru je provedeno chybně až 80% nouzových přistání, které mají za následek leteckou nehodu. Na základě údajů v databázi [299] byla též určena fáze letu, ve které nejčastěji dochází k letecké nehodě, tabulka 54, obrázek 64.

Tabulka 54. Fáze letu kdy k letecké nehodě došlo [299]

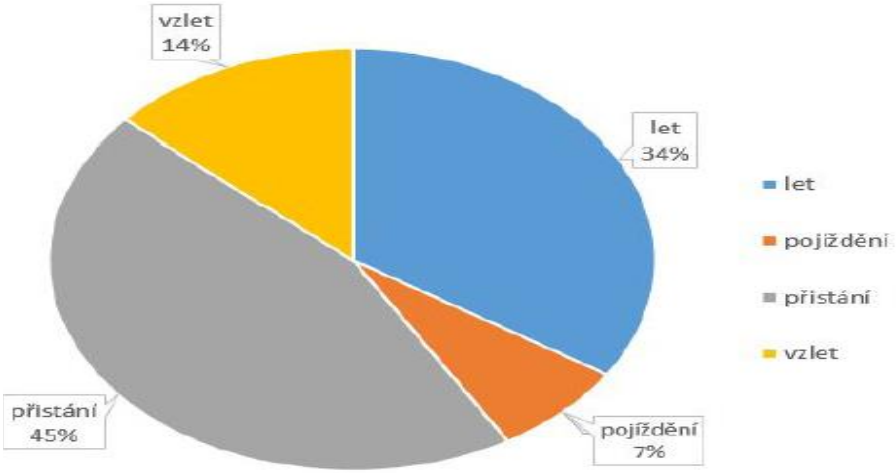
Fáze letu	**Počet výskytů**
Vzlet	33
Let	84
Přistání	111
Pojíždění	18

Z výsledků získaných v databázi vyplývá, že nejčastější fází letu se vznikem letecké nehody je přistání. Důvody jsou zřejmé z popisu fáze přistání a jednotlivé chyby, kterých se může pilot dopustit, jsou v práci [299].

Vzhledem k tomu, že ke vzniku letecké nehody dochází prakticky vždy, až po střetu se zemí, je nutno rozlišit v jaké fázi letu došlo ke vzniku podmínek, vedoucích k letecké nehodě. Proto jsou do zmíněné kategorie zahrnuty případy nezvládnutí nouzového přistání, které tvoří až 80% leteckých nehod ve fázi přistání.

Pro fázi vzletu je nejtypičtějším projevem porucha draku letounu, nestabilní chod či nízký tah motorové jednotky. Pro fázi letu je nejčastějším prvkem porušení předpisů v podobě nízké výšky letu, vlétnutí do podmínek, za kterých není pilot schopen pokračovat v letu či nezvládnutá pilotáž. Souhrnné výsledky nejčastějších projevů chyby pro jednotlivé fáze, získané na základě databáze [299] jsou uvedeny v tabulce 55.

.



Obr. 64. Četnostní rozložení fází letu, při kterých vznikla letecká nehoda [300].

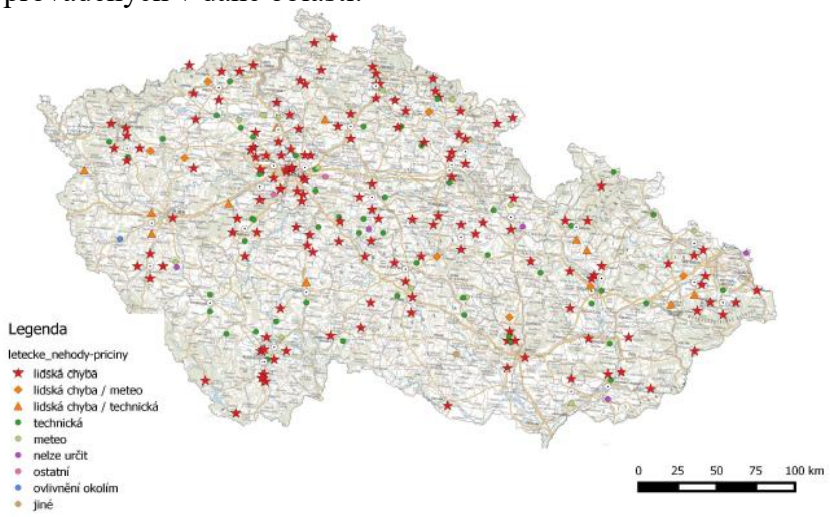
Tabulka 55. Typické chyby v průběhu letu [299].

Fáze letu	**Příčiny**	**Počet výskytů**
Vzlet	Nedodržení postupů	4
	Tah navijáku (kluzák)	3
	Tah motoru	2
	Destrukce konstrukce	2
	Porucha řiditelnosti	2
Let	Technika pilotáže	32
	Nedodržení postupů	16
	Nízká výška letu	9
	Srážka	6
	Porucha řiditelnosti	6
	Destrukce konstrukce	4
Přistání	Nedodržení postupů	25
	Chybný rozpočet	22
	Výpadek pohonné jednotky	21
	Chyba pilotáže	7
	Chybná interpretace pokynů	6
	Porucha řiditelnosti	3
	Nepozornost	3

	Destrukce konstrukce	1
Pojíždění	Nepozornost	7
	Nedodržení postupů	3
	Chybná interpretace pokynů	2
	Destrukce konstrukce	2

Meteorologické příčiny leteckých nehod zaujímají 6% případů. Drtivé většině případů, kdy svou roli při vzniku letecké nehody sehrálo aktuální počasí, lze předejít včasnou reakcí pilota na blížící se podmínky a těmto podmínkám se vyhnout, což mimo jiné uvádí letecké příručky [299]. Je jen málo situací, kdy se danému meteorologickému jevu vyhnout nelze, např. prudký střih větru při přistání, microburst, silný termický závan při přistání apod.; vlétnutí do oblačnosti je tedy zpravidla nutno klasifikovat jako závažné selhání lidského faktoru [299].

Z analýzy databáze sledovaného typu leteckých nehod je nejvíce kritickým místem oblast kolem letiště až do vzdálenosti do 2 km. Na obrázku 65 je možno vidět souhrn leteckých nehod v mapě, kdy až 70% nehod nastává ve zmíněné oblasti. To je způsobeno především markantním podílem počtu uskutečněných leteckých výkonů v okolí letiště a náročností operací prováděných v dané oblasti.



Obr. 65. Místa nehod malých letadel [299].

S geografickým rozborem leteckých nehod souvisí pojem okruh kolem letiště. Ten představuje předpisy stanovený letový manévr v bezprostřední blízkosti letiště určený pro přiblížení se na přistání všech letadel. Jeho tvar je pro motorová letadla přesně daný, pro kluzáky je rozměr manévru dán především výškou letadla v bodě vstupu do okruhu [301]. Předmětná oblast klade z bezpečnostního hlediska vysoké nároky ochranná opatření okolní zástavby kvůli vysoké koncentraci letadel a tím zvýšenému riziku nehody [299].

Dále ukážeme výsledky analýzy vybraných leteckých nehod s významným vlivem lidského činitele. Vybrané letecké nehody popisují častý výskyt určitého chování pilotů, které má zpravidla za následek leteckou nehodu. Identifikace dopadů jsou provedeny metodou What, If a hodnocení letecké nehody je provedeno na základě stupnice popsané v [299]:

1. Nehoda dne 14. 8. 2011u Bystřice. Typ letadla – kluzák; nikdo nebyl nezraněn, žádné úmrtí, místo nehody je vyznačeno červenou značkou na obrázku 66 vyneseném do mapového podkladu [302].

   Popis nehody: Dne 14. 8. 2011 obdržel ÚZPLN od RCC a PČR oznámení o letecké nehodě kluzáku v blízkosti obce Bystřice. V průběhu termického letu tohoto kluzáku došlo k jeho pádu ve výšce cca 600 m AGL. V průběhu pádu ve výšce cca 400 m AGL pilot odhodil

překryt kabiny a vyskočil z kluzáku. Kluzák dopadl na pole cca 250 m od zástavby rodinných domů. Nárazem do země byl poškozen. Pilot přistál na padáku bez zranění ve vzdálenosti cca 500 m od místa dopadu kluzáku. Dle [299] je pád z výšky na třetím místě důvodů letecké nehody kluzáků po nezdařeném nouzovém přistání a vzájemné srážce za letu. Dochází k němu zpravidla při kroužení, kdy se pilot soustředí především na proces kroužení [299].

Obr. 66. Místo letecké nehody u Bystřice.

Druhým aspektem je pád letounu v blízkosti zastavěné plochy. Z hlediska bezpečnostního inženýrství tak pilot představuje nebezpečí pro obydlenou oblast a je bezpodmínečně nutné důsledně dbát na dodržování minimálních výšek a vzdáleností vymezených v předpisech. Pomocí metody What, If je sestavena tabulka 56. která identifikuje dopady letecké nehody v daném území, které je zobrazeno na obrázku 66. Z tabulky 56 vyplývá, že nejzásadnější dopady dané letecké nehody jsou na místní obyvatele, kteří byli nehodou přímo zasaženi včetně možnosti vzniku požáru. Vyhodnocení letecké nehody dle stupnice hodnocení uvedené v [299] je: dopady - nízké; četnost výskytu nehody – méně častá; a celkové riziko – nízké.

Tabulka 56. What, If analýza letecké nehody v Bystřici, když dojde k pádu letadla do zastavěné oblasti [299].

Veřejná aktiva	**Možné dopady na veřejná aktiva**
Životy a zdraví lidí	Úmrtí posádky a cestujících v letadle
	Úmrtí či vážné následky obyvatel zasažených domů
	Úmrtí či vážné následky volně se pohybujících obyvatel v místě letecké nehody
Bezpečí lidí	Vznik paniky
Majetek	Škoda na havarovaném stroji
	Škoda na zástavbě v místě letecké nehody
	Poškození infrastruktury v místě LN
Veřejné blaho	Omezení dopravní obslužnosti díky poničené infrastruktuře
Životní prostředí	Zničení pozemků v místě nehody
	Poškození či úhyn fauny a flory v místě nehody díky úniku provozních kapalin

		Zamoření povrchových a podpovrchových vod ropnými látkami
		Vznik požáru a možnost dalšího šíření
Infrastruktury a technologie	Dodávky energií, tepla a plynu	Výpadek elektřiny způsobený přerušením elektrického vedení
		Přerušení dodávky plynu díky porušení plynovodu
	Dodávky vody	Přerušení dodávky vody při poruše vodovodu
		Kontaminace pitné vody provozními kapalinami letadla
	Kanalizace	Porušení kanalizačního potrubí
	Dopravní síť	Znehodnocení komunikace, porucha dopravní obslužnosti
	Bankovní sektor	Vysoké náklady na sanaci nehody
		Náklady na odškodnění účastníků LN
	Nouzové služby	Vytížení velkého počtu záchranných jednotek (hasiči, rychlá záchranná služba)
		Vysoké náklady na sanaci nehody
	Základní služby v území	Znehodnocení půdy pro zemědělství

2. Nehoda dne 3. 6. 2007 u Nové Vsi u Nepomuku. Typ letadla – SLZ ZENAIR 701, 2 úmrtí, 2 zranění, místo letecké nehody – obrázek 67, místo nehody je vyznačeno červenou značkou na obrázku 66 vyneseném do mapového podkladu [300].

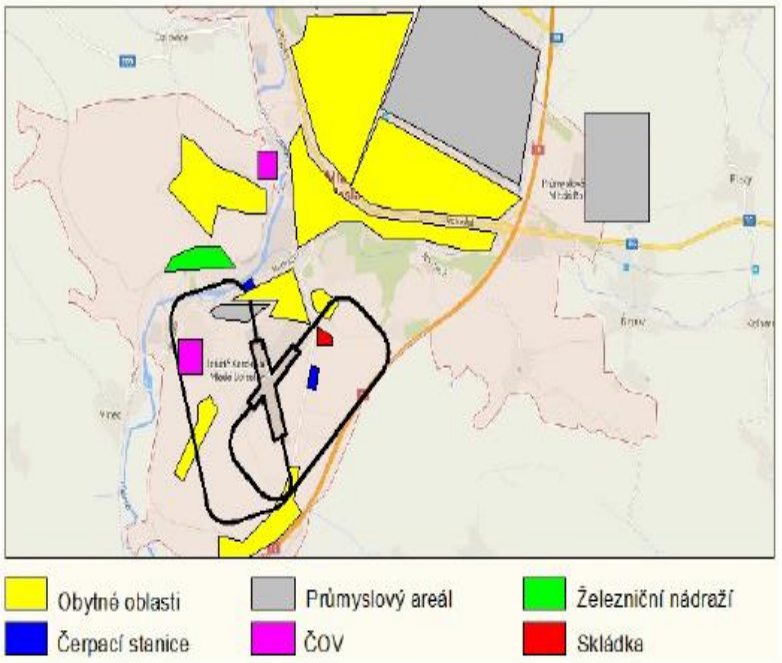
Obrázek 67. Místo letecké nehody u Nové vsi u Nepomuku.

Popis nehody: Pilot provedl vzlet z plochy SLZ Chotěšov s předpokládaným přistáním na letišti Strakonice. Uvedený let byl proveden pro vlastní potřebu bez letového plánu za VFR. V průběhu letu pilot pravděpodobně vlétl do prostoru s nízkou dohledností a nízkou spodní základnou oblačnosti. V tomto prostoru meteorologické podmínky neodpovídaly podmínkám pro let za VFR. Letoun narazil pod velkým úhlem do zvlněného, částečně zalesněného terénu. Pilot a cestující při nárazu zahynuli. Dle [299] je předmětná letecká nehoda jedním z mnoha zástupců stejné lidské chyby. Jde o vlétnutí do podmínek, za kterých není možné pokračovat v letu, je jednou z častých chyb zkušených pilotů. Drtivou většinu nízkých oblačností lze však obletět, nebo se vrátit, tak jak to nakazují letecké předpisy, a proto je tento případ typickým příkladem selhání lidského činitele. Stejně jako v předchozím případě je jediným možným prostředkem pro snížení počtu nehod tohoto typu zvýšení intenzity školení pilotů s důrazem na opakování zásadních předpisů [299].

Z hlediska hodnocení nehody metodou What, If je situace obdobná, jako v předchozím případě. Vyhodnocení rizika – vysoké, což vychází především z četnosti leteckých nehod

stejné příčiny identifikovaných v databázi leteckých nehod. Kvůli snížené až nulové viditelnosti, ve které se pilot pohybuje, dochází často k naprosté dezorientaci a srážce s povrchem ve vysoké rychlosti. Pravděpodobnost úmrtí pilota je v tomto případě značná [299].

3. Nehoda dne 16. 6. 2005 u letiště Mladá Boleslav. Typ letadla – letoun DS400/180 26 701, úmrtí žádné, jedno zranění, místo letecké nehody – obrázek 68, místo nehody je vyznačeno červenou značkou na obrázku 66 vyneseném do mapového podkladu [302].



Obr. 68. Schéma význačných bodů města Mladá Boleslav (převzato z [299]).

Popis nehody: Příčinou letecké nehody bylo pozdní rozhodnutí posádky letadla o provedení přistání a následné přistání v poslední třetině RWY 34. Toto rozhodnutí bylo zásadním způsobem ovlivněno poskytnutím rozporných informací potřebných pro bezpečné přistání dispečerem AFIS letiště Mladá Boleslav. Posádka letadla DR 400 prováděla přílet k letišti v pětičlenné skupině letadel. v pořadí na přistání jako první. Při vstupu do zóny letiště (ATZ) obdržely všechny posádky od dispečera AFIS vzhledem k momentálnímu směru větru informace o používání dráhy 34. Při přistávacím manévru uviděla posádka DR 400 na RWY 34 bílý kříž (zákaz přistání) a zároveň zjistila, že tráva je v prostoru místa dosednutí příliš vysoká. V okamžiku, kdy chtěla vznést dotaz na dispečera AFIS, zda přistává na správnou dráhu, uslyšela informaci druhé posádky v pořadí na přistání o úmyslu provést průlet bez přistání a následující reakci dispečera AFIS (letecké informační služby) předávajícího informace pro přistání na dráhu 24. Rozhodla se proto rovněž provést průlet. V tomto okamžiku ale zpozorovala, že se před ní nachází lesní porost a došla k závěru, že vzhledem k malé výšce letadla nad terénem v daném okamžiku nebude moci tento porost přeletět. Změnila proto své rozhodnutí a rozhodla se dokončit přistávací manévr. K dosednutí letadla došlo v poslední třetině RWY34. Přes usilovné brzdění se letadlo nepodařilo bezpečně zastavit a došlo k jeho nárazu do okraje místní komunikace.

Dle [299] na zmíněném příkladu je dobře identifikovatelný vliv letecké informační služby AFIS. Tato služba je zřizována na neřízených letištích a slouží pro informování leteckého provozu ohledně meteorologické situace, provozu a dalších zásadních informacích. Ačkoli služba nemá právo řídit letecký provoz, při intenzivním provozu není

možné ponechat provoz naprosto neřízen a pracovník AFIS často tak musí přejít k vydávání krátkých příkazů [299]. Pracovníci této služby však nejsou dostatečně technicky vybaveni, aby mohli provádět kvalifikované řízení. Jejich informace poskytované letadlům mohou však závažně ovlivnit bezpečnost celého provozu [300]. Je tedy nutné pracovníky této služby dostatečně vzdělávat, a pokud to je možné technicky vybavit tak, aby mohli svou práci vykonávat se vší zodpovědností. Jejich práce by měla být pravidelně kontrolována, aby se předešlo nehodám tohoto typu [299].

Letiště Mladá Boleslav je poměrně specifickým letištěm umístěným v těsné blízkosti města s velmi rušným provozem. Schématické zobrazení prvků letiště a okolí je zobrazeno na obrázku 68. Vliv leteckých nehod na bezpečnost oblasti je především spojen s existencí infrastruktury, která je potenciálním zdrojem domino efektu uvnitř tzv. okruhu kolem letiště popsaného na obrázku 68, ohraničeno černou čarou. Zde se odehrává naprostá většina pohybů letadel v malé výšce, a nebezpečí výskytu nehody je proto zvýšené. Ztráty, škody a újmy spojené s leteckou nehodou jsou v tabulce 57.

Tabulka 57. What, If analýza letecké nehody v Mladé Boleslavi, když dojde k pádu letadla do zastavěné oblasti [299].

Aktiva	**Specifikace aktiv**	**Možné dopady na aktiva**
Životy a zdraví lidí	Veřejná i soukromá	Úmrtí posádky a cestujících v letadle
		Úmrtí či vážné následky obyvatel zasažených domů
		Úmrtí či vážné následky volně se pohybujících obyvatel v místě letecké nehody
		Úmrtí pracovníků v průmyslovém areálu
Bezpečí lidí	Okolí nehody	Vznik paniky
		Vznik škodlivých exhalací při požáru
Majetek	Průmyslové areály	Škoda na havarovaném stroji
		Škoda na vybavení letiště
		Škoda na dalších letadlech umístěných na letišti
	Letecká technika	Škoda na zástavbě v místě letecké nehody
		Poškození veřejného prostranství města
		Poškození infrastruktury v místě LN
	Průmyslové areály	Škoda na výrobních prostředcích společností
		Poškození skladových zásob
Veřejné blaho		Omezení dopravní obslužnosti díky poničené infrastruktuře
		Zničení veřejných pozemků v místě nehody
Životní prostředí		Poškození či úhyn fauny a flory v místě nehody díky úniku provozních kapalin
		Exhalace z požáru na skládce
		Zamoření povrchových a podpovrchových vod ropnými látkami a provozními kapalinami letadla
		Únik nebezpečných látek z výrobního závodu a zamoření půdy

		Únik olejů a ropných látek do povrchové vody
		Vznik požáru a možnost dalšího šíření
Infrastruktury a technologie	Dodávky energií, tepla a plynu	Výpadek elektřiny obytných domů způsobený přerušením elektrického vedení
		Přerušení výroby závodů díky nedostatku elektrické energie
		Přerušení dodávky plynu díky přerušení plynovodu
	Dodávky vody	Přerušení dodávek pitné vody v postižené oblasti při poruše vodovodu
		Kontaminace pitné vody provozními kapalinami letadla
		Přerušení dodávky technologické vody do výrobního závodu
	Kanalizace	Porušení kanalizačního potrubí
	Dopravní síť	Znehodnocení komunikace, porucha dopravní obslužnosti
	Bankovní sektor	Vysoké náklady na sanaci nehody
		Náklady na odškodnění účastníků LN
		Vysoké částky pojistného při poškození technologií výrobního závodu
	Nouzové služby	Vytížení velkého počtu záchranných jednotek (hasiči, záchranná služba)
		Vysoké náklady na sanaci nehody
	Základní služby v území	Znehodnocení půdy pro zemědělství

Z tabulky 57 vyplývá, že nejvíce nebezpečné místo je čerpací stanice pohonných hmot v bezprostřední blízkosti letiště. Při pádu letadla na tento objekt je vysoké nebezpečí silného požáru včetně zahoření blízké zástavby. Další kritickou oblastí je skládka odpadu, na které se vyskytují i vyřazené pneumatiky, jejichž požár může svými exhalacemi značně ovlivnit široké okolí [299]. V širším okolí do pěti kilometrů je nejkritičtější oblastí pro vznik letecké nehody výrobní areál Škoda Auto, ve kterém je skladováno velké množství nebezpečných látek a hořlavin. Škody na majetku díky nákladnému vybavení mohou dosahovat vysokých hodnot. Přesto není nad areálem vyhlášen zakázaný letový prostor [299]. Proto také riziko vychází jako vysoké [299] – četnost nehod častá; dopady – vysoké. Nutno však podotknout, že nehodovost na tomto letišti je dlouhodobě minimální i přes značný provoz především o víkendových dnech. Největší koncentrace leteckých nehod je v době konání plachtařských závodů, kdy mnoho závodníků s kluzáky nedoletí na letiště a jsou nuceni nouzově přistávat v okolí [299].

Z hlediska bezpečnosti je přínosné minimálně v době konání závodů vyhlásit zakázaný prostor nad důležitými infrastrukturami, jako je areál Škoda Auto, skládka odpadů, železniční nádraží a dálnice [299]. Piloti by tak plánovali své přiblížení s ohledem na uvedené prostory a četnost nouzových přistání

Na základě identifikace dopadů leteckých nehod na veřejná chráněná aktiva byly navrženy postupy a opatření pro zvýšení bezpečnosti a ochrany zmíněných chráněných zájmů. Byl vymezen okruh kolem letiště s největším počtem leteckých nehod, předložen návrh na zřízení zakázaných letových prostor nad určitými objekty, které mohou být v případě letecké nehody zdrojem domino efektu a navržen způsob aktivace těchto prostorů.

Pro snížení nehodovosti z důsledku chyby v pilotáži je třeba především: zavedení pravidelných školení a rozborů leteckých nehod s důrazem na opatření prevence pravidelné přezkoušení pilotů z teoretických a praktických znalostí; průběh teoretického výcviku pro získání letového oprávnění doplnit o část věnovanou fyziologii a psychologii člověka včetně obtíží, které mohou u člověka během letu nastat; zavedení diferencovaného výcviku pro piloty různých věkových kategorií s důrazem na předání potřebných teoretických znalostí; zavedení minimální délky trvání praktické části výcviku, aby se pilot měl možnost seznámit s největší možnou variací meteorologických podmínek; zavedení letových úloh v rámci praktického výcviku na procvičení a zdokonalení procesu rozhodování a vyhodnocení nebezpečných situací; rozšíření letové úlohy „nácvik nouzového přistání“, především o simulaci výpadku pohonné jednotky [299].

5.9.5. Bezpečnost dopravní infrastruktury

Cílem řízení bezpečnosti dopravní infrastruktury ve veřejném zájmu v každém území je zajistit obslužnost území, tj. určitou kvalitu a hierarchii veřejných služeb. Obslužnost území je ovlivněna přímo i nepřímo různými skutečnostmi. Obecně jde o přírodní podmínky, pragmatický historický vývoj osídlení území i o nové aktivity politiky koheze EU. Zranitelnost infrastruktury je míra selhání infrastruktury (tj. infrastruktura přestane fungovat nebo bude fungovat nesprávně) v území a čase. Předmětnou míru lze měřit např. normovaným souhrnným (integrálním) rizikem od všech očekávaných pohrom v daném území nebo pravděpodobností výpadků infrastruktury, ke kterým dojde v důsledku očekávaných pohrom, do nichž se zahrnují i vnitřní problémy infrastruktury samotné.

5.9.5.1. Zásady pro řízení bezpečnosti

V uvedených souvislostech jsou významné dva faktory, a to důležitost a zranitelnost infrastruktury, z jejichž skórování zjistíme kritičnost infrastruktury [11] (pozn.: čím větší kritičnost infrastruktury, tím náročnější a sofistikovanější opatření a činnosti potřebujeme pro zajištění její bezpečnosti). Důležitost infrastruktury v území lze např. ocenit souhrnným oceněním dopadů selhání infrastruktury, tj. ztrát, škod a újmy na chráněných aktivech, a to veřejných, a v případě soukromých entit i privátních, při zohlednění doby trvání vzniklé nouzové situace, která zahrnuje jak dobu nutnou pro obnovu funkčnosti infrastruktury, kdy vznikají přímé škody i dobu, kdy se vyrovnávají nepřímé škody způsobené kauzálním řetězcem dopadů, vyvolaných selháním infrastruktury v území. Uvedené skutečnosti znamenají, že při všech akcích spojených s dopravní infrastrukturou, tj. i při obnově, musí být zvažována relevantní rizika a při jejich vypořádání veřejný zájem, kterým je bezpečí a rozvoj lidí v daném území. Z hlediska řízení dopravní infrastruktury je třeba u každého kritického prvku infrastruktury znát, zda může být jeho činnost přerušena nebo ne, a když ano, tak na jak dlouho – minuty, hodiny, dny atd. [1]. Řízení bezpečnosti dopravní infrastruktury 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 částí dopravních 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 částí dopravních 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 částí dopravních infrastruktur, které musí být součástí programu rozvoje území,
- respektovat právo občanů na spravedlivou pomoc (asistenční službu) při selhání životně důležitých částí dopravních 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 částí dopravních infrastruktur, a budou vědět, co obsahují, jaká je jejich role a odpovědnost, jak mohou napomoci v prevenci selhání životně důležitých částí dopravních infrastruktur, jak by měli reagovat, a proč, při vzniku selhání životně důležité infrastruktury apod.
- zajistit odezvu na selhání životně důležitých částí dopravních infrastruktur, která je transparentní i pro občany a je přizpůsobena místním podmínkám,
- zajistit legitimitu, udržitelnost, přijatelnost a systémovost odezvy.

Bezpečnost životně důležitých infrastruktur i kritické infrastruktury je věcí státního i privátního sektoru. Dokud se nepodaří najít účinné mechanismy řízení, je nutno používat nástroj spolupráce.

5.9.5.2. Rozdělení úkolů spojených s bezpečností dopravní infrastruktury zúčastněným

Zajištění bezpečnosti dopravní infrastruktury vyžaduje systematický přístup. Je nutné, aby iniciativy související s uvedeným problémem byly v souladu se začleněním ČR do mezinárodních společenství a aktivit. Proto je vhodné aplikovat následující model: stanovit co a proč je nutné chránit; stanovit minimální úroveň ochrany; posoudit současnou úroveň ochrany; v případě zjištění, že ochrana je nedostatečná navrhnout opatření; zajistit prostředky pro další ochranu a aplikovat opatření pro ochranu; periodicky kontrolovat stav; udržovat ochranu na odpovídající úrovni; a revidovat opatření v závislosti na vývoji. Protože rozdělení kompetencí a odpovědností je zásadní a důležité v každé složitější činnosti lidské společnosti, je si třeba uvědomit, že za dopravní infrastrukturu neodpovídají jen vlastníci a provozovatelé příslušné infrastruktury, ale i veřejná správa a občané.

Bezpečnost dopravní infrastruktury z hlediska provozovatele má tři cíle z hlediska veřejného zájmu. Prvním cílem je zajistit provozní spolehlivost (dependability), protože tím zabezpečuje služby dopravní infrastruktury. Druhým cílem je zajistit systémovou bezpečnost, tj. ochránit dopravní infrastrukturu před pohromami všeho druhu (vnitřními i vnějšími, a to včetně lidského faktoru). Třetím cílem je zajistit, aby dopravní infrastruktura neohrožovala okolí, tj. ostatní veřejné zájmy. Kvůli složitosti lidského systému i dnešní dopravní infrastruktury k zajištění zmíněných cílů potřebuje provozovatel náročné a sofistikované nástroje, Markovské řetězce, Petriho sítě, DSS pro zajištění stability složitých systémů apod. [1,5,10,15], kterými se provádí simulace chování infrastruktur. Uvedené nástroje vyžadují data i kvalifikované pracovníky, kteří umí kvalifikovaně pracovat s nástroji a daty. Proto z důvodu propojenosti veřejná správa musí pro provozovatele zajišťovat předmětnou vzdělanost, datové soubory o pohromách všeho druhu a výzkum. Kromě znalostní podpory, kterou by měli vlastníci infrastruktur dostávat od veřejné správy, je třeba, aby též přispívali k rozvoji znalostní základny, k tvorbě datových souborů a ke kvalitě výuky na vysokých školách a univerzitách (např. poskytovaly data, aby se studenti mohli naučit řešit praktické problémy). Na základě znalostí a zkušeností z praxe autorka vidí hlavní slabiny v: nedostatečné spolupráci mezi vlastníky dopravních infrastruktur;

mezi vlastníky dopravních infrastruktur a veřejnou správou; a v neexistenci koordinace činnosti dopravních infrastruktur náležících do kritické infrastruktury.

Každá položka infrastruktur i kritické infrastruktury se skládá z několika odlišných položek, které jsou podstatné pro její funkčnost. Jsou to: kritické liniové stavby, kritické objekty, kritické stroje a zařízení, kritické materiály a kritický personál. Z pohledu základních funkcí státu je třeba určit prvky a vazby, které jsou nutné pro zajištění přežití lidí. Zjištěné položky je pak nutno speciálně ochránit, což vyžaduje finance, materiální zdroje a vzdělaný personál. Protože zdroje jsou všude omezené, ochraňují se jen prioritní položky. Metody výběru priorit jsou obvykle velmi nákladné.

V praxi se osvědčila metoda multikriteriálního hodnocení [1,5,10,15] založená na posuzování zranitelnosti jednotlivých prvků systému. Při výběru optimální varianty se dává přednost variantám, které znamenají velkou zranitelnost u jednotlivců a malou zranitelnost u společnosti. Při hodnocení složitých systémů je třeba oklasifikovat poměrně složitý systém vazeb, ve kterém působení jednotlivých faktorů na výsledný efekt nelze kvantifikovat. Celkové hodnocení je proto relativní a může být ovlivněno subjektivním přístupem jednotlivých hodnotitelů. Je proto výhodné, jestliže hodnocení provede několik na sobě nezávislých expertů. Výsledky hodnocení platí pouze pro hodnocený systém a nelze porovnávat výsledky hodnocení různých systémů posuzovaných zvlášť [1,5,10,15]. Položky, které pro zajištění bezpečnosti příslušné dopravní infrastruktury musí zajistit vlastník či provozovatel infrastruktury dle zásad strategického řízení jsou uvedeny v práci [1,10].

Selhání životně důležitých infrastruktur naruší obslužnost území a tím i život obyvatel postiženého území, proto předmětné selhání není jen problémem provozovatele infrastruktury, ale i veřejné správy, která plní úkoly státu v oblasti ochrany životů a zdraví lidí. Kromě základní ochrany životů a zdraví lidí je zde skutečnost, že v dnešní společnosti, která je závislá na dobré funkci řady technologií a infrastruktur, je často při odezvě na nouzové situace většího rozsahu nutno provést nejprve činnosti podporující provoz infrastruktur a technologií (např. dodávka elektrického proudu, vody, zajištění dopravní dostupnosti, zvládnutí paniky a chaosu apod.) k zajištění zázemí pro provádění klasických záchranných a likvidačních prací v potřebném rozsahu. Proto veřejná správa musí dbát o kvalitní provoz životně důležitých infrastruktur.

Bezpečnost dopravní infrastruktury z hlediska veřejné správy má tři hlavní cíle z hlediska veřejného zájmu. Hlavní cíl je zaměřen na ochranu obyvatel v území, které spravuje, protože dlouhodobější nefunkčnost dopravní infrastruktury dopadá na každodenní život obyvatel, a proto infrastruktury i kritickou infrastrukturu posuzuje z hlediska obslužnosti (serviceability) při poskytování život podporujících služeb obyvatelstvu. Druhým cílem je donutit provozovatele dopravních infrastruktur k tomu, aby udělaly taková opatření a činnosti, které zajistí, že dopravní infrastruktury nebudou ohrožovat své okolí, tj. ostatní chráněné veřejné zájmy. Třetím cílem je zajistit kvalifikovaný výzkum možných pohrom s cílem zajistit takové řízení pohrom, které bude znalostně, organizačně, personálně, finančně i materiálně připravené na zvládnutí kritických až extrémních situací tak, aby potenciál přežití lidí, stabilizace situace i dalšího rozvoje byl vysoký. V uvedeném kontextu řízení integrální bezpečnosti, jehož částí je i zajištění bezpečnosti infrastruktur i kritické infrastruktury, znamená především budovat odolné území, vynucovat bezpečné a odolné dopravní infrastruktury, a vytvářet znalostní potenciál a materiálně technickou základnu pro zajištění schopnosti komunity přežít kritické situace.

K zajištění výše zmíněných cílů nepotřebuje veřejná správa tak sofistikované nástroje, jako musí používat provozovatel infrastruktur, stačí ji nástroje manažerské, kterými kontroluje a vynucuje: dodržení požadavků legislativy na umísťování, projektování, výstavbu a provozování infrastruktur; kvalitní propojení a vzájemnou spolupráci infrastruktur náležících do kritické infrastruktury za podmínek normálních, abnormálních a kritických; a úroveň organizačního, znalostního, materiálního, technického a finančního potenciálu potřebného pro zvyšování

odolnosti (resilience) infrastruktur a kritické infrastruktury a pro zvládnutí kritických situací, a to i těch málo očekávaných. Z pohledu nástrojů rizikového inženýrství ji stačí kontrolní seznamy, které jsou správně sestavené a používají hodnotovou stupnici zohledňující místní specifika [5,15]. Z pohledu přežití kritických situací je třeba, aby veřejná správa vytvářela mechanismy, podpořené legislativou, kterými se systematicky prověřuje schopnost vlastníků infrastruktur zvládnout kritické situace (dle české legislativy jde o krizovou připravenost). Na základě znalostí a zkušeností z praxe autorka vidí hlavní slabinu v neexistenci koordinace činnosti dopravních infrastruktur náležících do kritické infrastruktury z hlediska ochrany obyvatelstva. Předmětný úkol pochopitelně náleží veřejné správě, která si však v České republice problém a úkol nepřipouští, protože dosud není trestána za neplnění úkolů ve veřejném zájmu.

Jelikož veřejná správa nemá potenciál zvládnout nouzové a krizové situace vlastními silami, jsou legislativou zřízeny bezpečnostní složky. Jejich cílem je zabránit pohromám, kterým lze zabránit a zvládnout dopady pohrom, kterým zabránit nelze s dostupnými prostředky, zdroji a silami. Bezpečnostní složky jsou charakterizovány např. v práci [2], jejich činnosti jsou pak vymezeny příslušnými právními předpisy. Bezpečnostní složky České republiky jsou zřízení ústavním zákonem č. 110/1998 Sb., o bezpečnosti České republiky. Patří do nich ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby a státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby. Rozsah povinností a další podrobnosti stanovují zákony.

Chování lidí za nouzových situací je ovlivněno jejich vnímáním rizik, povahou rizika, způsobem komunikace o riziku v území a způsobem řízením rizika v daných konkrétních podmínkách. Vnímání rizika závisí na tom, jak člověk vyhodnotí ohrožení, kterému může být vystaven. Způsob vnímání rizika řídí rozhodování o přijatelnosti rizika a je zdrojem, který určuje chování člověka před, při a po pohromě. Posouzení rizika lidmi je výsledkem komplexního procesu zvážení jak rysů ohrožení, tak osobní filosofie. Postoj k riziku je dán tím, jak člověk vyhodnotí dopad rizika na život, tj. co považuje za příznivé a co za nepříznivé. Základními rysy postoje k riziku jsou náchylnost k riziku a averze k riziku, tj. opatrnost. Je skutečností, že vysoká náchylnost k riziku může indukovat ohrožení, na druhé straně však činnosti řízení rizik vyžadují určitou náchylnost k riziku, protože lidstvo nemá dostatek financí a dalších zdrojů na eliminaci všech rizik. Postoj k riziku není ani stabilní ani stejný s ohledem na všechny typy ohrožení; tj. některá ohrožení či pohromy jsou vnímány jako horší apod. Uvedená fakta je nutno zvažovat i v případě zajištění spolupráce občanů při velkém výpadku životně důležité infrastruktury.

Při přežití za extrémních situací má na jedné straně roli stát a na straně druhé i každý občan. Realizace opatření a činností spadajících do obou rolí musí být koordinované a provázané. Zajištění bezpečnosti dopravní infrastruktury ze strany občanů má z hlediska veřejného zájmu tři cíle. Prvním cílem je vlastní prací pomoci provozovatelům dopravních infrastruktur obnovit bezpečný provoz v nejkratší možné době. Druhým cílem je usměrněním vlastního chování pomoci veřejné správě zorganizovat přežití tíživé situace postižené komunity. Třetím cílem je vytvářet si vlastní schopnost, která umožní jemu i jeho blízkým a sousedům přežít tíživou situaci. V uvedeném kontextu řízení integrální bezpečnosti, jehož částí je i zajištění bezpečnosti dopravních infrastruktur i kritické infrastruktury, znamená především budovat u lidí sociální cítění, odpovědnost, vzájemnost a schopnost přežití. Předmětná fakta ukazují, že výchova lidí správným směrem je vysoce důležitá (je třeba poznamenat, že současné hodnoty lidské společnosti, které oceňují snadné získání peněz a bohatství bez ohledu na veřejný zájem, etiku a lidskou sounáležitost nejsou správným směrem).

Filozofie ochrany obyvatelstva proto musí mít požadavek, že každý občan má povinnost postarat se o sebe a svou rodinu, zabezpečit svůj majetek, mít k dispozici základní potraviny a vodu alespoň na 24 hodin. V případech výskytu extrémních pohrom je třeba, aby každý občan

v zájmu přežití připustil ztrátu pohodlí, omezení jídla a pití, psychickou a újmu. Zde již hovoříme o přežití. Občan musí být též připraven spolupracovat se záchranným systémem.

Na základě občanských opatření používaných v Japonsku, USA, UK, Rusku a Číně pro případ živelních pohrom [220] je metodou analogie sestaven soubor občanských opatření pro případ selhání infrastruktur:

- řídit se pokyny hasičů, policie a orgánů státní správy,
- věnovat pozornost přesným informacím (zapnout televizi, rádio),
- nepodléhat panice a uklidňovat spoluobčany,
- poskytnout pomoc zraněným a handicapovaným spoluobčanům,
- zkontrolovat stav objektu, rozvodů vody, elektřiny a plynu (při kontrole stavu rozvodu plynu nepoužívat otevřeného ohně – nebezpečí požáru). V případě nalezení poruchy uzavřít příslušný hlavní uzávěr, při poruše plynového potrubí otevřít okna, opustit objekt a nahlásit poruchu příslušnému orgánu státní správy, hasičů a do objektu se nevracet, dokud odpovědný orgán neoznačí objekt za bezpečný. V technologických objektech věnovat zvláštní péči místům, ve kterých hrozí nebezpečí výronu nebo vzniku nebezpečných škodlivin, toxických, biologických (bakteriologických), radioaktivních, výbušných a jiných látek ohrožujících životy lidí a životní prostředí,
- ponechat volné telefonní linky pro zajištění spojení zdravotníků, požárníků, záchranářů apod.,
- v případě nařízené evakuace či přemístění do jiného objektu vzít s sebou pitnou vodu, potraviny, léky, baterku, přenosný rozhlasový přijímač, důležité dokumenty a vhodný oděv,
- případná zranění pečlivě ošetřit a přitom dbát o zvýšenou hygienu,
- používat výhradně nezávadnou vodu a nezávadné jídlo.

5.10. Výsledky studia rizik výrobních systémů a návrh ochranných opatření

Výrobní sektor zahrnuje všechna odvětví lidské činnosti, která přeměňují suroviny na výrobky nebo zboží. Zajišťuje produkty pro přímou i nepřímou podporu životů lidí a jejich bezpečí. Je základem ekonomické prosperity státu i jeho obranyschopnosti, Proto je nutné soustředit se na rizika, která ho ohrožují a řídit je tak, aby výrobní sektor byl bezpečný. Jde o velmi širokou oblast, která se musí vypořádat jak s riziky od pohrom spadajících pod All-Hazard-Approach, tak s mnoha interdependences, které jsou příčinami selhání technologií, když se vyskytnou podmínky, pro které nebyly konstruovány. Navíc je nutné zvažovat proces stárnutí materiálů a jejich propojení i proces zastarávání technologií, jak je uvedeno výše.

Protože každé selhání či havárie v důležitém (kritickém) výrobním sektoru má dopady na veřejná aktiva a značně ovlivňuje konkurenceschopnost, soběstačnost a obranyschopnost státu, tak musí být jeho bezpečnosti věnována velká pozornost. V další části se zaměříme především na technologické objekty, které slouží průmyslové výrobě a k výrobě energií.

Řada států má své vlastní databáze údajů o haváriích (např. Nizozemí – databáze FACTS od TNO, Velká Británie – databáze MHIDAS od AEA Technology, aj.). V oblasti prevence závažných havárií směrnice Seveso č. 82/501/EHS v současném znění [303] obsahuje povinnost členských států nahlásit závažné havárie do registru nazvaného „Systém hlášení závažných havárií“ (Major Accident Reporting Systém – MARS). Tento registr provozuje Úřad pro ohrožení závažnými haváriemi (Major Accident Hazard Bureau – MAHB) ve Spojeném výzkumném středisku Evropské unie ve městě Ispra v Itálii [5]. Předmětný úřad provádí též analýzy havárií, získaných zkušeností a analýzy přijatých opatření s cílem využít získané informace pro účely prevence závažných havárií. Informace jsou uvedené v příslušné odborné

literatuře nebo na Internetu na adrese <http://mahbsrv.jrc.it>. Dalším zdrojem je publikace Loss Prevention Bulletin.

Směrnice Seveso II č. 96/82/ES popsaný vývoj podpořila zavedením kritérií pro povinné hlášení závažných havárií a formálními požadavky směrnice pro zajištění využívání získaných obecných ponaučení. Další vylepšení přinesla směrnice SEVESO III [303]. Nová forma směrnice byla přijata 4. 7. 2012, publikována 24. 7. 2012 a vstoupila v platnost 13. 8. 2012. Od 1. 6. 2015 platí ve všech státech EU. V novém znění se opět zvýšil důraz na práci s riziky, a to hlavně na analýzu a řízení, přičemž principy ALARP a ALARA zůstaly zachovány, tj. pro řízení a vypořádání rizik platí zásady CBA. Vyžaduje zvýšit pozornost zpracování scénářů havárií, což je v souladu s prosazovanými zásadami [1,5,8,9]; což znamená, že aplikace software používaných v ČR založených na jednoduchých fyzikálních modelech nevyhovuje a je třeba aplikovat postupy rizikového inženýrství pro systémy systémů.

Výsledky výzkumu dále uvedené vychází především ze studia havárií v průmyslu.

5.10.1. Havárie a jejich dopady

Jestliže zvážíme lidstvem nahromaděné zkušenosti, tak žádná technologie ani žádná látka nejsou absolutně bezpečné pro člověka, jejich nebezpečnost je určená množstvím a způsobem použití. Vyřazení každého technického díla z provozu ovlivňuje lidskou společnost; přínosem je např. odstranění zdroje hluku, exhalací apod., dopadem je ztráta příležitostí pro zaměstnání a s tím spojené sociální problémy, nedostatek výrobků, ztráta peněz pro státní správu apod. S ohledem na historické zkušenosti je však třeba specifickou pozornost věnovat průmyslu zpracovávajícímu nebezpečné látky a technologickým objektům vyrábějícím energii, a proto je jim věnována specifická pozornost.

Příčinou havárií je zpravidla kombinace technických a organizačních jevů. Podrobně jsou výsledky sledování technologických havárií v posledních 20 letech popsány v pracích [304-306]. Z předmětných prací vyplývá, že u většiny havárií ve výrobních podnicích došlo ke ztrátě soudržnosti zařízení. Podle [307] počet závažných technologických havárií roste v čase téměř exponenciálně a hlavní příčiny havárií v průmyslu jsou z:

- 54% technické příčiny - mechanické poruchy zařízení (např. koroze); nestandardní situace při výrobě (např. odstávky v provoze, znovu start výroby); nedostatečné materiální a technické vybavení; nesystémová inovace technologie nebo procesu; nekvalitní systém údržby a oprav zařízení; nepořádek; a chyby v automatice,
- 46% selhání lidského činitele – při návrhu zařízení a procesu; při konstrukci a instalaci zařízení a procesu; při provozu; při provádění údržby; a při řízení lidí a procesů,

což hrubě souhlasí s výsledky výzkumu [306].

Dle výsledků v práci [308] jsou nejčastější chyby, které vedly k technologickým haváriím: 35% chyby při údržbě zařízení; 17% chyby v projekci zařízení; 15% chyby v řízení výroby; 15% chyby pracovníků; 11% chyba při instalaci zařízení; a 7% chyby při zhotovení zařízení a jeho nastavení (software).

Podle [305,306,309] je podíl nejvýznamnějších kořenových příčin na vzniku havárií následující:

- 41% nedostatečné bezpečnostní zařízení a vybavení,
- 39% nevhodný zásah během pracovní operace,
- 31% problémy při společné práci,
- 27% nedostatečná analýza rizik, tj. nerozpoznaný zdroj havárie (nerozpoznaný škodlivý jev),
- 25% zapnutí / přepnutí zařízení,
- 25% automatické najetí stroje,
- 17% nedostatečný čas na interakci v pracovním systému,

- 15% nedostatečné nebo chybějící znalosti obsluhy,
- 14% výron energie,
- 14% provádění standardních operací,
- 11% nastavení stroje,
- 11% vypnuté bezpečnostní zařízení / bariéra,
- 9% vysmeknutí / sklouznutí,
- 9% stress,
- 8% nadměrné množství práce pro pracovníka,
- 5% přehlédnutí nebo podcenění rizika,
- 4% porucha bezpečnostního zařízení / bariéry,
- 4% nedostatečná kvalifikace pracovníka,
- 2% provedené změny bez informování pracovníků,
- 2% únava pracovníka.

Je si třeba uvědomit, že uvedené skutečnosti jsou velmi závažné, a to nejen z pohledu ochrany životů a zdraví lidí, ale i ochrany majetku a zisku vlastníka technického díla (veřejného nebo soukromého) a ochrany veřejného blaha, protože havárie a selhání technických děl mají kruté dopady ekonomické a sociální na komunitu, která je přímo nebo zprostředkovaně závislá na výrobcích a službách technického díla.

5.10.2. Havárie v průmyslu zpracovávajícím nebezpečné látky

Výrobky chemického, petrochemického a farmaceutického průmyslu a jiných příbuzných odvětví dnes doprovázejí člověka na každém kroku. Pomáhají mu při práci doma i v zaměstnání, přispívají k zabezpečení jeho výživy a všestranně usnadňují jeho život. Denně používáme výrobky z plastických hmot, k léčení nemocí se používají stále nové a nové léky, oblékáme se do různých oděvů zhotovených z umělých vláken apod. Život bez těchto produktů si člověk vůbec nedovede představit a používá je naprosto samozřejmě, aniž si uvědomuje celý proces, jak vznikaly.

Dále jsou uvedeny výsledky výzkumu, kterými jsou databáze technologických havárií s přítomností nebezpečných látek [12], vybrané příklady předmětných havárií a výsledky analýzy shromážděných údajů. V závěru pak navrhuje opatření pro snížení rizik, aby se zvýšila ochrana obyvatelstva, tj. jak zaměstnanců, tak občanů.

Technologická havárie s přítomností nebezpečných látek je havárie spojená s destrukcí nebo selháním průmyslového komplexu, při kterých dojde k uvolnění nebezpečných látek, požáru, vzniku tlakové vlny a rozletu úlomků. Potenciál působit škody je vlastní (vrozený) všem nebezpečným chemickým látkám, je projevem jejich konkrétních vlastností, jako jsou hořlavost, výbušnost (směsí jejich par s ovzduším nebo kyslíkem) a toxicita. Příčinou havárií je zpravidla kombinace technických a organizačních jevů. Článek shrnuje výsledky výzkumu zaměřeného na příčiny havárií a na analýzu kritických dopadů předmětných havárií ve světě i v ČR, a obsahuje návrhy opatření na zvýšení bezpečnosti technologických objektů, které zlepší ochranu lidí před nebezpečnými látkami.

Na základě vyhodnocení již publikovaných výsledků v odborné literatuře [1,27,29,304-329] platí:

1. Havárie, při kterých zdrojem nebezpečí jsou chemické látky, lze rozdělit na jevy, při kterých dojde k jejich úniku při jejich: výrobě v chemickém závodě; zpracování (v chemickém nebo jiném závodě); skladování; a transportu (po železnici, po silnici apod.). Únik toxických látek může být dvojího druhu - buď unikají látky spojené se zavedenou technologií (suroviny, meziprodukty, produkty), například po destrukci potrubí nebo zásobníku; nebo unikají látky vzniklé chemickou přeměnou látek vyskytujících se v technologickém

procesu, která pro něj nejsou charakteristické, např. při požáru zásob nebo výrobního zařízení nebo při nedodržení podmínek technologického procesu.

2. Příčiny havárií jsou různé, ale v podstatě je lze rozdělit na havárie úmyslné a neúmyslné. Úmyslné havárie jsou způsobeny lidmi. Jsou obvykle spojovány s klasickým válečným použitím, lokálním konfliktem, teroristickým útokem, atentátem nebo sabotáží. Neúmyslné havárie jsou sice většinou také ovlivněny lidským faktorem, ale není zde úmysl havárii způsobit. Jsou obvykle spojovány se živelnou pohromou, náhodnou shodou nepříznivých podmínek, technickou závadou nebo selháním lidského faktoru.
3. Po uvolnění chemické látky z aparátu mohou nastat tři základní nebezpečné situace: požár (např. požár kaluže, tryskový oheň, ohňová koule, bleskový oheň apod.); výbuch (ohraničeného mraku par, neohraničeného mraku par, kondenzované fáze, expandujících par vroucí kapaliny neboli BLEVE (boiling liquid expanding vapor explosion) apod.) a s ním spojený rozlet úlomků; a toxický rozptyl. Většinou platí údaje uvedené v tabulce 58.

Tabulka 58. Střední vlastnosti havárií.

Typ havárie	**Pravděpodobnost výskytu**	**Potenciál působit úraz**	**Potenciál působit ekonomické ztráty**
Požár	VYSOKÁ	NÍZKÁ	STŘEDNÍ
Exploze	STŘEDNÍ	STŘEDNÍ	VYSOKÁ
Toxický únik	NÍZKÁ	VYSOKÁ	NÍZKÁ

4. Mnohé nehody se vyskytují jako výsledek vzájemného působení mezi jednotlivými aktivními prvky technického díla – člověk, stroj, prostředí a IT, které vedou čas od času ke konfliktům.

Z hlediska ochrany lidí je třeba zmínit i úmyslné zneužití chemických látek, které lze shrnout následovně:

1. Za počátek éry chemických zbraní je všeobecně považován útok německých vojsk s použitím chlóru dne 22. 4. 1915 na 6-8 km úseku fronty u belgického města Ypres v západních Flandrech proti Francouzům. Bylo během 5 minut do vzduchu rozptýleno 180 tun chlóru. Bylo zasaženo 15 000 osob, z nichž do dvou dnů zemřela jedna třetina.
2. Koncem května 1915 provedli Němci u Bolimova další útok chlorem proti ruským vojskům na 12 km úseku. Bylo použito 264 tun chlóru, 9 000 osob bylo otráveno, 1 200 zemřelo.
3. V prosinci 1915 Němci poprvé použili toxičtější plyn – fosgen, který se stal nejpoužívanější otravnou látkou 1. světové války.
4. Dne 12. 7. 1917 – Němci použili yperit (β,β-dichlordiethylsulfid, hořčičný plyn).
5. V letech 1961-1971 tzv. neúmyslné použití jedovatých chemických látek USA ve Vietnamu (defolianty). Při použití těchto látek se ještě nic nevědělo o jedovatosti dioxinu, na jehož účinky se přišlo náhodně na farmě s kuřaty. V deseti tisících tun směsi herbicidů „Agent Orange“ bylo rozprášeno 110 kg dioxinu.
6. Při zkouškách leteckého postřiku v roce 1968 došlo k odvátí primárního oblaku látky VX v důsledku překročení výšky pro vypouštění do blízkého Skull Valley a Rush Valley, kde bylo zasaženo přes 6000 ovcí. Vyšetřování prováděly orgány civilní zdravotnické služby a tím se částečně prozradilo složení látky i její struktura. Proto byla látka odtajněna a publikována i její syntéza v roce 1974.
7. V březnu 1988 byl proti Kurdům použit Saddámem Husajnem yperit s následkem 5000 mrtvých, 16 000 lidí s dlouhodobým poškozením plic, očí a kůže.

8. Atentát v r. 1978, kdy byl v Londýně bulharskou tajnou službou zavražděn injekcí ricinu bulharský disident G. Markov.
9. Vražda látkou VX v Osace v prosinci 1994. Muži byla vstříknuta VX látka na zadní část krku. Perkutánní intoxikace skončila po 2 týdnech smrtí.
10. Dne 27. června 2004 byl v Matsumoto použit sarin. Měl být použit v budově soudu, ale dodávka s teroristy, která vezla před deseti dny vyrobený sarin, přijela k budově soudu pozdě. Protože však teroristé věděli, kde soudci bydlí, odjeli tam a začali vypouštět sarin. Protože se však vítr obrátil, zasáhly páry sarinu i jiné obytné domy. Sedm lidí zemřelo, stovky byly zasaženy.
11. Dne 20. března 1995 byl v Tokiu na několika místech v metru teroristy použit sarin. Bylo zasaženo kolem 10 000 osob, 12 zemřelo, 5000 bylo vážně intoxikováno
12. V roce 2004 ukrajinský prezident (ještě jako kandidát na prezidenta) Viktor Juščenko byl

Databáze havárií v [12] obsahuje údaje z 248 dostupných světových zdrojů o sledovaném typu havárií v průmyslových objektech, k místním zdrojům jsme se nedostali. Z nich byly získány údaje pro 222 velkých technologických havárií s přítomností nebezpečných látek. Na jejich základě jsme sestavili chronologicky uspořádanou databázi, která obsahuje technologické havárií s přítomností nebezpečných látek od roku 1916.

Dále uvedeme pět příkladů velkých havárií, o kterých se mnoho nemluví, ale obsahují jistá poučení, která platí dodnes.

Oppau (fa BASF, Německo, 21. 9. 1921)

V Oppau, nedaleko Mannheimu, byla v roce 1911 na 8 ha postavena továrna na výrobu dusíkatých hnojiv. To zahrnovalo především směs chloridu draselného a dusičnanu amonného ve stejném poměru. Amoniak pro výrobu dusičnanu amonného byl vyráběn pomocí nového Haber-Bosch postupu, při kterém byl používán atmosférický dusík. V továrně bylo zaměstnáno 8 000 místních lidí. Během války byly amonné soli vyráběny pro vojenské použití, jako složky pro výbušniny, ale po roce 1918 se amonné soli vyráběly pro civilní účely. Od roku 1919 se směs chlorid draselný / dusičnan amonný postupně nahrazovala směsi síranu amonného a dusičnanu amonného v poměru 50/50. Ale tato směs byla silně hygroskopická a měla tu nevýhodu, že se tlakem své vlastní hmotnosti při skladování změnila ve ztvrdlou hmotu. Běžnou praxí bylo, že k uvolnění této hmoty se do ní navrtaly otvory a použilo se výbušniny. Objekt, kde se tento proces prováděl, se nazýval "silo" a byla to 60m x 30m x 20m polozasypaná budova, která byla 4 metry pod zemí. V továrně na umělá hnojiva byl používán střelný prach k rozdrobení ztvrdlé směsi síranu amonného a dusičnanu amonného (50:50). Tento způsob byl do té doby proveden 20 000krát bez nehody [330,331].

Dne 21 září 1921 ráno bylo tady uloženo 4500 tun síranu amonného. Poté co technik v 07:00 připravil otvory pro odpálení náloží v silu, došlo v 07:32 v silu k velmi silné explozi, která vytvořila kráter 90 m x 125 m o hloubce 20 m! Podle svědků to byly dvě po sobě jdoucí exploze, první z nich byla slabá a druhá devastující. Seismografický záznam ze Stuttgartu, 150 km od Oppau také ukázal dvě výrazné exploze, k nimž došlo v intervalu půl sekundy. Exploze byla slyšet v Mnichově, 275 km od továrny a způsobila paniku mezi lidmi. Hmotné škody byly hlášeny několik desítek kilometrů od místa nehody. Tmavě zelený mrak zakryl oblohu v Ludwigshafenu a Mannheimu. Celá oblast pak byla pokryta hustým kouřem, který spolu s přerušením telegrafní a telekomunikační služby ještě ztížily záchranné práce.

Brzy po výbuchu, došlo k řadě požárů různých zařízení a k řadě dalších méně intenzivních výbuchů a vzduch byl plný par amoniaku. Oficiálně bylo uvedeno 561 mrtvých, 1952 zraněných a 7500 lidí zůstalo bez přístřeší. Mezi oběťmi jsou též cestující ze tří vlaků vezoucích na místo obměnu směny. Několik dětí bylo zraněno na cestě do školy, byly poškozeny lodě na řece Rýn a zraněni jejich námořníci. Přibližně 80% budov v Oppau bylo zničeno. Značné škody byly hlášeny také v Ludwigshafenu a Mannheimu. V Heidelbergu (30 km od Oppau), přerušily

masivní skleněné nečistoty na silnicích dopravu ve městě. Podle článku v New York Times z 29. ledna 1922, byla hmotná škoda stanovena na 321 milionů marek, tj. 1.700.000 $.

Vyšetřování nehody, které vedla odborná porota v čele parlamentní komise, bylo obtížné vzhledem k rozsahu poškození a absenci přímých svědků, kteří byli oběťmi pohromy. Vyšetřování trvalo 2 roky a zpráva byla publikována v roce 1925. Bylo zjištěno, že jeden ze zážehů provedených v silu, aby se uvolnila masa hnojiva, byl příčinou nehody - některé otvory byly totiž vyvrtány v oblasti změklé směsi již předchozího dne. Studium výbušných vlastností směsi 50-50 síranu a dusičnanu amonného a směsi podobného složení ukázalo: výbušnost směsi 50-50 při velmi omezených podmínkách a relativně nízké hustotě, je exploze omezena na oblast v okolí, kde jsou umístěny výbušniny; významný vliv některých fyzikálních vlastností hnojiva (hustota, vlhkost, atd.), na jeho schopnosti explodovat; a zvýšení koncentrace dusičnanu amonného ve směsi na 50 až 55% a dokonce na 55-60%, přispívá k významnému zvýšení výbušnosti a výbušné síly směsi.

Ukázalo se, že několik měsíců před nehodou, byl modifikován výrobní proces: úroveň vlhkosti (2% místo 3 až 4%), a tedy i zdánlivá hustota vyrobené směsi byla nižší než dříve. Odborníci dospěli k závěru, že tyto změny způsobily, že směs snadněji explodovala. Kromě toho několik shodujících se svědectví vedlo k domněnce, že složení hromady 4500 tun směsi v zásobníku, který byl postaven až v měsíci před výbuchem, nebylo jednotné. Tam mohlo být několik desítek tun zón s bohatším obsahem dusičnanu amonného. Tudíž scénář vysvětlující nehodu může být následující: otvory byly vyvrtány v oblasti obsahující 55 až 60% směsi dusičnanu amonného; při spalování, tato směs obohacená dusičnanem amonným mohla explodovat a přivést sousední směs 50/50 k detonaci; a pouze 10% zásoby bylo zapojeno do výbuchu, celý obsah sila nevybuchl, a to zejména v zónách složení 50/50, kde hustota produktu byla relativně vysoká.

Rozsah věcné škody a ztrát na životech udělaly záchranné operace obzvláště obtížnými. Záchranné služby, které byly rychle upozorněny, nemohly dorazit na místo před 9:00 z obav z nových výbuchů. Francouzská armáda se sídlem v Ludwigshafenu a Mannheimu vytvořila bezpečnostní linii kolem místa. Nouzové služby (lékaři, hasiči, sanitky, francouzští a němečtí dobrovolníci Červeného kříže, armáda, atd.), přijeli ze sousedních měst. Soukromá a veřejná vozidla byla zabavena. Nouzová nemocnice se sídlem v Ludwigshafenu byla velmi brzo plná a zranění museli být převezeni do Mannheimu, Heidelbergu, Frankenthalu a Wormsu. Bezdomovci byli ubytováni ve školách, sanatoriích nebo v rodinách v okolních městech. Mnozí však odmítli opustit své zničené domovy.

Minamata (Japonsko, 1953)

V 50. a 60. letech došlo v Japonsku poprvé k hromadným otravám, které měla na svědomí rtuť a její sloučeniny. První hromadná otrava byla zaznamenána v okolí zálivu Minamata v roce 1953. Postiženi byli většinou rybáři a členové jejich rodin, kteří byli velkými konzumenty rybího masa. Bylo zaznamenáno 116 případů, z nich 43 bylo smrtelných. Ti, co nezemřeli, byli trvale postiženi. Teprve během tří let bylo zjištěno, že primárním znečištěním jsou odpadní vody z chemického závodu obsahující sloučeniny rtuti, které se používaly při syntéze acetaldehydu a výrobě vinylchloridu. Chemickou a biochemickou transformací vznikaly methylmerkuri-sloučeniny s vysokým akumulačním potenciálem, které kontaminovaly ryby a byly pak příčinou vlastního onemocnění. Od této události se hovoří o tzv. minamatské nemoci [332,333].

Chronologicky jde asi o nejstarší a nejpoučnější katastrofu otravy rtutí v zálivu Minamato v Japonsku. Dle tehdejšího přesvědčení se těžké kovy nemohly zapojovat do biochemických cyklů živých organismů, a proto bylo považováno za bezpečné odpadní sloučeniny rtuti skladovat na mořském dně. Bohužel se nevědělo o existenci bakterií, které umí rtuť do svých metabolických cyklů zapojit a tak jí zapojit následně do potravních řetězců, na jejichž vrcholu

stojí člověk.

Severní moře (fa Occidental Petroleum, 6. 7. 1988)

Na ropné plošině Piper Alpha v Severním moři, která patřila společnosti Occidental Petroleum, došlo k explozi a ropy a zemního plynu, obrázek 69. Bylo zabito 167 mužů, přežilo pouze 61 [334]. Předmětná havárie je podobně jako potopení Titaniku považována za atypickou havárii, která vznikla neobvyklou kombinací mnoha jevů a lidské chyby [10]. Předmětná havárie je modelem havárie, na kterou mnoho projektů EU reaguje tím, že hledá příčiny a postupy optimální odezvy; např. projekt EDEN [335].

Obr. 69. Požár na plošině Piper Alpha [334].

Pasadena (fa PHILLIPS HOUSTON, Texas, USA, 23. 10. 1989)

V závodě Phillips v blízkosti Houstonského lodního kanálu v rafinérii ropy došlo k požáru a výbuchu. Výbuch zničil závod na výrobu polyetylenu, mohutná exploze zabila 23 lidí a dalších 314 jich zranila. Zdroj výbuchu – isobutan. Trosky z výbuchu byly nalezeny až 9.7 km od místa exploze [336]. Ekonomická ztráta činila celkem 1.4 mld. USD. Primární příčinou exploze a požáru byl únik hořlavých plynů. Oficiální šetření nehody zjistilo, že firemní bezpečnostní postupy společnosti Phillips a odvětvová standardní praxe vyžadovaly během údržbářských prací na potrubí záložní ochranu ve formě dvojitého ventilu nebo zaslepovací příruby. Avšak na místní úrovni měla společnost zvláštní postup, jehož součástí nebyla vyžadovaná záloha. Společnost Phillips byla organizací OSHA obviněna z toho, že zaměstnance údržby neinformovala a nevyškolila v tom, jak pracovat bezpečně s nebezpečnými chemickými látkami. Společnost souhlasila se zaplacením pokuty ve výši 4 mil. USD [336].

Z havárie plyne ponaučení, že pro operaci v rámci údržby musí být stanoveny bezpečné pracovní systémy, které musí být dodržovány. Zaměstnavatelé musí zajistit, aby pracovníci údržby byli informováni o rizicích a aby byli vyškoleni o tom, jak pracovat bezpečně s nebezpečnými chemickými látkami.

Illiopolis (fa Formosa Plastics, Illinois, USA, 23. 4. 2004)

V závodě Formosa Plastics Corporation tajwanské společnosti na výrobu polyvinylchloridu došlo po úniku vysoce hořlavého vinylchloridu k požáru a výbuchu, obrázek 4. Při havárii zahynulo 5 osob, 2 osoby byly zraněny a část města byla evakuována. Oheň hořel několik dní.

V roce 2007 byl závod znovu otevřen [337-339].

Výsledky analýzy databáze světových havárií

Více než pětina všech havárií s přítomností nebezpečných látek v databázi [12] má spojitost s ropou nebo zemním plynem nebo přesněji řečeno s produkty z nich připravených, ať už se jedná o směsi jako je nafta, oleje, benzíny a propan butan, které jsou používány jako palivo nebo čisté látky používané pro další výrobu v organické chemii (methan, ethan, ethen, propan, propen, butan, isobutan, butadien, hexan, cyklohexan, styren). Přehled nejznámějších je následující:

- ropa: Mexico City (1961), Czechowice (1971), Thessaloniki (1986), Remeios (1993), Buncefield + nafta a benzin (2005)
- zemní plyn: Agha Jari (1970), Staten Island (1973), Severní moře (1988), Baohe (1993), Shenzhen (1993), Geleen (2003),
- nafta: Chihuahua (1988), Bombay (1988),
- topný olej: Tacoa (1982),
- olej: Jaipur (2009),
- benzín: Dhulwari (1983), Monterrey (1988), Guadalajara (1992), Nam Khe(1993), Texas City (2005), San Juan (2009),
- uhlovodíky: Pembroke (1994), Vishakhapatnam (1997),
- methan: Santacruz (1978), Corlu (1992),
- ethan: Nagothane (1990)
- ethen (ethylen): Antwerpy (1975), Beek (1975), Geismar (2013),
- propan: Port Newark (1951), Feyzin (1966), Duque de Caxias (1972), Umm Said (1977), Ortuella (1980), Nagothane (1990), Chateauneuf-les-Martigues (1992), Toronto (2008),
- propen (propylen): Geismar (2013),
- propan-butan: Mexico City (1984), Romeoville (1984),
- butadien: Ludwigshafen (1943), Amsterdam (1971),
- isobutan: Pasadena (1989),
- hexan: Louisville (1981),
- cyklohexan: Flixborough (1974), Belpre (1994),
- styren: Belpre (1994)

Skoro v jedné šestině havárií se vyskytuje amoniak, z něho vyráběná kyselina dusičná a dusičnan amonný. Havárie spojené s amoniakem mohou být co do rozsahu od drobných úniků z chladících zařízení až po havárie spojené s evakuacemi desítek tisíc obyvatel. Obzvláště havárie spojené s dusičnanem amonným patří co do rozsahu ničivých škod mezi nejdestruktivnější.

Roztřídění havárií s přítomností zmíněných nebezpečných látek v databázi [12] je následující:

- amoniak: Blair (1970), Potchefstroom (1973), Pasacaballos (1977), Manfredonia (1978), Bhópál (1987), Bhatinda (1989), Ionava (1989), Lusknow (1990), Dhaka (1991), Dakar (1992), Westalake (1992), Bratislava (2000), Nanchital (2005), Šanghaj (2013),
- kyselina dusičná: Omaha (1984), West Bromwich (1988), Richmond (1992), Shenzhen (1993)
- dusičnan amonný: Faversham (1916), Morgan (1918), Kriewald (1921), Oppau (1921), Nixon (1924), Tessenderlo (1942), Texas City (1947), Manouba (1978), Porgera (1994), Port Neal (1994), Xingping Shaanxi (1998), Toulouse (2001), Saint-Romain-en-Jarez (2003), Bryan (2009), West (2013).

Téměř jednu osminu tvoří havárie s chlórem. Opět se podobně jako u amoniaku jedná o rozsah od drobných úniků ze zařízení upravujících vodu až po havárie spojené s evakuací desítek tisíc obyvatel. Nejznámější jsou: St.Auban (1926), Zarnesti (1939), Rauma (1947),

Walsum (1952), Nitro (1957), Malaga (1974), Baton Rouge (1976), Massachusets (1980), San Juan (1981), Geismar (1981), Massachusets (1981), West Virginia (1982), Woodfibre (1983), Bombay (1985), Simi Valley (1989), Brittania Chowk (1989), Calcutta (1990), Coatzahoulcos (1991), Coatzacoalcos (1991), Henderson (1991), Calcutta (1991), Schkopau (1992), Chabarovsk (1997), Nanchang (2004).

Téměř jednu desetinu tvoří havárie spojené s výbušninami. Zde nehrají prim výbušniny v pravém slova smyslu (dynamit, střelný prach, trinitrotoluen, munice), ale hlavně tak zvaná zábavná pyrotechnika obzvláště v zemích, kde si potrpí na oslavy spojené s příchodem Nového roku (např. Mexiko, jihoamerické státy, Čína a jihovýchodní Asie). V Evropě je známa havárie továrny vyrábějící zábavnou pyrotechniku v Enschede. Nejznámější jsou:

- munice: Alexandria (1987), Islamabad (1988),
- pyrotechnika: Rawalpindi (1979), Mexico City (1988), Kuala Lumpur (1991), Al-Sanouani (1992), Piya (1996), Tultepec (1998), Celaya (1999), Enschede (2000), Ciudad de Vera Cruz (2003), Kolding (2004), Linzhou (2006), Sanmenxia (2013),
- střelný prach: Mexico City (1957),
- TNT: Faversham (1916), Dottikon (1969),
- výbušniny: Mandir Asad (1980), Pyongyan (1991).

Zbytek, téměř 40%, tvoří havárie s nejrozmanitějšími dalšími chemickými látkami, mezi kterými se vyskytují jak jedovaté látky, tak hořlaviny nebo výbušniny. Poměrně početně jsou zastoupeny havárie s deriváty síry (sulfan – sirovodík, oxid siřičitý a sírový) a s dioxiny. Své zastoupení zde mají jedovaté prvky jako arsen a rtuť, kyanidy, fosgen, methylisokyanát, organofosfáty, pesticidy atd. Příklady havárií jsou:

- sulfan (sirovodík): Poza Rica (1950), Berwick (1971), Chicago (1978), Daesan (1990), Chhota (1993), Savannah (1995), Whittehall (1999), Pennington (2002), Chuandongbei (2003),
- oxid siřičitý: Meuse Valley (1930), Donora + fluor (1948), Cincinnati (1968), Jhurkully (1988), Kaohsiung (1991)
- oxid sírový: New Delhi (1985),
- dioxiny: Nitro (1949), Ludwigshafen (1953), Hamburg (1954), Midland (1960), Amsterdam (1963), Butermilk Lane (1968), Times Beach (1972-6), Seveso (1976), Niagara Falls (1978),
- akrolein: Taft (1982),
- arsen: Manfredonia (1976), Ajka (2010),
- benzoylperoxid: Xuchang (1991), Zhengzhou (1993),
- dimethylether: Ludwigshafen (1948),
- ethylacetát: Des Moines (2007),
- ethylenoxid: Port Lavaca (1991), Seadrift (1991), Kaohsiung (1994),
- fluorovodík: Texas City (1987),
- fosforoxychlorid: Sauget (1984),
- fosgen: Hamburg (1928), Map Tha Phut (2000),
- hexachlorocyklopentadien: Cochin (1985),
- hořčík: Woodbine (1971),
- chemické látky: Basel (1986), Springfield (1988), New Delhi (1992),
- chlorbutadien: Reserve (1983),
- chlorid křemičitý: Chicago (1974), San Francisco (1981),
- chlorid sirnatý: Catenoy (2006),
- chloristan amonný: Henderson (1988), Sriharikota (2004),
- chrom: Ajka (2010)
- kyanidy: Baia Mare (2000), Bonanza (2003),
- kyanovodík: Huairou (2004),

- kyselina chlorovodíková: South Charleston (1985),
- merkaptan: Mexico City (1996),
- methanol: Guangxi (1987),
- methylbromid: Houston (1983)
- methylethylketon peroxid: Faridabad (1997),
- methylisokyanát: Bhopal (1984),
- nitromethan: Sterlington (1991),
- obilný prach: Houston (1976), Westwego (1977),
- organofosfáty: Memphis (1979), Linden (1984), Cordoba (1991),
- oxid dusnatý: Miamisburg (2003),
- oxid uhličitý kapalný: Repcelak (1969),
- pesticidy: Coachella (1985), Charleston (1985), Institute (2008),
- plasty: Bangkok (1993),
- rtuť: Minamata (1953), Ajka (2010)
- uhelný plyn: Liu Pan Shui (1988), Košice (1995),
- vinylchlorid: Illiopolis (2004),
- vodík: Sodegaura (1992),
- zinek: Noyelles-Godault (1994).

Na základě analýzy databáze [12] byly určeny bezprostřední a zásadní příčiny havárií v chemickém průmyslu. Bezprostřední příčiny havárie určitého zařízení jsou spojeny se: zařízením, které selhalo; havárií jiných zařízení nacházejících se v podniku; výskytem externí jevy v okolí podniku; a přírodní pohromy. Zásadní příčiny havárií, které nazýváme organizační havárie, jsou: chyby v řízení a organizaci podniku; chyby v řízení provozu zařízení; a nedodržování předpisů.

Příčiny havárie určitého zařízení spojené s určitým zařízením (tzv. vnitřní) lze rozdělit do pěti dále uvedených okruhů:

1. Chyby provozovatele zařízení při:
   - provozu
   - údržbě,
   - inspekci, testování či kalibraci,
   - při návrhu konstrukčního řešení.
2. Poruchy komponent zařízení:
   - způsobené poškozením potrubí nebo potrubních prvků,
   - způsobené chybnými svary,
   - způsobené poškozením ventilů,
   - způsobené poškozením hlavních zařízení jako jsou: nádoby / kolony; zásobníky; reaktory; výměníky tepla; pece; vařáky,
   - způsobené strojním zařízením jako jsou: čerpadla; kompresory /dmychadla; míchadla / směšovače; mlecí zařízení; mechanické dopravníky; sušičky; odstředivky,
   - způsobené selháním komponent měření a regulace,
   - způsobené selháním elektrických komponent
   - způsobené nadprojektovými živelními poruchami.
3. Poškození materiálu komponent zařízení v důsledku:
   - vnitřní koroze,
   - vnější koroze,
   - koroze napětím,
   - koroze cyklickou únavou.
4. Výskyt neočekávaných (nepředvídaných) reakcí látek v zařízení:
   - neovladatelné / rozkladné reakce,
   - fyzikálně-chemické reakce,

- jiné nepředvídané reakce.

5. Neočekávaný výskyt elektrostatického náboje v zařízení.

Příčiny havárie určitého zařízení spojené s havárií jiných zařízení nacházejících se v podniku lze rozdělit do tří dále uvedených okruhů:

1. Domino efekt vyvolaný havárií jiného zařízení.
2. Selhání energie nebo dodávek potřebných látek:
   - selhání dodávek elektrického proudu,
   - neexistence nebo porucha záložního zdroje energie,
   - nedostatek nebo výpadek chladiva (voda či jiné chladivo v závislosti na používaných chemických látkách),
   - porucha pneumatického / elektrického měřícího a regulačního zařízení,
   - výpadek dodávek páry,
   - výpadek dodávek paliva,
   - výpadek dodávek látek jako je dusík či jiná inertní látka.
3. Dopad dopravní nehody uvnitř podniku na sledované zařízení.

Příčiny havárie určitého zařízení spojené s externími jevy v okolí podniku lze rozdělit do čtyř kategorií:

1. Domino efekt způsobený havárií zařízení v jiném podniku.
2. Dopravní nehoda vně podniku, která poškodí zařízení tak, že vyvolá jeho havárii.
3. Selhání infrastruktur a služeb:
   - výpadek elektrické sítě,
   - výpadek dodávek vody,
   - porucha produktovodů důležitých pro činnost zařízení,
   - výpadek informačních toků důležitých pro činnost zařízení.
4. Úmyslné útoky na zařízení a jeho činnost:
   - sabotáž,
   - vandalismus,
   - narušení datového toku v ovládacím zařízení.

Příčiny havárie určitého zařízení spojené s přírodními pohromami lze rozdělit do šesti kategorií:

1. Výskyt nadprojektové intenzity větru.
2. Výskyt nadprojektové teploty ovzduší (mimo podmínek stanovených v zadání).
3. Výskyt nadprojektového zemětřesení.
4. Výskyt nadprojektové povodně.
5. Výskyt nadprojektového sesuvu půdy.
6. Výskyt nadprojektových meteorologických podmínek - blesků, námraz, vlhkosti apod.

Příčiny havárie určitého zařízení spojené s chybami v řízení a organizaci podniku lze rozdělit do sedmi kategorií:

1. Nízká úroveň bezpečnostní kultury v podniku.
2. Nízká úroveň řízení bezpečnosti v podniku.
3. Neúměrné navyšování výroby na úkor dodržení bezpečných postupů při výrobě.
4. Chybné nebo nedostatečné pracovní postupy v podniku.
5. Zanedbávání péče o pracující.
6. Nedostatečná úroveň vzdělávání a výcviku v podniku.
7. Nedostatečné zabezpečení informovanosti pracujících při výskytu závažných nouzových situací.

Příčiny havárie určitého zařízení spojené s chybami v řízení provozu zařízení lze rozdělit do pěti kategorií:

1. Použití nesprávných algoritmů při poloautomatickém nebo plně automatickém řízení zařízení.

2. Použití nesprávných norem / pracovních postupů pro určitou výrobu.
3. Neprovedení adekvátního hodnocení rizik a z toho plynoucí podceňování možných nebezpečí.
4. Chybná nebo nevhodná režimová opatření, která umožňují opomenutí, použití nesprávných norem nebo předpisů.
5. Nedodržování ergonomických požadavků v relaci „člověk – stroj“.

Příčiny havárie určitého zařízení spojené s nedodržováním předpisů při provozu zařízení lze rozdělit do deseti kategorií:

1. Výrobní předpisy.
2. Předpisy pro údržbu.
3. Předpisy pro opravy.
4. Předpisy pro kalibraci regulačních a měřících zařízení.
5. Předpisy pro inspekci.
6. Předpisy pro tvorbu / konstrukci výrobků.
7. Předpisy pro vnitřní komunikaci.
8. Předpisy pro povolování specifických prací.
9. Předpisy pro laboratorní testy.
10. Předpisy pro skladování látek.

Všem průmyslovým nehodám a haváriím ve stabilních zařízeních s přítomností chemických látek je společné jedno stadium, které bývá v odborné literatuře označováno termínem „Loss of Containment“ [5] a znamená v chemickém průmyslu ztrátu soudržnosti nádoby či objektu. Proto je třeba upozornit, že v chemické průmyslové praxi je rozdíl oproti jaderné energetice, ve které je kontejnment realizován jako ochranná obálka reaktorové haly se všemi svými vlastnostmi a funkcemi. Podobný technický objekt se v chemickém průmyslu vyskytuje velmi zřídka a jen v několika zvláštních případech chrání zařízení bezpečnostní obálka – kontejnment. Většina velkých zařízení, jak výrobních, tak skladovacích je obvykle postavena na volných prostranstvích a jejich zařízení se zpravidla nacházejí pod širým nebem. Proto jakákoliv porucha v kterémkoliv místě technologického systému znamená ztrátu soudržnosti (také ztrátu obsahu nebo zádrže) tohoto systému a únik nebezpečné chemikálie do okolního prostředí, tj. na terén a do ovzduší. Některé, zejména malé úniky neboli úkapy, jsou nezbytné a vznikají zejména při přečerpávání chemikálií, protože zvláště některá čerpadla (ucpávková) nejsou nikdy absolutně těsná.

Havárie v České republice

Mezi technologické havárie s přítomností nebezpečných látek nejsou zahrnuty havárie, které jsou způsobené úniky zemního plynu, když se jedná o úniky v obytných domech, tedy mimo chemické závody. Nejsou zde uváděny výbuchy spojené se střelným prachem, když nešlo o jeho výrobu, ale o neopatrnou a neodbornou manipulaci s ním.

To znamená, že v databázi chybí exploze velkých zásob střelného prachu v Týně nad Vltavou ze dne 21. června 1753, ke které došlo během příprav na vojenské manévry konané během návštěvy Marie Terezie [340]. Bylo tam 80 mrtvých a 40 těžce zraněných. Nejsou tam ani výbuchy v muničním skladu blízko Vrbětic z roku 2014 [341-343].

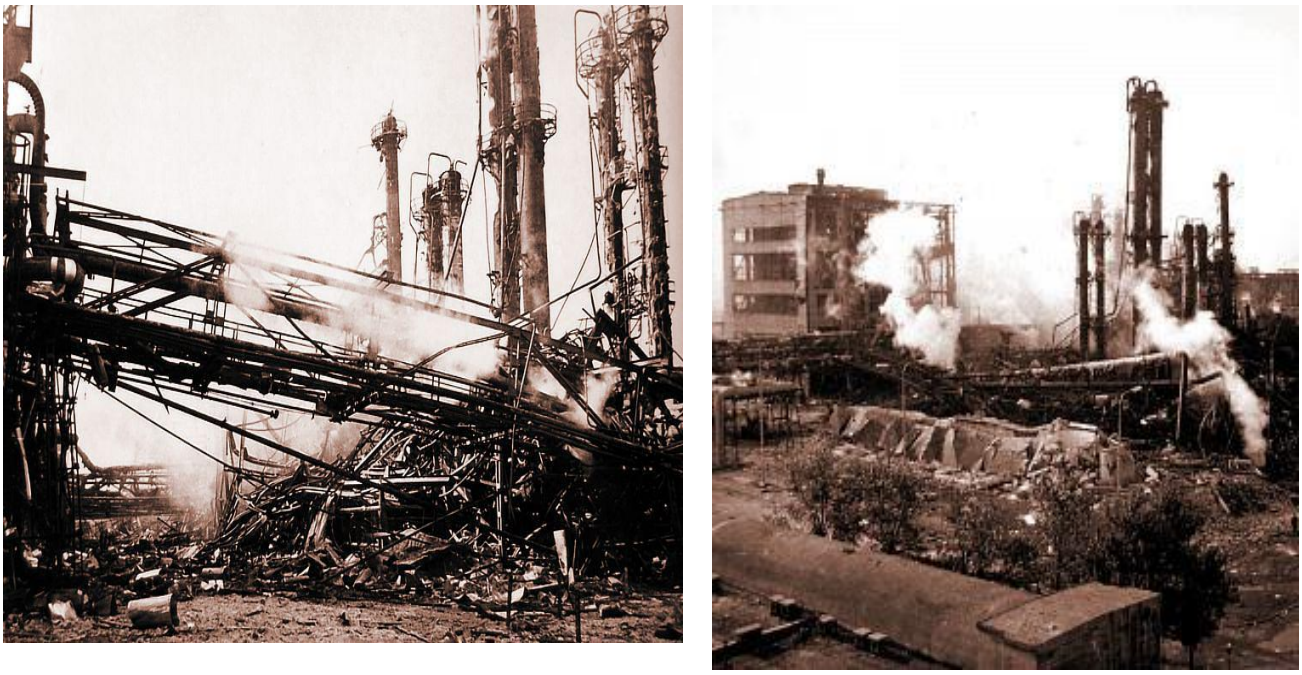
Pro získání dat do databáze jsme prostudovali dostupných 178 českých zdrojů [12], ze kterých jsme získali údaje pro 129 větších technologických havárií s přítomností nebezpečných látek od roku 1929. Dále uvedeme tři příklady větších havárií, o kterých se mnoho nemluví, ale obsahují jistá poučení, která platí dodnes.

Záluží (19. 7. 1974)

Výbuch ethenu v chemičce poničil 300 domů a zabil 17 lidí [344], tj. za takové kulisy by se

nemusel stydět žádný katastrofický film, obrázek 70 – 2 záběry. Den havárie byl nejtragičtějším dnem v historii Českých chemických závodů. Tak se hovoří o explozi z 19. července 1974 v tehdejší výrobně lihu v Záluží u Mostu. Katastrofa se stala při večerní směně. Nejdříve se ozvala jen dutá rána. Výrobní dispečer si pak všiml, že z potrubí uniká vysoce hořlavý plyn, a okamžitě běžel pro podnikové hasiče. Bylo přesně sedm minut po osmé hodině. Než ale stačili záchranáři naskákat do aut, ozval se ohlušující výbuch. Experti pak vypočítali, že měl sílu 20 až 30 tun TNT. Když zásahové vozy dorazily na místo, naskytl se jejich posádkám děsivý pohled. Kam oko dohlédlo, zuřil požár, jehož plameny zachvátily plochu velkou 36 tisíc metrů čtverečních. Do boje se živlem se postupně zapojilo 22 jednotek, tedy asi dvě stovky hasičů. To nejhorší se jim podařilo zlikvidovat až za čtyři dny [344].

Postupně se ukazoval neskutečný rozsah tragédie. Při výbuchu zemřelo 15 lidí, další dva pak v nemocnici podlehli těžkým popáleninám. Kromě nich lékaři ošetřili ještě 124 dalších zraněných. Část z nich pocházela z tramvaje, která v osudnou chvíli projížděla kolem závodu. Tlaková vlna srovnala se zemí část chemičky a poničila celkem 313 dalších objektů v okolí, z toho 220 rodinných domů. Některé přitom byly až osm kilometrů daleko! Na opravu všech vysypaných oken bylo zapotřebí 80 vagonů skla a celková škoda se vyšplhala na několik miliard korun [344].



Obr. 70. Výbuch ethenu v Záluží [344].

Vyšetřovatelé zjistili, že plyn začal unikat z kolena potrubí, které mělo korozí zeslabenou stěnu z původních šesti milimetrů jen na zlomek této hodnoty. Oblak vysoce výbušných par vzápětí zažehl otevřený plamen v přilehlé peci. Vina tak byla svalena na pracovníky údržby, z nichž tři stanuli před soudem a odpykali si tresty [344].

Lze jen uvést, že velká havárie v Unipetrolu 13. 8. 2015, při které na etylenové jednotce unikl etylen, což způsobilo několik výbuchů a velký požár nedosáhla škody a ztráty havárie popsané výše. Údaje shromážděné v [12] o této havárií ukazují:

- na likvidaci se podílelo 43 hasičských jednotek, tedy skoro 500 hasičů,
- byl vyhlášen zvláštní stupeň poplachu,
- dle inspekce (šetření dle zákona č. 224/2015, o prevenci závažných havárií): bylo na životech ohroženo asi 250 zaměstnanců; po výbuších byl zmatek; na místě nebylo chladivo, a tak hasiči 4 dny jen ochlazovali okolní budovy, aby se požár nerozšířil do okolí,

- nedošlo ke ztrátám na lidských životech,
- celková škoda přesáhla 850 mil. Kč., kterou téměř celou uhradila pojišťovna,
- ekonomické ztráty způsobené odstávkou technologie dosáhly téměř 9 miliard Kč,
- nefungoval veřejný rozhlas, a tak vznikla mezi lidmi v okolí podniku panika.

Pardubice (28. 5. 1984)

Došlo k výbuchu ve skladu střelného prachu (nitrocelulózy) v n. p. Východočeské chemické závody Synthesia Pardubice, který způsobil smrt 5ti zaměstnanců, na 200 těžkých řezných zranění a tisíce vybitých oken [345]. Nejvíce poškozeny byly budovy v přilehlé obci Rybitví a na přilehlých sídlištích Pardubic (poškozené střechy a praskliny ve zdech), vysklená okna však byla zaznamenána dokonce až ve dvacet kilometrů vzdáleném Hradci Králové a v Chrudimi. Příčinou neštěstí byla nepozornost při manipulaci s vozíkem, který převážel střelný prach. Tření železné hrany vozíku o nákladovou rampu vyvolalo jiskry, které způsobily vznícení převáženého nákladu a následně i výbuch celého skladu, po kterém zbyl jen kráter. Následky ale mohly být ještě horší, nebýt toho, že několik dní před výbuchem ze skladu většinu střelného prachu odvezli pryč [345]. Je absurdní, že kromě postiženého regionu byla pro zbytek republiky celá událost dokonale ututlána, noviny se omezily jen na kratičkou zprávu na nevýznamném místě a lidé z okolí se dodnes dohadují, co se vlastně stalo.

Kyjov-Boršov (3. 1. 1988)

Při požáru skladu agrochemikálií na jižní Moravě došlo k úniku velkých množství chemických látek. Od samého začátku došlo k řadě pochybení, která mohla mít katastrofální následky. Díky mnoha příznivým okolnostem a obětavosti účastníků likvidace požáru škody „Boršovbylu“, jak požár označila lidová slovesnost, nedosáhly takového rozsahu jako v roce 1976 v italském Sevesu, kde se následkem přehřátí chemického reaktoru začala syntetizovat látka TCDD, běžně zvaná dioxin [346]. Ani dnes nedovedou odborníci předvídat vznik nových toxických zplodin při požárech chemikálií.

Vyšetřování havárie ukázalo, že večer 3. ledna 1988 ve 21.08 hodin hlídač chemického skladu hlásil „požár v cihelně“. Sklad chemikálií byl sice ve staré cihelně, ale v Kyjově je ještě jedna cihelna v provozu, a tak se hasiči dostali k požáru s patnáctiminutovým zpožděním a začali hasit vodou, aniž věděli, co vlastně ve skladu hoří. Ve staré cihelně bylo uskladněno víc než padesát různých chemikálií o celkové váze 278 tun.

Vedle sebe byly hořlaviny, chlorované deriváty, organofosfáty, látky potencionálně samovznítitelné, organické i anorganické, pevné i tekuté uložené ve skleněných obalech, které při přehřátí vybuchují. Voda s hořícími chemikáliemi vytvořila velký mrak s dráždivými sloučeninami chloru a síry, stopami organofosfátů, kyanovodíků a arsenovodíku. Přivolaní odborníci vojenské části Civilní obrany z Bučovic měli k dispozici jen běžnou detekční techniku, která byla nedostatečná. 4. ledna 1988 provedl letecký průzkum letoun L− 410 a zjistil délku chemického mraku 5 km s šířkou 2 km. Díky inverzi se mrak šířil pomalu údolím Kyjovky [346].

Havarijní komise v nemocnici přijala okamžitá opatření, aby zvládla i větší postižení obyvatelstva toxickými látkami. Byla uvolněna polovina lůžek na interně, posílen personál a zaveden nepřetržitý provoz na interní ambulanci. Bylo rozhodnuto, že všichni účastníci likvidace požáru budou vyšetřeni klinicky a biochemicky a pokud budou zjištěny patologické hodnoty, budou ihned hospitalizováni. Na interním oddělení měli už zkušenosti s otravami organofosfátovými pesticidy, které jsou chemicky blízké bojovým chemickým látkám a vstřebávají se kůží a sliznicemi stejně rychle jako při požití [346].

Postupem hodin se zdánlivě uhašený požár k ránu znovu rozhořel a do jeho likvidace byly zapojeny jednotky báňských záchranářů z Jihomoravských lignitových dolů a Moravských naftových dolů, kolem požářiště se pohybovala řada příslušníků SNB, zaměstnanci ZNZ, řidiči

vozidel a další lidé [346].

Složitost toxikologické situace byla způsobena zahořením 173 tun chemikálií z 278 tun ve skladu, kde nebylo dodrženo pravidlo, že chemikálie mají být od sebe při uložení odděleny. Ze čtyř zvlášť nebezpečných jedů zahořely tři, z deseti látek zařazených mezi ostatní jedy zahořelo sedm [346].

Už ve večerních hodinách 4. ledna byly zjištěny patologické biochemické hodnoty u devíti účastníků likvidace požáru a byli přijati na interní oddělení. 6. ledna bylo přijato 17 pacientů, 7. ledna 25, o den později 14 pacientů. V následujících dnech až do 1. února počet postižených klesal [346]. V kyjovské nemocnici bylo hospitalizováno celkem 85 pacientů, v Hodoníně 10. Během týdne bylo vyšetřeno 591 osob a provedeno 1 397 laboratorních vyšetření. Hospitalizace si vyžádala 1 214 dnů a celková délka pracovních neschopností byla 3 974 dnů. Protože u 12 pacientů z patnácti provedených biopsií bylo zjištěno histologicky poškození jaterní tkáně, bylo dále sledováno 153 pracovníků z požářiště. Byli mezi nimi všichni hospitalizovaní a dále ti, kteří byli léčeni ambulantně. Sledování probíhalo šest měsíců a výsledky byly předány řediteli Okresního ústavu národního zdraví v Hodoníně, Klinice chorob z povolání Fakultní nemocnice Brno a prostřednictvím ředitelství OÚNZ i na Ministerstvo zemědělství a výživy [346].

S odstupem let už je obtížné oddělit fámy od skutečností. Pro evakuaci obyvatel bylo přichystáno 48 autobusů, které naštěstí nebyly použity. Je ale nutno přiznat fakt, že vládní orgány celou situaci zlehčovaly a ČTK zásobovaly sděleními rázu „situace je plně zvládnuta a pod kontrolou“, a v době, kdy na interním oddělení leželo prvních 26 pacientů, bylo možné si v novinách přečíst, že „při hasebním zákroku byli kouřovými zplodinami postiženy dýchací cesty čtyř požárníků a jednoho příslušníka SNB“ [346].

Lidé byli v roce 1988 už daleko kritičtější k reprezentantům strany a státu a nebáli se často veřejně vyjadřovat kriticky na pozdějších schůzích na téma boršovského požáru. Také Mladá fronta uveřejnila dva velmi kritické články během roku. Články si všímaly i skutečnosti, jak bude naloženo s 57 velkými ocelovými nádobami se zbytky chemikálií a kontaminované zeminy. Ze šesti různých variant byla vybrána jako nejschůdnější varianta ponechat toxický materiál na místě a zajistit jej do betonové vany, která bude zabezpečena proti průsaku i proti povrchovým vodám. Občané z okolí tomuto pohřebišti chemikálií říkají betonový sarkofág [346].

Jak dopadli účastníci likvidace požáru? Všichni byli vyšetřeni na Klinice chorob z povolání FN v Brně u sv. Anny, 142 z nich bylo odškodněno částkou od 800 do 1 650 korun, 98 bylo posláno do lázní, 2 dostali invalidní důchod. Všichni dostali plný plat za dobu pracovní neschopnosti. Zdá se vám to málo? Lze zdraví vůbec přepočítávat na peníze? [346].

„Boršovbyl“ měl i jednu kladnou stránku. Donutil k zamyšlení řadu odpovědných činitelů a výsledkem byla velmi přesná zpráva o celé situaci kolem požáru, kterou sepsal genmjr. Miroslav Budský a doc. MUDr. Vladimír Doležal, DrSc., i když jen pro vnitřní potřebu civilní obrany. Jsou v ní uvedeny všechny nedostatky a navrženo, jak by měly vypadat havarijní plány. Základním poznatkem z boršovského případu je, že čím menší informovanost v době katastrofy, tím větší prostor pro fámy, které už nepůjde nikdy docela vyvrátit [346].

Z analýzy databáze českých technologických havárií s přítomností nebezpečných látek [12] vyplývá, že mezi nejpočetněji zastoupené patří havárie s amoniakem (velmi často pouze s tzv. čpavkovými vodami), které představují téměř jednu pětinu, s chlórem, rovněž téměř jedna pětina havárií a s kyanidy s jednou desetinou ze všech havárií. U amoniaku se nejčastěji jedná o úniky z chladírenských zařízení, u chloru potom kromě výroby jsou zastoupeny úniky ze zařízení na úpravu vody. U kyanidů jde vždy o úniky do vod s následnou ekologickou havárií. Opět převažují úniky ze zařízení, která s kyanidy pracují, ne která je vyrábějí.

Havárie roztříděné podle nejvíce přítomných nebezpečných látek jsou:

- amoniak: Přerov (1966), Jeseník (1975), Příbram (1999), Hodonice u Znojma (2000), Praha (2000), Mochov (2000), Cheb (2001), Praha (2001), Cheb (2001), Havlíčkův Brod (2001), Liberec (2002), Hroznětín (2003), Praha (2004), Tachov (2005), Malý Rohozec (2007), Roudnice n. L. (2007), Praha (2010), Prachatice (2010), Domažlice (2013), Rosice (2013),
- chlor: Ústí n. L. (1982), Neratovice (1991), Ústí n. L. (1996), Ústí n. L. (1996), Neratovice (1998), Prostějov (1999), Ústí n. L. (1999), Neratovice (2000), Neratovice (2002), Neratovice (2002), Ústí n. L. (2002), Neratovice (2002), Varnsdorf (2004), Ústí n. L. (2005), Nový Rychnov (2006), Karviná (2007), Neratovice (2008), Vítkov u Opavy 2009),
- kyanidy: Jihlava (1964), Kopřivnice (1967), Blatná (1969), Frýdek-Místek (1973), Turnov (1976), Rožnov pod Radhoštěm (1979), Hořovice (1980), Žatec (1981), Adamov (1986), Ostrava (1998), Kolín (2006).

Ropné produkty a zemní plyn jsou zastoupeny rovněž, ale nejsou na rozdíl od havárií ve světě dominantní, mají zastoupení necelé jedné desetiny ze všech havárií. Jde např. o havárie:

- asfalt: Pardubice (2005),
- benzín: Litvínov (1981), Litvínov (1996), Litvínov (2009),
- ethen: Záluží (1974),
- LPG: Praha (2003),
- minerální oleje: Pardubice (1994),
- nafta: Pardubice (1966)
- propan-butan: Žižice (2001), Mladá Boleslav (2003).

Výbušniny, díky pardubické Explozii Semtín si najdou též své zastoupení. Podílejí se na tom cca 6 %, ale následky jsou nesrovnatelně větší. Např.:

- nitroglycerin: Pardubice (2011),
- střelný prach: Pardubice (1984), Pardubice (1995)
- výbušniny: Semtín (1929), Semtín (1937), Semtín (1938).

Mezi zbytkem, který představuje cca 40% havárií, mají své zastoupení jak hořlaviny, tak látky jedovaté. Jsou zde kyseliny (kyselina chlorovodíková, či chlorovodík, kyselina dusičná, sírová, chlorsulfonová, deriváty kyseliny sulfonové), deriváty síry (kromě zmíněné kyseliny sírové též sulfan – sirovodík, oxid siřičitý a sírový), ale i dioxiny a pesticidy. Např.:

- agrochemikálie: Kyjov-Boršov (1988)
- dichlormethan: Opava (2009),
- dioxiny: Neratovice (1965-68), Neratovice (2002),
- epoxidové pryskyřice: Ústí n. L. (2002),
- ethylacetát: Břidličná (1997),
- fenoly: Vřesová (1970), Neratovice (1978),
- fosgen: Pardubice (1974),
- hydroxid vápenatý: České Meziříčí (2007),
- chlorované uhlovodíky: Krásné Březno (1983),
- chlorovodík: Neratovice (2001),
- kyanurchlorid: Pardubice (1997),
- kyselina alkylarylsulfonová: Rakovník (1970),
- kyselina dusičná: Smiřice (2001), Pardubice (2005), Chrudim (2014),
- kyselina chlorovodíková: Olomouc (1998), Bohumín (1999), Olomouc (1999), Slatiňany (2009),
- kyselina chlorsulfonová: Neratovice (2000),
- kyselina sírová: Mladá Boleslav (1982), Hlinsko (2003),
- lněný olej: Ústí n. L. (1987),
- měď: Mladá Boleslav (1982)
- melasa: Chrudim (1969),
- močovinoformaldehydové pryskyřice: Jihlava (1998),

- nitrocelulozové barvy: Bojanovice (1997),
- nitrozní plyny: Pardubice (2004), Pardubice (2010),
- oxid siřičitý: Přerov (2001), Neratovice (2002),
- oxid sírový: Ústí n. L. (2004), Ústí n. L. (2004),
- pesticidy: Frýdek-Místek (2008),
- pryskyřice: Bělá nad Radbuzou (1998),
- sirovodík: Olomouc (1996),
- trchlorsilan: Rožnov p. R. (2002),
- vinylchlorid: Neratovice (1991), Neratovice (1993), Neratovice (2002).

Výsledky uvedené výše ukazují, že mnoho havárií je způsobeno nedodržováním norem, provozních postupů, bezpečnostních předpisů, špatnou údržbou zařízení a podceněním situace. Proto je třeba zlepšovat kulturu bezpečnosti [1,2,10,11] a do praxe implementovat účinné programy na zvyšování bezpečnosti [1,10].

Výskyt atypických havárií, jejichž příčinou byly neočekávané kombinace jevů, vede k tomu, že kvalitní plány odezvy musí zvažovat více scénářů havárií [11].

Při screeningu příslušné odborné literatury velmi často se setkáváme s látkami chlór, amoniak, dusičnan amonný a dioxiny. Chlór a amoniak se řadí mezi látky s toxickými vlastnostmi. Bez chlóru se neobejde žádný plavecký bazén a žádná úpravna vody, bez amoniaku žádný zimní stadion a žádné chladírenské zařízení. Po chemické stránce patří mezi látky, u kterých je jejich výroba bezproblémová, vlastnosti jsou všeobecně známé a jejich přítomnost, v případě úniku, je velmi snadno detekovatelná.

Další látka dusičnan amonný, patří mezi velmi rozšířená hnojiva, takže možnost se s ním setkat je velmi častá, ale bohužel patří též mezi látky záludné, poněvadž funguje také jako výbušnina. Lze říci, že při manipulaci s ním se deset tisíckrát nic nestane a po desetitisící a jedné máme na místě fabriky, skladu či podobně, hluboký kráter s okolím dokonale zničeným. Vysvětlení je nutné hledat v jeho chemických vlastnostech.

Buncefield (Velká Británie), 11. 12. 2005.

Ve skladišti a distribučním terminálu ropných produktů došlo k přeplnění zásobníku č. 9012. Mrak par, který se utvořil z uniklého paliva, zakrátko explodoval za následného vzniku rozsáhlého požáru, při němž bylo zraněno více než 40 osob. Vyšetřování ukázalo, že instalovaný servomechanický hladinoměr indikoval neměnnou polohu hladiny, ačkoliv zásobník byl v té době plněn benzínem. Na zásobníku byl současně nainstalován mechanický detektor horní mezní polohy hladiny, který také selhal a nevydal výstražný signál.

Z analýzy údajů v [12] vyplývá, že nehody ve skladech a výrobách kapalných uhlovodíků jsou charakterizovány: velkou rychlostí šíření požáru, velkou intenzitou hoření spojenou s vývinem značného množství tepla a vysokou teplotou plamene, intenzivní výměnou plynů a uvolňováním velkého množství zplodin hoření, možností výbuchu, nebezpečím rozšíření požáru do okolních prostor; při postupující degradaci sousedních nádrží s hořlavými kapalinami, může intenzita hoření skokově narůstat, možností šíření požáru roztékáním hořících kapalin, nebezpečím úniku nebezpečných látek.

5.10.3. Nebezpečné nežádoucí vedlejší produkty výroby

Dioxiny, se kterými se na první pohled nemusíme setkávat tak často, patří mezi nejtoxičtější látky. Jejich přítomnost se nám na rozdíl od chlóru nebo amoniaku, nikterak neohlásí, v řadě případů jsme po dlouhá léta vystaveni jejich účinkům, a teprve poté detekujeme jejich důsledky. Většinou nejsou cíleně připravovány, setkáváme se s nimi jako s nežádoucími produkty při nedokonale zvládnuté syntéze jiné požadované látky, vznikají v řadě případů, při nedokonalém spalování plastů na bázi chlorovaných polymerů, a při uvolnění do životního prostředí

poškozují lidí i vše živé. V přírodě se velmi pomalu rozkládají (podobně jako další halogenované organické sloučeniny) a díky své rozpustnosti v tucích mají schopnost se akumulovat v tukových tkáních.

Dioxiny je obecný název pro skupinu toxických polychlorovaných organických heterocyklických sloučenin, odvozených od dibenzo(b,e)(1,4) dioxinu, obsahujícího šestičlenný 1,4-dioxanový cyklus. Většinou se mezi ně řadí i polychlorované deriváty dibenzofuranu. Nejznámějším dioxinem je 2,3,7,8-tetrachlordibenzo-p-dioxin (TCDD), který vzniká nedokonalým spalováním chlorovaných organických látek, například dichlorbenzenu.

Ve velmi vysokých dávkách způsobují dioxiny trvalé poškození pokožky známé jako chlorakné. V nízkých dávkách je dioxinům připisována teratogenita (vývojová toxicita) a karcinogenicita. Karcinogenita TCDD byla potvrzena v roce 2001, kdy byl dioxin překlasifikován ze skupiny „pravděpodobný karcinogen“ (2A) na „známý karcinogen“ (1). Na rozdíl od většiny jiných toxických látek či karcinogenů není pro dioxin stanovena bezpečná dávka; předpokládá se, že je škodlivý v jakékoliv detekovatelné koncentraci. Některé zdroje dokonce udávají, že TCDD je nejsilnější známý karcinogen.

Dioxin, přesněji 2,3,7,8-tetrachloro-dibenzo(b,e)(1,4)dioxin, zkratkou TCDD, je bezbarvá nebo bílá krystalická látka, vysoce toxická a znečišťující přírodní prostředí. Patří do širší skupiny tzv. dioxinů, jejímž je nejvýznamnějším zástupcem. Po chemické stránce patří mezi kyslíkaté heterocyklické sloučeniny, odvozené od 1,4-dioxanu. Vzniká jako vedlejší produkt při výrobě herbicidů, resp. jejich polotovarů jako 2,4,5-trichlorofenolu a 2(2,4,5-trichlorofenoxy) propanové kyseliny. Vytváří se také neúplnou oxidací 1,2-dichlorbenzenu, což je příčinou jeho výskytu v kouřových plynech špatně technologicky řešených spaloven komunálního odpadu, obsahujícího chlorované plasty, především polyvinylchlorid (PVC).

Na počátku třicátých let začala americká firma Dow Chemical vyrábět nové prostředky na konzervování dřeviny — polychlórfenoly, první látky obsahující dioxin. Už v roce 1936 se ve státě Mississippi objevily v masovém měřítku mezi dělníky, kteří pomocí tohoto prostředku zpracovávali dřevo, různé převážně kožní choroby. Postupem doby přicházely zprávy o nových a nových analogických případech. Jejich dalšímu rozšíření napomohla druhá světová válka. Právě tehdy byly v USA na základě stejných látek získány první herbicidní přípravky, které měly v podstatě hormonální účinky. Měly být použity k ničení vegetace v Japonsku, ale do výzbroje americké armády byly zařazeny až po válce. V téže době se začaly používat i pro mírové účely — k hubení plevele v obilných porostech, k ničení porostů křovin a stromů. Vojenskoprůmyslovým kruhům USA to umožnilo vybudovat ohromné výrobní kapacity.

Různých havárií a případů poškození zdraví bylo při výrobě těchto látek velmi mnoho, ale téměř nikdy nebyla veřejnost informována. Ještě dnes se neví, jaké následky zanechaly na zdraví obyvatelstva a na životním prostředí. Zvláště v letech 1961 až 1970 docházelo často k úniku dioxinu. Závody vyrábějící dioxin pracovaly na nejvyšší obrátky, aby uspokojily ohromné vojenské objednávky armády USA, která herbicidy používala v jižním Vietnamu. K explozím a následnému poškození zdraví nedocházelo pouze v továrnách v USA, ale také v bývalém Německu (NSR), Holandsku, Francii, Itálii a ve Velké Británii. S výjimkou případů, ke kterým došlo ve Francii, tomu až do konce sedmdesátých let 20. století tisk nevěnoval pozornost.

K nejhorším patřila havárie v továrně firmy Philips Duffar v roce 1963 v Amsterodamu. Po havárii byly výrobní haly demontovány a potopeny v oceánu. Strašná byla i katastrofa v italském Sevesu v roce 1976, kdy byli postiženi nejen zaměstnanci továrny, ale i místní obyvatelstvo. Při likvidaci následků bylo nutno na velkém území odstranit povrchovou vrstvu orné půdy.

Přitom byla vysoká toxicita dioxinu zjištěna už v roce 1957 skupinou vědců v NSR a zároveň i v USA po nešťastném případu s americkým chemikem J. Dietrichem, který se věnoval syntéze dioxinu a příbuzných látek. Avšak i tato skutečnost byla před veřejností utajena a sloučeniny

syntetizované J. Dietrichem převzaly k dalšímu výzkumu vojenské úřady. Tehdy už dioxin jako součást nejrůznějších přípravků v široké míře pronikl do techniky, zemědělství, textilního a papírenského průmyslu, do medicíny a veterinárního lékařství. Kolem roku 1960 dosahovala výroba těchto přípravků impozantní úrovně mnoha tisíc tun ročně. Biocidní, insekticidní a herbicidní přípravky obsahující dioxin se vyvážely do velkého počtu zemí amerického evropského kontinentu, dále do některých zemí Afriky a jihovýchodní Asie, do Austrálie a Oceánie. Dioxin se dostával do orné půdy i vodních ploch značné části světa.

Později se zjistilo, že herbicidy, které byly v šedesátých letech dodávány na americký vnitřní i zahraniční trh, obsahovaly dioxin v koncentracích stokrát a dokonce i tisíckrát převyšujících přípustnou mez. Do životního prostředí se tak v USA dostaly stovky kilogramů jedu. Přibližně stejné množství se objevilo i na území států, které výrobky z USA dovážely [347].

Problémům spojeným s výskytem dioxinů nebylo ušetřeno ani naše území, tedy Československo. Koncem 60. let 20. století byla Spolana jedním ze tří výrobců chemických prostředků pro zemědělství a lesnictví u nás. Vyráběla rovněž Arboricid - herbicid obsahující jako účinnou látku sodnou sůl kyseliny 2,4,5-trichlorfenoxyoctové (2,4,5-T). Účinná látka byla prodávána i do zahraničí a míchána s 2,4-dichlorfenoxyoctovou kyselinou (2,4-D) do směsi známé jako Agent Orange a používané armádou USA během války ve Vietnamu. Během výroby vznikaly jako vedlejší nežádoucí produkty dioxiny, které zamořily výrobní objekt a 2 sklady a vedly k vážným nemocem části zaměstnanců výrobního provozu koncem 60. a začátkem 70. let 20. století [348].

Vyhodnocením shromážděných údajů byly identifikovány nouzové situace, které způsobil dioxin jako vedlejší produkt žádoucích chemických reakcí, a které významně poškodily veřejná aktiva tabulka 59.

Tabulka 59. Pohromy způsobené dioxinem jako vedlejším produktem žádoucích chemických reakcí.

Místo a čas	**Příčina**	**Důsledky**
Nitro, West Virginia (fa Monsanto, USA, 1949) – výroba kyseliny 2,4,5-tri-chlorophenoxy-octové	Otevření pojistného ventilu.	Zasaženo 240 osob. Zvýšila se úmrtnost ze sarkomů měkkých tkání, močového měchýře a rakoviny dýchacích cest [349].
Ludwigshafen (fa BASF, Německo 17. 11. 1953) - výroba dioxinu	Únik z tlakové nádoby.	Účinkům bylo vystaveno 55 osob, jeden zaměstnanec zemřel, postižení trpěli chlorakné. Výroba byla později zastavena a budova v roce 1968 za velkých bezpečnostních opatření zbořena [350,351].
Amsterdam (fa Philips-Duphar, Nizozemí 6. 3. 1963)	Exotermická reakce v závodě Philips-Duphar v blízkosti Amsterdamu, která způsobila explosi v několika trichlorfenolových reaktorech. Teplota vystoupala na 400 – 450 °C a tlak na 80 atmosfér.	Únik dioxinového mraku. Závod byl po nehodě tak znečištěn dioxinem, že musel být demontován, vložen do betonu a vhozen do moře [352].

Buttermilk Lane (fa Coalite Chemical Productions, Derbyshire, Velký Britanie, 1968) - výroba 2,4,5-trichlorfenolu	Exploze v poloprovozním zařízení.	Zabit chemik a dioxiny se rozšířily nad troskami. 79 zaměstnanců bylo postiženo chlorakné. Společnost neuveřejnila umístění lokality, kde byly uloženy kontaminované trosky a poznámky nezávislého vyšetřovatele byly ukradeny [353].
Seveso (fa Icmesa Chem.Corp., Itálie 10. 6. 1976)	V chemické továrně společností ICMESA (Industrie Chimiche Meda Società) vybuchl chemický reaktor a z ventilu umístěného mimo budovu vytryskly do ovzduší horké jedovaté páry. Do ovzduší unikly dva kilogramy dioxinu (což je množství, které by dokázalo otrávit přibližně 19 000 lidí) a zamořily plochu téměř 2 000 hektarů.	Vytvořil se bílý oblak a mírný vánek jej zanesl k městečku Seveso. Ptáci, které zasáhl v letu, padali mrtví k zemi. Oblak pokryl plochu dlouhou pět kilometrů a širokou sedm set metrů. Děti si nic netušíce hrály dál. Brzy se však u nich začaly projevovat bolesti hlavy, dýchací potíže a svědění pokožky. Zasažená byla i další města - Meda (19 000), Desio (33 000), Cesano Maderno (34 000) a v menším rozsahu Barlassina (6 000) a Bovisio-Masciago (11 000). Působení toxického mraku bylo vystaveno 37 000 lidí, z nichž bylo 736 evakuováno na 6 měsíců. Na následky otravy onemocnělo na 200 dospělých a mnoho dětí. Zranění kůže (tzv. chlorakné) utrpělo 447 osob. Preventivně došlo k řadě potratů, 4% místních zvířat zemřelo (většinou drůbež a králíci), a následně bylo 80 000 zvířat preventivně usmrceno, aby se dioxin nedostal do potravinového řetězce. Jen zázrakem nikdo bezprostředně po havárii nezemřel [354].
Niagara Falls (fa Hooker Chemical) Love Canal, USA, 1978)	Kdysi nedokončený kanál byl používán chemickou firmou jako skládka, 21 000 tun chemikálií a mezi nimi byly i chlorované uhlovodíky	Při výstavbě v dalších letech byly objevovány při výkopech sudy s chemickými odpady, při přívalových deštích se tvořily kaluže barevných tekutin. Nálezy vrozených vad a mnoha anomálií, abnormální výskyt potratů [355].
Times Beach 1978 (Missouri, USA)	Při úpravě silnic v letech 1972-76 byl použit vyjetý motorový olej smíšený s průmyslovým odpadem z továrny vyrábějící Agent Orange (kódové označení používané armádou USA pro směs dvou herbicidů 2,4-dichlorfenoxyoctové kyseliny (2,4-D) a	Evakuace 2000 obyvatel a hermetické uzavření St. Louiského předměstí Times Beach do roku 1985 – vytvoření města duchů. Kompletně zbouráno v roce 1992. V letech 1996-97 provedena dekontaminace odstraněním 240 000 tun zeminy. Na místě zbudován „Route 66 State Park“. [356].

	2,4,5-trichlorfenoxyoctové kyseliny (2,4,5-T).	
Belgie – květen 1999	K výkrmu domácího zvířectva použito kontaminované krmivo.	Potravinářská inspekce zjistila přítomnost polychlorovaných bifenylů (PCB) s dioxinovým efektem v živočišných produktech, především ve vejcích a kuřatech. K ochraně lidí bylo poraženo 7 000 000 kuřat a 60 000 prasat [357].
Itálie 2007	Pozemek, který spásali buvoli, byl kontaminován ilegálně likvidovanými odpady s dioxinem.	Potravinářská inspekce zjistila polychlorované dibenzodioxiny v buvolím mléce, které používalo 29 výrobců mozzarelly. Prodej mozzarelly klesl v Itálii o 50% [358].
Irsko 2008	K výkrmu bylo použito kontaminované krmivo jednoho z dodavatelů.	Dioxiny byly zjištěny na 45 farmách, testy překračovaly 200-krát bezpečnou úroveň. Nakonec byl omezen dovoz vepřového masa z Irska do 23 zemí a bylo zlikvidováno 100 000 prasat [359].
Německo 2010	Do průmyslově vyráběných krmiv byl přidán krmný tuk, který byl vyroben z technické směsi mastných kyselin, jež vzniká při výrobě bionafty. Daná směs byla kontaminována dioxiny, byla podávána drůbeži, prasatům a později i skotu.	Úřady v Německu zavřely přes tisíc zemědělských podniků (drůbežáren, vepřínů). Kontaminované vepřové maso bylo dovezeno i do ČR [360].

Vedlejší produkty byly a často i dosud jsou považovány za odpad, a proto jim je věnována menší pozornost při řízení bezpečnosti. Příkladem, kam může vést snížená pozornost vedlejším produktům a jejich likvidaci je, i když nejde o dioxiny, „objev“ přítomnosti chlorovaných uhlovodíků v pivu. Při náhodném vyšetření vzorku piva ze závodu Severočeského pivovaru v Krásném Březně v roce 1983 byl zjištěn obsah 57 µg/l trichlorethylenu a 40 µg/l perchlorethylenu. Následným stanovením bylo stanoveno, že voda ze studny pivovaru obsahuje 478 - 611 µg /l TCE a 286 - 345 µg/l PCE, provedený další průzkum okolních studní prokázal ještě vyšší koncentrace, např. studna lihovaru 1 140 µg/l TCE. Bylo provedeno rozsáhlé šetření v 16 okolních průmyslových závodech, 7 z nich používalo chlorované uhlovodíky, ve vzdálenosti od studny pivovaru bylo skladování chlorovaných uhlovodíku n. p. Chema, ale i u dalších podniků byly zjištěny nedostatky ve vodohospodářském zabezpečení nakládání s těmito látkami. Bylo vybudováno náhradní zásobování pitnou vodou z veřejného vodovodu. Rozbory archivovaných vzorků lihovin bylo prokázáno, že uvedená kontaminace nebyla krátkodobou záležitostí, přítomnost TCE a PCE v lihovinách byla zpětně prokázána i ve vzorcích z roku 1975 [361].

Rozhodně nejvýznamnějším zdrojem dioxinů v životním prostředí je spalování organických sloučenin, především komunálního odpadu. Důvodem je především fakt, že aromatické

benzenové jádro je značně stálé a při spalování organických sloučenin dochází k přednostní oxidaci běžných uhlovodíků. Benzenový skelet přitom často zůstává nedotčen a jeho reakcí s kyslíkem a chlorem vznikají dioxiny.

5.10.4. Radiační a jaderné havárie

Jaderné elektrárny i další jaderná zařízení v současné době patří mezi kritické objekty, jež jsou sledovány v souvislosti se zajišťováním bezpečnosti nadnárodních uskupení a států v souvislosti s ochranou kritických infrastruktur. Proto v rámci výzkumu musíme také věnovat pozornost jaderné oblasti a jaderným zařízením.

Je pravdou, že od svržení bomb na Hirošimu a Nagasaki má lidstvo velké obavy z jevů, při kterých dochází k uvolnění radioaktivního záření, explozi a k uvolnění velkého množství tepla. Obavy lidstva posílily jak dopady jaderných testů, tak dopady havárií civilních jaderných zařízení, které pomáhají naplňovat potřeby lidí a zajišťovat jim kvalitní život.

Jelikož jaderná zařízení jsou významnými prvky energetické a výrobní infrastruktury, jsou potřebná, a proto je nutné zajistit jejich bezpečnost. Prvním krokem je poučit se z minulých havárií, pochopit rizika a jejich dopady v souvislostech. Na základě poznání je pak možné udělat kvalifikovaná opatření pro bezpečnost a ochranu občanů, veřejných aktiv, samotných jaderných zařízení a vůbec celého státu.

Proto jsme sestavili na základě dostupných údajů databázi, která obsahuje jak souhrn jaderných havárií, jejich příčin a dopadů, tak souhrn vojenských jaderných útoků a testů a jejich dopadů [12].

Na základě kritického posouzení údajů v [12,362] jsme odvodili následující fakta:

- od r. 1954 (kdy byl zkonstruován první jaderný reaktor) již bylo více než 100 jaderných havárií a nehod na civilních objektech:
    - jaderné elektrárny (roztavení aktivní zóny: 1969 Vaud, 1979 Three Mile Islands, 1986 Černobyl, 2011 Fukushima, menší Idaho 1954….; únik radioaktivity: např. 1980 Saint Laurent, 1986 Hamm a další),
    - havárie v průmyslu (např. 1957 Majak u Čeljabinsku – výroba plutonia a přepracování vyhořelého paliva; 1957 Hanford v Richlandu – přepracování jaderného paliva; 1999 Tokaimura – přepracování jaderného paliva),
    - havárie v nemocnicích ((Mexiko, Brazilie, USA, Španělsko, Maroko, Thajsko, Jižní Afrika, Indie, Egypt, Izrael a další),
    - havárie v laboratořích (např. 1957 v Simi Valley (Kalifornia); Izrael, Čína, Estonsko, Maďarsko a další),
    - přeprava jaderných materiálů,
- od r. 1940 již bylo několik set jaderných havárií na vojenských objektech:
    - útoky (1945 Nagasaki, Hirošima),
    - vojenské reaktory (např. 1952 Ontario, 1957 Windscale (Sellafield a další),
    - letecká přeprava bomb (záznamy jsou od r. 1950),
    - jaderné ponorky (záznamy havárií jsou od r. 1963),
    - jaderné testy (nadzemní: USA-1032, Rusko-792, VB-88, Francie-212, Indie-3, Čína-47, Pákistán, Severní Korea-3; nejvíce podzemních USA přes 1000 zkoušek v Pacifiku a více než 900 v Nevadě; Rusko – Semipalatinsk, Novaja Zemlja cca 600).

Na některých místech došlo k haváriím opakovaně, v řadě případů ze stejné příčiny, a proto jsou uvedeny v jednom bloku. Z hodnocení vyplývá, že:

- IAEA registruje 1266 jaderných nehod za posledních 12 let v 99 zemích,
- jaderné havárie a jaderné nehody se nevyhýbají žádnému typu reaktoru, žádné jaderné elektrárně a žádnému státu,

- dobře zvládají jaderné nehody jaderné elektrárny s tlakovodními reaktory typu PWR s kontejnmentem (tj. typ, který je v ČR),
- jsou jaderné elektrárny, které přežily jaderné nehody i jaderné havárie a po rekonstrukci obnovily provoz,
- mnoho firem tajilo jaderné nehody a havárie před světem i občany v okolí, a tím nedošlo k nasazení ochranných opatření u občanů,
- u mnoha jaderných havárií a nehod hrál významnou roli lidský faktor. Je skutečností, že i když bezprostřední příčinou byla technická závada nebo chybný úkon obsluhy, tak se vždy našly chyby v dlouhodobém řízení a kultuře bezpečnosti, což znamená, že události spadají do kategorie označované od r. 1981 jako organizační havárie.

Proto nezbývá nic jiného, než konstatovat, že jaderná zařízení jsou složitá technologická zařízení typu systémy systémů [1], a proto v souladu s výsledky Charlese Perrowa z roku 1980 získanými po důkladné analýze jaderné havárie TMI [37] je třeba u nich mít po všech stránkách připravenou kvalifikovanou odezvu (personál, odpovědnosti, postupy, materiál, techniku).

Analýza ze světa shromážděných údajů ve [12] odhalila velmi mnoho nehod s jadernými materiály v nemocnicích a také velmi mnoho v dobré víře prováděných testů jaderných materiálů na lidech vedoucích k úmrtí. Proto je důležité upozornit na roli kultury bezpečnosti v předmětné oblasti a u výzkumu zdůraznit roli předběžné opatrnosti.

Jaderné materiály a technologie zlepšují kvalitu života lidí. Protože z aplikace poznatků z přírodovědných, technických i sociálních věd vyplývá, že nic není absolutní, tak je v každém technologickém zařízení nutno počítat s poruchami, nehodami, skoro nehodami i haváriemi.

Z pohledu ochrany životů a zdraví lidí nás především zajímají jaderné nehody a havárie, které mají významné dopady na lidi, životní prostředí nebo samotné zařízení. Proto se musíme velmi dbát na bezpečnost jaderných materiálů a jaderných zařízení, tj. kvalifikovaně pracovat s riziky, a protože v čase přibývají stále nová rizika, tak je třeba sofistikovaně řídit bezpečnost jaderných zařízení v čase, což platí pro všechna složitá technologická zařízení.

5.10.5. Poučení z minulých havárií technických děl

Dosavadní provedené analýzy havárií provedené v širokém kontextu, tj. nejenom podle struktury provozu, [304-306,308-314] ukázaly, že příčinami havárií složitých technologických systémů jsou:

1. Externí systémy, tj. vlivy mimo hranice systému, které na něj působí, ale nejsou významně ovlivněny systémem samotným, jako: vliv nové legislativy; vliv externích inspektorů; nedostatečná podpora mateřské společnosti; tlak od zákazníků; know-how; nedostatečné vazby mezi vnějšími službami; nedostatečné informace o toxicitě a způsobu léčení postižených chemickými látkami; nátlakové skupiny; přehnaný místní stavební rozvoj; vývoj v životním prostředí.
2. Klima v systému, tj. vlivy jako obchodní faktory, kultura ve společnosti, bezpečnostní kultura a technické know-how, které reprezentují víru, vnímání a očekávání jednotlivci uvnitř této společnosti, jako: nedostatečné procesní a technologické know-how; nedostatečné průmyslové normy; změněné požadavky na umístění; záměrná porušení; pojišťovací požadavky; veřejné mínění; nekorektní oznámení rizik; nedostatek personálu a zařízení; nedostatek nároků na výrobky; výrobní kapacita; rozmístěn zdrojů a dostupnost; investiční strategie; expanze do méně obydlených nebo méně bezpečných oblastí; zájem na profitu; nedostatečné zkušenosti; sociální postoje; špatný přístup managementu k bezpečnosti; nízké uvědomění o rizicích.
3. Organizace a řízení, tj. možnosti pro řešení problémů a učinění závěrů v systému jako: nedostatečná strategie; nedostatečné pracovní priority; absence bezpečnostního oddělení; není deklarace bezpečnostní politiky; nejasné směrnice k bezpečnosti nebo řízení rizika;

nedostatečná organizační rozhraní; nevyjasněné vztahy mezi skupinami; nedostatečná komunikace; nedostatečné projekční a inženýrské zabezpečení; špatné umístění zařízení; nedostatečná analýza rizika; nedostatečné finance; nedostatečná výrobní kapacita; úroveň obsluhy.

4. Umístění objektu a výrobní zařízení ve vztahu k projektu a jeho realizaci, jako: chybné určení bezpečnostních zón a oddělení zařízení; nedostatečná bezpečnostní zařízení; nedostatečné nouzové postupy; nedostatečná ochrana před vnějšími riziky; nedostatečná dokumentace; nedostatečné určení požadavků; nedostatečná předběžná analýza rizika; chyby ve stavbě; neodpovídající montáž zařízení podle projektu; chyby v řízení prací; nevhodný způsob dopravy; nevhodné skladování a skladování ve velkých objemech; nevhodné použití materiálu.
5. Technická integrita, tj. otázky spolehlivosti a použitelnosti zařízení, včetně života zařízení - projekt, stavba, provoz, údržba a kontrola jako: nedostatečný projekt nebo specifikace služby; nedostatečná kontrola kvality; nevhodné nástroje a zařízení; nedostatečná výrobní pohotovost; nedostatečná dokumentace; nepřiměřené prodloužení životnosti zařízení; nedostatečná preventivní údržba; nekvalifikovaně a nedostatečně provedené opravy; nevhodná modifikace; nedostatečné řešení změn; nevhodné standardy; nevhodné specifikace a/nebo projektová kritéria.
6. Kontrola řízení z pohledu řízení bezpečnosti jako: chybějící kapitál; chybějící personál nebo čas; nepřiměřené plánování a kontrola zdrojů; nedostatečná provozní opatření; nedostatečné korigující akce; nedostatečná odezva na změnu; změna v technologii, zařízení nebo postupech; chyba ve vnímání nebo výběru mezi podmínkami; nedostatečný bezpečnostní výcvik nebo technické znalosti; nedostatečné definování odpovědnosti; akceptování rizika na příliš nízké úrovni; nesprávné příkazy a delegování; nedostatečná kontrola pracovního klimatu a praktik; nejasné nebo konfliktní určení odpovědností; zanedbávání bezpečnostních faktorů; chybějící přehled o bezpečných postupech; chabé nouzové plánování; špatná koordinace havarijní odezvy uvnitř/v okolí zařízení.
7. Komunikace a informace, tj. informace životně důležité z hlediska bezpečného provozu zařízení jako: nedostatečná verbální komunikace; nedostatek informací; chybné informace o zařízení a procesu; nedostatečné informace o materiálu; nedostatečné modelování scénářů havárií; nedostatečná bezpečnostní dokumentace; absence informačních kanálů; nedostatečný monitoring a sběr dat; nedostatečné informování; nesprávná odezva na informace; nevhodné řídící centrum; nedostatečné znalosti modelů úniků; nedostatečné postupy odezvy; absence informačních kanálů pro případ havárie; přetížení zařízení.
8. Postupy a praxe, tj. jasné postupy pro bezpečný způsob nakládání s nebezpečnými látkami, výrobní postupy a operace jako: nepřiměřené provozní/údržbářské postupy; nedostatečná pracovní disciplína; nedostatečná identifikace zdrojů rizik; nedostatečné modelování scénářů; žádné nebo nedostatečné postupy hodnocení rizik; nedostatečná kontrola kvality produktů; nedostatečný audit; nedostatečné úvahy o zdraví a bezpečnosti; nedostatečné plánování; absence řízení pro havarijní postupy; nepřiměřený výcvik; nepřiměřené informování o nehodě; nedostatečné vyšetření nehody.
9. Pracovní prostředí, tj. pracoviště a podmínky na pracovišti jako: stres, přetížení; špatné pracovní podmínky; nedostatečná ochrana; nedostatečná péče o zdraví pracovníků; neposkytnutí řádných pracovních podmínek; nedostatečné určení rizik; malý důraz na dodržování bezpečnostních opatření; slabá kontrola; špatná organizace práce; nedostatek zkušených pracovních sil; nedostatečné technické porozumění.
10. Výkon obsluhy, tj. provozní obsluha, inspektoři, údržba a další jako: nedostatečné výběrové řízení; nedostatečný počáteční výcvik a zácvik; nedostatečné fyzické a mentální předpoklady; nedostatečná motivace; nedostatek vzdělání a zkušeností; žádné nebo nedostatečné školení; nedostatečné hodnocení školení; nepřiměřené pracovní normy;

odchylky od pracovních postupů; nedostatečné bezpečnostní hranice; nízká úroveň bezpečnostních opatření.

Na základě výsledků šetření velkých průmyslových havárií, shrnutých v práci [1,10], lze konstatovat, že řada primárních (kauzálních) a sekundárních příčin se u nehod opakuje, ačkoliv existuje poměrně dost znalostí potřebných k prevenci nejen skoro nehod, ale i závažných havárií, popř. ke zmírnění jejich dopadů, a tím ke zmenšení ztrát a škod s nimi spojených. Příčinou daného stavu, kromě lidského činitele, jsou nedostatky jak v zavedení funkčního systému řízení bezpečnosti, tak i neznalost závěrů z již vyšetřovaných nehod a havárií.

Je skutečností, že i v organizacích, v kterých se vyskytly havárie, jsou s postupem času a změnami personálu původní opatření provedená po proběhlé havárii zapomenuta nebo nejsou předána všem pracovníkům v dané organizace. Proto je třeba znovu zdůraznit, že je třeba zavést následující opatření ke zlepšení společné paměti organizace:

1. Připojení poznámky ke každému pokynu, předpisu nebo normě, proč je právě takový.
2. Popis staré i nedávné havárie v podnikovém tisku s poučeními z nich vyplývající, a projednání na školeních o bezpečnosti pro všechny složky podniku.
3. Pravidelná kontrola dodržování vydaných opatření.
4. Odstranění existujících zařízení teprve po poznání, proč bylo instalováno. Rušení původního postupu po zjištění, proč byl přijat. Je to nutné, aby se neodstranilo něco, co má zabránit havárii nebo má zmírnit její dopady.
5. Zavedení lepšího informačního systému pro nalezení podrobností o haváriích a vydaných doporučeních po havárii.

Protože lidská selhání mohou mít původ v úmyslu [2], tak při řízení a vypořádání rizik je nezbytné v rámci procesní analýzy porozumět motivaci úmyslných činů nejen teroristů, ale i tzv. insiderů (vlastní zaměstnanci). Mezi motivy insiderů náleží například: nepraktické bezpečnostní postupy (vynechají se); nerealistické plány (použijí se osvědčená řešení bez ohledu na reálnou situaci); špatné vnímání bezpečnostních rizik; nedostatečná odpovědnost; a tlak a postoje managementu nebo finanční prospěch. Motivace insiderů přímo souvisí s kulturou bezpečnosti.

Kultura označuje specifické materiální a duchovní hodnoty, které lidé vytváří svou činností a kterými obohacují život svůj i život celé lidské společnosti. Kultura společnosti je celistvý systém významů, hodnot a společenských norem, kterými se řídí členové dané společnosti a které prostřednictvím sdílení předávají dalším generacím. Je to sbírka hodnot, symbolů, podnikových hrdinů, rituálů a vlastních dějin, které působí pod povrchem a mají velký vliv na jednání lidí na pracovních místech. Na základě právě uvedených definic pak 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 zájmů a jejich obnově a k nastartování jejich dalšího rozvoje. Podle některých autorů jde o soubor postojů, domněnek, norem a hodnot, které existují v dané entitě, který je odrazem toho, jak je podnik řízený, tj. jsou to všeobecné principy rozdělení pravomoci a odpovědnosti, zásady řízení a jistý poměr mezi důrazem na pracovní výsledky, autoritou, péčí o lidi, dodržování zásad bezpečnosti a zajištění funkčnosti dané entity.

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

Účinná kultura bezpečnosti je základním prvkem bezpečnosti organizace [1,2,27]. Odráží koncepci bezpečnosti a vychází z hodnot, stanovisek a jednání vrcholových řídících pracovníků organizace a z jejich komunikace se všemi zúčastněnými. Je zřetelným závazkem aktivně se podílet na řešení otázek bezpečnosti a prosazuje, aby všichni zúčastnění konali bezpečně a aby dodržovali příslušné právní předpisy, standardy a normy. Pravidla kultury bezpečnosti musí být zapracována do všech činností v organizaci. Jejich základem není koncentrace na potrestání viníků / původců chyb, ale poučení z chyb a zavedení takových nápravných opatření, aby se chyby nemohly opakovat nebo aby se alespoň výrazně snížila četnost jejich výskytu. Efektivním nástrojem pro její tvorbu je řízení bezpečnosti, které má fáze: prevence, připravenost zvládnout pohromy, odezva a obnova.

Základním principem je kvalifikované propojení řízení oblastí technické, organizační, finanční, personální, sociální, znalostní; jasné role a odpovědnosti všech zúčastněných. Systém řízení bezpečnosti organizace (SMS – Safety Management System) proto zahrnuje řadu oblastí, tj. technickou, vojenskou, legislativní, finanční, ekonomickou, sociální, ekologickou, vzdělávací, výzkumnou apod. [1,9,27]. Úkoly jednotlivých zúčastněných a jejich propojení v různých situacích stanoví právní předpisy, morální a jiné standardy a normy.

Zjednodušeně riziko je možné nebezpečí (tj. možný stav vzniku újmy) pro chráněné zájmy a důraz je na slovo „možné“, kdežto samotný výraz „nebezpečí“ označuje jistou aktuální újmu pro chráněné zájmy. Diskusi různých definic rizika lze najít v práci [5]. Abychom mohli stanovit riziko v daném místě pro každou selhání lidského faktoru, musíme udělat:

1. Stanovení možných zdrojů selhání lidského faktoru, která se může projevit dopady v daném místě.
2. Pro každý možný zdroj selhání lidského faktoru vypočítat ohrožení v daném místě.
3. Na základě zvolené hladiny věrohodnosti za specifikovaný časový interval stanovit v daném místě hodnotu ohrožení pro případ selhání lidského faktoru jako nejvyšší z hodnot určených v bodě 2.
4. Dle velikosti ohrožení pro případ selhání lidského faktoru provést stanovení souboru možných dopadů pro dané místo a celou entitu.
5. Analýza sledovaného místa a provedení šetření, jak soubor možných dopadů se projeví v daném místě s ohledem na místní zranitelnosti a příspěvky od možných náhodných jevů, do kterých patří např. specifické meteorologické situace, objekty, které mohou způsobit eskalaci dopadů (tzv. domino efekty), náhodná přítomnost nebezpečné látky apod.
6. Zpracování možných scénářů dopadů selhání lidského faktoru pro jednotlivé varianty situací, které v daném místě mohou nastat.
7. Určení pravděpodobnosti realizace jednotlivých scénářů dopadů selhání lidského faktoru ve sledovaném místě.
8. Pro každý nepřijatelný dopad selhání lidského faktoru v daném místě či variantu scénáře, který obsahuje nepřijatelný dopad určit pravděpodobnost výskytu při zohlednění pravděpodobnosti výskytu selhání lidského faktoru.
9. Metodou skórování [15] roztřídit rizika na přijatelná, nepřijatelná a podmíněně přijatelná, a k nim stanovit příslušná opatření [28] s cílem zajistit bezpečnou entitu.

Podle údajů v oborných pracích [28,363] selháním člověka v organizaci lze předejít, když:

- řízením odborných záležitostí jsou pověřováni jen odborníci se schopností vést pracovní kolektivy, kteří jdou příkladem, umí vysvětlit, podpořit, zabránit šikaně apod.),
- je zajištěna aplikace kvalifikovaného řízení procesů, které vytváří projekty a ty následně programy, jejichž výsledkem jsou produkty,
- jsou systematicky vytvářeny podmínky pro kvalifikovanou práci,
- je zajištěno dostatečné vzdělání pracovníků a systém poskytování výpomoci při řešení složitých úkolů,

- je prováděna motivace a stimulace pracovníků pro dodržování provozních a bezpečnostních předpisů,
- je prováděna důkladná kontrola procesů a jejich propojení do projektů a následně i programů.

Z výše uvedeného vyplývá, že organizační havárie vznikají v důsledku chybného řízení organizace. Nevznikají však jen v podnicích, ale také při řízení států či správních územních celků, kde se označují jako selhání vlády nebo selhání veřejné správy. Na základě odborného poznání je proto třeba zavádět v organizacích i ve správních celcích procesy řízení bezpečnosti, které svazují ostatní procesy a zavádět systémy řízení integrální bezpečnosti. V jejich rámci je třeba věnovat péči řízení lidských zdrojů, tj. procesům, které zajišťují kvalitní lidské zdroje [1,10].

Pro zvládnutí lidského faktoru je důležité aplikovat v každé entitě kompetentní řízení (tj. řízení integrální bezpečnosti) a zvládnutí rizik zaměřené na bezpečí a udržitelný rozvoj entity a lidského systému, kam každá entita patří, s tím, že je zváženo selhání lidského faktoru, a správně budovat kulturu bezpečnosti, která musí být respektována všemi zúčastněnými; přičemž hlavní odpovědnost mát top management.

Před průmyslovou revolucí byly nehody, havárie a neštěstí výsledkem živelních pohrom nebo několika, relativně dobře známých, jednoduchých technologických zařízení (např. vysokotlaké parní kotle). V 20. století vědecký a technologický pokrok zredukoval nebo eliminoval mnohá z tehdejších rizik. Na druhou stranu věda a technologie přinesla nová nebezpečí. Příkladem může být přítomnost nebezpečných chemických látek produkovaných antropogenními technologiemi v ovzduší nebo využívání radioaktivního záření, které zvýšilo potenciál pro úmrtí a choroby z ozáření.

Mnohá z nových nebezpečí jsou záludnější, hůře odhalitelná a odstranitelná, 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 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.

I když redundance (znásobení součástkových komponent pro ochranu před selháním obvodů měřící nebo regulační funkce - zálohování) poskytuje ochranu před haváriemi zapříčiněnými selháním individuálních částí, není stejně efektivní vůči nebezpečím, která vygenerují interakce mezi komponenty 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.

Mnohá z nových nebezpečí jsou svázaná se zvětšující se složitostí systémů, které se dnes budují. Složitost nejen vytváří nová nebezpečí, ale dělá je i hůře odhalitelnými. ***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.

V pracích [1,28,304-306,309-314] jsou shrnuty výsledky podrobných analýz expertů v případě havárií Flixbourgh (1. 4. 1974, Velká Británie), Seveso (10. 7. 1976, Itálie) a Bhópal (2. - 3. 12. 1984, Indie), pro které jsou v odborné literatuře dostupná fakta v dostatečné podrobnosti. Např. při analyzování tragédie v Bhópalu bylo konstatováno, že lidé nejsou úplně bezpeční před riziky, která přinášejí nebezpečné technologie a každý výběr nové technologie přináší s sebou možnost nejhoršího možného scénáře, který je třeba vzít v úvahu při každém

rozhodování o její realizaci a že lidé mají právo nejen přesně vědět, jaké jsou nejhorší scénáře, ale také se musí podílet na všech rozhodnutích, které přímo nebo nepřímo ovlivňují jejich budoucí zdraví a blahobyt. V mnoha případech je nutné přijmout fakt, že výsledkem využití uvedených kritérií může být rozhodnutí zabránit realizaci nebezpečné technologie nebo důkladně monitorovat rizika dle principu předběžné opatrnosti.

Studiem nehod provozovatelé mohou omezit nebezpečné nebo neproduktivní pracovní praktiky, a tím zvýšit kulturu bezpečnosti práce. Pozitivní zpětnou vazbu na vznik nehod mohou mít i audity řízení, audity bezpečnosti, audity nebezpečných dějů, chemických reakcí, zprávy o nehodách a skoro nehodách a monitoring dodržování všech opatření [1]. Existují 3 kategorie nebo „úrovně“ doporučení, a to:

1. Bezprostřední technická doporučení.
2. Doporučení pro zabránění nebezpečí.
3. Doporučení pro řízení zaměřená na primární příčiny nehod.

Bezprostřední technická doporučení jsou zaměřená na zabránění určitých nehod. Např. u odběru vzorků kapalného chlóru ve výrobně chlóru existuje určité nebezpečí úniku chlóru a následná inhalace plynného chlóru obsluhou při vzorkování chlóru. Příslušná doporučení jsou:

- změna techniky vzorkování,
- trénink správného odběru,
- použití ochranných pomůcek.

Doporučení pro zabránění (odvrácení) nebezpečí jsou zaměřená na odvrácení nepřijatelných nehod nebo alespoň jejich nepřijatelných dopadů. Např. se provede zlepšení běžných, oddělujících opatření umístěných mezi obsluhu a vlastní nebezpečí, tj. modifikace vzorkovací aparatury, vzorkováním v jiném místě nebo in-line analyzátorem, který odstraňuje potřebu ručního vzorkování.

Doporučení pro řízení zaměřené na primární příčiny nehody. Analýzou situace se identifikují nutné změny v systému řízení bezpečnosti, je-li ustaven nebo v jiných řídicích systémech. Vše je zaměřené nejen na prevenci dané nehody, ale i na jiné podobné nehody. Opatření takto koncipovaná jsou více důsledná a déle přetrvávající. V případě vzorkování chlóru to může být:

1. Zlepšení v metodách odběru vzorků. Sofistikovaně se odpoví na otázky: Kdo se účastní rozhodování? Jaká jsou kritéria pro stanovení místa odběru? Jaké jsou metody odběru a přístrojové vybavení? Kdo je oprávněn k odběru? Existuje periodický audit?, a odpovědi se zavedou do praxe.
2. Zlepšení v systému řízení pro zaváděcí, hodnotící a monitorovací standardní výrobní postupy. Sofistikovaně se odpoví na otázky: Jsou postupy adekvátní, srozumitelné a jsou důsledně prováděny? Je tento pracovní úkol stále nezbytný?, a odpovědi se zavedou do praxe.
3. Zavedení rutinního postupu jako je např. analýza bezpečnosti práce, ve které jsou úkoly systematicky posuzovány z hlediska potenciálního nebezpečí.

5.10.6. Zjištěné zdroje rizik v průmyslu

Na základě analýzy databáze nehod v průmyslových komplexech [12] je skutečností, že příčinou nehod v technologických objektech jsou:

- nesprávné provedení staveb (v zadávacích podmínkách není zohledněna dostatečným způsobem pohroma, která vyvolala havárii, ač, patří mezi specifické pohromy, tj. pohromy možné v předmětném území (s některými se vůbec nepočítalo),
- zadávací podmínky nejsou kompletní, zahrnují jen opatření do velikosti projektových pohrom a nepočítají s výskytem nadprojektových velikostí pohrom,
- chybí monitoring stavu staveb a zařízení a odpovídající systémy kontroly a řízení,

- chybí režim údržby a oprav, tj. neprovádí se kvalitní údržba a včasné opravy staveb, strojů a dalších zařízení s ohledem na stárnutí materiálů,
- chybí některé důležité pracovní postupy a zajištění jejich řádného provádění,
- nedostatečná kvalifikovanost pracovníků,
- nízká úroveň pracovní kázně,
- nízká kultura bezpečnosti.

Charakteristiky a dopady selhání technických objektů stabilních i mobilních, odvozené z údajů v databázi [12] jsou v tabulce 60.

Tabulka 60. Charakteristiky a dopady selhání technických objektů stabilních i mobilních.

Charakteristika	**Dopady**
Nehody a havárie v průmyslu	
- pravděpodobnost výskytu je vysoká a velikost dopadů havárie je často značná, - příčiny havárií v hlavních zařízeních průmyslových komplexů jsou početná a rozmanitá, - průmyslové komplexy se často nacházejí v blízkosti obytných zón, - sekvence událostí vedoucích k nehodě může být velmi rychlá a záchranné útvary se nemají čas organizovat; nebezpečné látky se rychle uvolňují a okamžitě ohrožují, - je často obtížné detekovat a analyzovat uvolněné látka a posoudit jejich dopady, - přestože podnik má vlastní složky odezvy, je často nutná pomoc od externích složek odezvy.	- vysoké a široké nebezpečí otravy lidí a zvířectva, - velké nebezpečí znečištění vod a půdy, - úroda může být zničena, - postižené území může být na určitý čas vyhlášeno jako “zakázaná zóna”.
Doprava a skladování nebezpečných látek	
- různá lokalizace místa vzniku nehody či havárie / mobilní zdroje rizik (kromě nádraží a překladišť), - uvolněné látky je obtížné identifikovat, - za účelem získání informací o vlastnostech látek, je třeba obstarat údaje od expertů, - mobilní ohrožení se týká přístavů, silnic, železnic, vnitrozemských vodních cest, obchodních center apod.	- velké a široké nebezpečí otravy lidí a zvířectva, - velké nebezpečí znečištění vod a půdy, - postižené území může být na určitý čas vyhlášeno jako “zakázaná zóna”
Dopravní nehody	
- velké nehody zpravidla vznikají v železniční a letecké dopravě, - možnost předběžného varování téměř neexistuje, tj. složky odezvy se nemohou včas zorganizovat, je vždy časová prodleva, - při odezvě jsou nutná speciální technická zařízení, - uvolňují se nebezpečné chemikálie, kouř apod.,	- velmi časté znečištění povrchové a podzemní vody, - znečištění ovzduší a ohrožení zdraví zúčastněných, - kontaminace půdy, - možné sekundární nebezpečí vzniku požáru a stavebních škod, - možný vysoký počet úmrtí a zranění.

- jde o mobilní zdroj nebezpečí - může nastat na mnoha místech.	

Analýzy příčin minulých havárií sledované v pracích [1,5,6,10,11,304-306,309-314,321-329] ukazují, že problematika je značně složitá a její řešení vyžaduje vysoký odborný nadhled a skutečnou snahu řešit problémy, a to jak v oblasti řízení, tak v oblasti inženýrských disciplín. Příčiny havárií jsou rozmanité a většinou jde o kombinaci několika příčin. Při vyšetřování havárií obvykle hledáme příčiny primární. Existují různé kategorie primárních příčin. V nich jsou určitá klíčová slova, která charakterizují určitou množinu jevů / stavů / provedení / atd., tzv. „před-podmínek“ pro selhání; tj. klíčová příčina havárie. Pro ukázku je uvedena tabulka 61, která uvádí ve sloupci „konkrétní příklady“ vždy pouze několik vybraných příkladů určitého zájmového okruhu.

Tabulka 61. Vybrané primární příčiny nehod, které vyústily v havárie a jejich příklady.

Kategorie primárních příčin havárií	**Původce příčiny havárie**	**Konkrétní příklady**
Vnější vlivy, které působí na technické dílo	Správní orgány	Důsledek nové legislativy Důsledek jednání externích inspektorů
	Průmyslové a obchodní subjekty	Nedostatečná podpora při řízení rizik od vedení společnosti Tlak od zákazníků Nedostatečné know-how
	Spolupráce s externími nouzovými službami	Nedostatečné vazby s vnějšími nouzovými službami Nedostatečné informace o toxicitě a způsobu léčení postižených chemickými látkami
	Veřejnost	Nátlakové skupiny Přehnaný místní stavební rozvoj Vývoj v životním prostředí
Kultura bezpečnosti v technickém díle (působení obchodních faktorů, kultury ve společnosti, přístupu vedení k bezpečnosti a technického know-how, které určují vnímání a očekávání jednotlivců uvnitř	Technické znalosti	Nedostatečné procesní a technologické know-how Nedostatečné průmyslové normy Chybějící nebo chybné postupy pro zvládání kritických podmínek
	Legislativa / předpisy	Změněné požadavky na umístění technického objektu (např. direktiva SEVESO v úplném znění požaduje při umísťování průmyslových objektů zpracovávajících nebezpečné látky stejné požadavky jako u jaderných elektráren [1,10,303], avšak české zákony, a to ani ten poslední č. 224/2015 Sb., o prevenci závažných havárií v platném znění požadavek zatím neobsahují) Záměrná porušení Pojišťovací požadavky Chybí bezpečnostní předpisy

technického díla)	Politické klima / nátlakové skupiny	Veřejné mínění Nekorektní práce s riziky (např. šíření nesprávných oceňování dopadů technických děl na okolí; šíření falešných zpráv)
	Ekonomické klima / obchodní faktory	Nedostatek personálu a zařízení Nedostatek nároků na výrobky Nedostatečná výrobní kapacita a velké požadavky na produkci
	Obchodní zaměření	Chybné rozmístění výrobních zdrojů a špatná dostupnost technických děl Chybná investiční strategie technického díla Umístění technického díla do méně obydlených nebo méně bezpečných oblastí
	Kultura společnosti	Zájem pouze o zisk Nedostatečné zkušenosti s provozem technického díla Sociální postoje / chování vedení společnosti k zaměstnancům
	Kultura bezpečnosti	Špatný přístup managementu k bezpečnosti Nízké povědomí vedení společnosti o rizicích
Organizace a řízení technického díla (způsob řešení problémů)	Posloupnost rozhodování	Nedostatečná úroveň strategie řízení bezpečnosti Chybí proces řízení bezpečnosti Nedostatečně stanovené pracovní priority Chybí oddělení pro řízení bezpečnosti
	Závazek k bezpečnosti	Není dokument o bezpečnostní politice Jsou nejasné směrnice pro řízení bezpečnosti a řízení rizik
	Interakce s interními/externími systémy	Nedostatečná organizační rozhraní Nevyjasněné vztahy mezi skupinami ve výrobě; výrova vs. administrativa; výroba vs. IT Nedostatečná komunikace mezi vedením a zaměstnanci
	Kvalita zajištění základny	Nedostatečné projekční a inženýrské zabezpečení Špatné umístění zařízení – nesplněny požadavky ergonomie Nedostatečná analýza a hodnocení rizik
	Výrobní zdroje	Nedostatečné finance Nedostatečná výrobní kapacita Nedostatečná úroveň obsluhy po odborné stránce Chybný režim údržby (příliš dlouhé intervaly) Chybí režim včasných oprav důležitých zařízení Nedostatečně určené odpovědnosti

Umístění objektů a výrobních zařízení technického díla (vztahuje se k projektu a jeho realizaci)	Umístění zařízení a jeho projekt	Chybné určení bezpečnostních zón a oddělení zařízení, která se mohou vzájemně ovlivnit (selhání v důsledku těsného spojení) Nedostatečná úroveň zařízení pro nouzovou odezvu Nedostatečná ochrana technického díla před vnějšími pohromami a jejich riziky
	Inženýrství a výrobní projekt	Nedostatečná dokumentace technického díla Nedostatečné určení požadavků na provoz při abnormálních a kritických podmínkách Nedostatečná předběžná analýza rizik od všech možných zdrojů havárií a selhání Nedostatečné určení prioritních rizik (tj. nerespektování zásad TQM [46]).
	Zadání a realizace zařízení	Chybné nebo nedostatečné zadávací podmínky Chyby v provedení stavby Chyby v montáži zařízení podle projektu Chyby v řízení prací stavby a konstrukce
	Doprava, skladování, zpracovávání materiálu, odpad materiálu	Nevhodný způsob dopravy materiálu Nevhodné skladování nebo skladování ve velkých objemech (což je nebezpečné u vysoce nebezpečných látek) Použití nevhodných materiálů
Integrita technického díla (provázání bezpečnosti, spolehlivosti a funkčnosti zařízení během životnosti - projekt, stavba, provoz, údržba a řízení, dozor)	Bezpečnost provozu	Neexistuje program zvyšování bezpečnosti technického díla [1,10,315] Nejsou jasné limity a podmínky provozu technického díla Nejsou podmínky provozu za abnormálních a kritických podmínek Nejsou postupy pro zvládnutí kritických podmínek zacílené na zachování provozuschopnosti technického díla po opravě Chybí plán kontinuity technického díla pro případ výskytu extrémních podmínek
	Kvalita zařízení	Nedostatečný projekt nebo nedostatečná specifikace údržby, včasných oprav a oprav po poruchách Nedostatečná kontrola technického stavu Používání nevhodných nástrojů, materiálů a zařízení
	Použitelnost, dostupnost	Nedostatečná výrobní pohotovost Nedostatečná dokumentace provozu Nepřiměřené prodloužení životnosti zařízení
	Údržba	Nedostatečná preventivní údržba Nekvalifikovaně a nedostatečně prováděné opravy

	Vylepšení zařízení / modifikace	Nevhodná modifikace zařízení Nedostatečné řešení změn Použití zastaralých postupů
	Standardy, normy	Nevhodné standardy a normy Nevhodné specifikace a/nebo projektová kritéria
Oblast řízení technického díla orientovaná na jeho bezpečnost (celkovou / integrální)	Umístění zdrojů a vývoj	Chybějící kapitál Chybějící personál nebo čas Nepřiměřené plánování a kontrola zdrojů Chybí vlastní výzkumná základna nebo alespoň spolupráce s výzkumnou základnou
	Monitoring, kontrola kvality a audit	Chybí monitoring rizik Chybí pravidelná kontrola řízení prioritních rizik Chybí seznam nápravných opatření nebo jejich zajištění (kdo, co, jak, čím provede) Nedostatečná provozní opatření Nedostatečné provádění nápravných opatření
	Řízení změn	Nedostatečná odezva na změnu Nekompetentní změna v technologii, zařízení nebo postupech prací Provádění změn bez ohledu na minulé zkušenosti (odstraní se něco, co plnilo ochranu před možným vysoce nežádoucím jevem)
	Kompetence / způsobilost managementu	Nedostatečné odborné znalosti vedení a kritického personálu Chyba ve vnímání rizik nebo vnímání různých podmínek při provozu Nedostatečný výcvik zacílený na bezpečnost osob a bezpečnost zařízení nebo technické znalosti
	Odpovědnost	Chybí konkrétní rozdělení odpovědnosti Řízení rizika na příliš nízké úrovni
	Dohled a kontrola	Nesprávné příkazy a delegování pravomocí Nedostatečná kontrola pracovní atmosféry a pracovních praktik
	Odpovědnost za bezpečnost	Nejasné nebo konfliktní stanovení odpovědností Zanedbávání bezpečnostních faktorů Chybí přehled o bezpečných postupech a jejich zavádění do praxe
	Kvalita obsluhy zařízení za normálních, abnormálních a kritických podmínek	Chybí nouzové plánování Špatná koordinace odezvy na havárie a selhání uvnitř nebo v okolí zařízení

Komunikace a informace, které jsou životně důležité pro bezpečný provoz technického díla	Kvalita informací	Nedostatečná verbální komunikace mezi managementem a zaměstnanci Nedostatek informací Šíření chybných informací o zařízení a rizicích spojených s výrobními procesy Utajování informací o možných rizicích Utajování informací o nehodách
	Bezpečnostní informace	Nedostatečné informace o materiálu a o dopadech při jeho používání Nedostatečné modelování scénářů havárií Nedostatečná bezpečnostní dokumentace Chybí plány odezvy
	Informační kanály	Absence informačních kanálů Nedostatečný monitoring a sběr dat
	Média	Nedostatečné informování Nesprávná odezva na informace
	Kvalita odezvy a informování v případě havárie	Není centrum pro řízení havárií Nevhodně zvolené řídící centrum pro odezvu na havárie Nedostatečné znalosti modelů úniků nebezpečných látek Nedostatečné postupy odezvy
	Komunikace v případě havárie	Absence informačních kanálů o haváriích Nedostatečná kapacita zařízení pro šíření informací o haváriích
Postupy a praxe (jasné postupy pro bezpečný způsob nakládání s nebezpečnými látkami, výrobní postupy a operace)	Pracovní postupy a praktiky	Nedostatečné provozní / údržbářské postupy Nedostatečná pracovní disciplína
	Bezpečnostní studie	Nedostatečná identifikace zdrojů rizik Nedostatečné modelování scénářů Žádné nebo nedostatečné postupy pro hodnocení rizik (chybí stupnice nebo jsou používány subjektivní stupnice)
	Kontrola kvality	Nedostatečná kontrola kvality produktů Nedostatečný audit výrobků Nedostatečné úvahy o zdraví a bezpečnosti
	Provozní postupy pro abnormální a kritické situace	Nedostatečné plánování postupů při podmínkách jiných než normálních Chybí jasné řízení odezvy na nouzové situace Nepřiměřený výcvik zaměstnanců a řídících pracovníků pro případ odezvy na nouzové situace Chybí zavedení poučení ze zkušeností z havárií v daném díle nebo v díle podobném
	Informování o nehodě	Nepřiměřené informování o nehodě Nedostatečné vyšetření nehody Neoznámení poučení z nehody

Pracovní prostředí (pracoviště a podmínky na pracovišti)	Pracovní prostředí	Stres, přetížení Špatné pracovní podmínky Nedostatečná ochrana pracovníků Šikana na pracovišti
	Péče o pracující	Nedostatečná péče o zdraví a bezpečí pracovníků Nezajištění řádných pracovních podmínek
	Kultura bezpečnosti	Nedostatečná práce s riziky Malý důraz na dodržování bezpečnostních opatření
	Bezprostřední dozor a podpora	Slabá kontrola Špatná organizace práce Nedostatek zkušených pracovních sil Nedostatečné technické porozumění úkolům
Výkon obsluhy (provozní obsluha, inspektoři, údržba a další)	Přijímání do pracovního poměru	Nedostatečné výběrové řízení Nedostatečný počáteční výcvik a zácvik
	Osobní vlastnosti	Nedostatečné fyzické a mentální předpoklady zaměstnance pro práci Nedostatečná motivace zaměstnance ke kvalitní práci Nedostatek vzdělání a zkušeností zaměstnance
	Školení	Žádné nebo nedostatečné školení zaměstnanců Nekvalitní školení zaměstnanců
	Pracovní disciplína	Nepřiměřené pracovní normy Povolované nebo vynucované odchylky od pracovních postupů
	Bezpečnostní a provozní hranice (tolerance)	Nedostatečné bezpečnostní hranice Nízká úroveň bezpečnostních opatření

Z tabulky 61 vyplývá velká rozmanitost příčin poruch a nehod, které vyústily v havárie. Kromě pochopitelných příčin jako jsou živelní pohromy a technické problémy jsou zdroji rizik i chybné zásahy správních orgánů, chybné předpisy, politická situace a aktivity politiků zacílené na získání volebních preferencí, situace na trhu a nátlakové skupiny.

5.10.7. Opatření pro zvyšování bezpečnosti výrobních technických děl

Základním principem řízení bezpečnosti technologických objektů, které zajistí prevenci havárií, a když již havárie vznikne, tak její kvalifikované zvládnutí, je kvalifikované propojení oblastí technické, organizační, finanční, personální, sociální, znalostní; a jasné role a povinnosti všech zúčastněných. Systém řízení bezpečnosti kritických zařízení, tedy pokrývá řadu oblastí, a to technickou, vojenskou, legislativní, finanční, ekonomickou, sociální, ekologickou, vzdělávací, výzkumnou, atd. Úkoly v oblasti bezpečnosti, na základě současných znalosti a současného pojetí důmyslných bezpečnostních systémů, mají všichni účastníci. Úkoly jednotlivých zúčastněných a jejich propojení v různých situacích musí být stanoveny zákony, morální a dalších standardů a norem.

Po zkušenostech s dopady velkých technologických havárií je dnes pro každý objekt nebo území důležité, aby tvořily bezpečný systém, tj. aby nebyl ohrožen ani zevnitř, ani zvenku a aby neohrožoval své okolí. Moderní typ řízení, který se k uvedenému cíli používá, je procesní

řízení, které je strategické, systémové a proaktivní a je zaměřené na bezpečnost. Pro jeho implementaci je velmi důležité pochopení příčin možných havárií a instalace specifických opatření a činností, které zajistí kvalitní prevenci a v případě vzniku havárie kvalitní a rychlou odezvu, která zmírní dopady a sníží újmy na chráněných aktivech veřejných i vlastníka objektu.

Provedená analýza havárií a selhání technických děl ukazuje, že obvykle jejich příčiny nejsou jednoduché, obvykle jde o souběh celé řady příčin a popřípadě náhodných kombinací příčin. Postup pro určení mnohonásobných příčin vychází z cíle vyšetřování nehody, kterým je zabránit opakování nehody tím, že:

- identifikujeme a oceníme příčiny (primární příčiny a přispívající příčiny),
- identifikujeme a oceníme doporučená preventivní opatření, která redukují pravděpodobnost vzniku nehod a / nebo dopady nehod,
- zajistíme efektivní provádění a sledování všech doporučených opatření.

Scénář postupu je následující:

1. Shromažďování důkazů.
2. Určení chronologického vývoje událostí.
3. Seznam faktů.
4. Vytvoření logického stromu událostí.
5. Přezkoumání a potvrzení úplnosti logického stromu procesu při srovnání s fakty, které se získáme z odpovědí na otázky:
   Je logický strom úplný?
   Jsou identifikované příčiny systémové příčiny?
   Je celkový přehled výsledků v souladu s logickými pravidly?
   Byly uváženy všechny informace?

Pokud jsou odpovědi na všechny otázky ANO, tak se zpracují doporučení na zvýšení bezpečnosti s ohledem na mnohonásobné příčiny.

Shrnutí

Při řízení a vypořádání rizik organizačních procesů spojených s technickým dílem jde vlastně o řízení a vypořádání rizik čtyř podprocesů, a to: projekce a konstrukce, výstavba, provoz a údržba. Uvedené podprocesy jsou zabudovány ve třech provázaných činnostech: stanovení cílů v rámci hospodářské a sociální situace podniku; organizace podniku pro splnění stanovených dlouhodobých strategických cílů; a řízení provozních činností. Každý z uvedených podprocesů a činností má své zdroje rizik vedoucí k jeho selhání, např.:

1. Stanovení cílů – vyskytnou se neslučitelné cíle.
2. Organizace – jsou zavedeny nepřiměřené struktury.
3. Řízení - je špatná komunikace mezi zúčastněnými, špatné plánování, nepřiměřená kontrola a sledování.
4. Projekce a konstrukce - chybná projekce, neodpovídající zábrany.
5. Výstavba: k dispozici jsou nevhodné materiály, neodpovídající podmínky.
6. Provoz: špatné provozní postupy, špatné školení a vzdělávání.
7. Údržba: špatný rozvrh údržby, špatné postupy údržby.

Předmětným rizikům je třeba věnovat péči.

Ze všech údajů dříve uvedených vyplývá, že při řízení a vypořádání rizik spojených s podmínkami, které působí vznik chyb nebo porušení předpisů je třeba zvažovat dopady na bezpečnost, když dojde k: nedostatku času; neporozumění mezi konstruktérem a uživatelem; výskytu nevratných chyb; zahlcení informacemi; špatnému předání úkolů; špatnému vnímání (podcenění) rizika, špatné zpětné vazbě; zaměstnání nezkušeného personálu; výskytu špatných pokynů a postupů; nedostatečné kontrole; pověření provedení úkolu osobě s neodpovídajícím vzdělání; výskytu nepřátelství mezi osobami, které musí spolupracovat; potřebě vykonat monotónní a nudnou práci.

Při řízení a vypořádání rizik, které jsou zdrojem chyb, anebo porušením předpisů je třeba řešit: kulturu bezpečnosti v organizaci; rozpory mezi řídícími pracovníky a zaměstnanci; morálku vedoucích pracovníků i zaměstnanců; dohled a kontrolu; normy tolerující porušování předpisů; vnímání zdrojů rizik; postřehnutelný nedostatek péče a zájmu vedoucích pracovníků; hrdost pracovníků na vlastní práci; způsob odstranění machrovského přístupu k práci, který povzbuzuje podstupování rizik; odstranění přesvědčení, že se nemůže nic špatného stát; otázky sebeúcty a vzájemné úcty zaměstnanců; sebevědomí klíčových pracovníků, a to hlavně po haváriích; postřehnutelné povolení pro porušování pravidel; odstranění obojakých, dvojsmyslných nebo zjevně nesmyslných pravidel.

Nebezpečné konání se dá rozdělit na chyby a porušení předpisů / pravidel:

1. Chyby se dějí jako důsledek problémů v informačních procesech a dají se pochopit ve vztahu k poznávacím funkcím jednotlivce. Dají se minimalizovat školením, zlepšením pracovišť, rozhraní, lepším informováním atd.
2. Porušení předpisů / pravidel jsou založeny na motivaci. Jsou společenským jevem a dají se pochopit jen v souvislostech dané organizace. Porušení se musí odstranit změnou přístupů, přesvědčení, norem, morálky a kultury bezpečnosti.

Další podrobnosti lze najít v práci [28] a v pracích, které jsou v ní citované.

5.10.8. Výsledky šetření úrovně řízení havárií spojených s technickými díly v EU

Šetření úrovně řízení havárií spojených s technologiemi a infrastrukturami v EU bylo provedeno v rámci projektu FOCUS [19] a použita data z odborné oblasti, která jsou citována na příslušných místech a data o legislativě a řídících mechanismech v EU [7]; např. SEVESO, REACH aj. Ve vlastním výzkumu byly zváženy pohromy, které se vztahují ke sledované oblasti, a to nehody, havárie, selhání infrastruktur, selhání technologií, ztráty obslužnosti apod. Metoda šetření spočívala v expertním vyhodnocení dotazníku, který byl sestaven pro projekt FOCUS [7,19] a byl zacílen na zjištění nedostatků v řízení EU a členských zemí s ohledem řízení pohrom (Disaster Management), které je základem pro budování bezpečné EU s udržitelným rozvojem.

Dotazník byl vyhodnocen 25 experty s vysokoškolským vzděláním a s praktickými zkušenostmi (příslušníci bezpečnostních složek, bezpečnostní manažeři v průmyslu a veřejných organizacích, inženýři z průmyslu, inspektoři BOZP, pracovníci veřejné správy, akademičtí pracovníci, právníci, ekonomové a jeden politolog). Celkové vyhodnocení úrovně řízení pohrom spojených s technologiemi a infrastrukturami v EU provedené 5 experty ČVUT je uvedeno v tabulce 62.

Tabulka 62. Výsledky posouzení úrovně řízení pohrom spojených s technologiemi a infrastrukturami

Otázka	**Odpověď + její průkaz**
Obsahuje seznam sledovaných pohrom uvedený výše všechny pohromy možné na území EU?	Je třeba doplnit zneužití technologií (jaderných, nano i IT), zneužití genetického inženýrství a zneužití látek CBRNE.
Které ze sledovaných pohrom jsou pro území EU nejhorší? Udělejte pořadí dle vašich znalostí a zkušeností.	1. Nadprojektová havárie s přítomností radioaktivních látek. 2. Nadprojektová havárie s přítomností nebezpečných látek mutagenních, karcinogenních a nebezpečných pro reprodukci.

	3. Dlouhodobý výpadek elektrické infrastruktury. 4. Dlouhodobý výpadek dodávek pitné vody. 5. Dlouhodobý nedostatek základních potravin.
Pro které sledované pohromy není systematicky prováděna prevence? Je úroveň prevence dostatečná? Jaká je situace ve vaší zemi? Co je třeba zlepšit?	Prevenci jaderných havárií i připravenost na jejich zvládnutí je třeba zlepšit na základě poučení z havárie jaderné elektrárny Fukushima [364]. Jistá zlepšení je třeba provést v oblasti řízení bezpečnosti i u dalších technologií v EU i v ČR. Pozornost je třeba věnovat transportu nebezpečných látek, a to především technickým otázkám, Je třeba zavést normy a standardy pro infrastruktury, které zajistí jejich kapacitu, robustnost a posílí jejich odolnost. V EU i v ČR chybí robustní opatření zabraňující zneužití technologií.
Pro které sledované pohromy není v EU systematicky zajišťována připravenost? Je úroveň připravenosti dostatečná? Je připravenost prováděna všemi složkami společnosti (včetně veřejnosti) dostatečná? Jaká je situace ve vaší zemi? Co je třeba zlepšit?	Na základě poučení z Fukushimy [364] zcela chybí připravenost na nouzové situace, které nastanou, když selžou bezpečnostní systémy [12].
Pro které sledované pohromy nemá EU systematicky připravenou kvalifikovanou odezvu? Je úroveň této odezvy dostatečná? Jaká je situace ve vaší zemi? Co je třeba zlepšit?	EU nemá zajištěn systém odezvy. Členské státy mají systémy odezvy různé; jsou určené národní legislativou. V ČR jsou funkční systémy odezvy zajišťované IZS a hygienickou službou. V ostatních oblastech jako je finanční sektor, sektor správného řízení věcí veřejných apod. úroveň systémů je nízká.
Pro které sledované pohromy nemá EU systematicky připravenou kvalifikovanou obnovu? Je úroveň této obnovy dostatečná? Jaká je situace ve vaší zemi? Co je třeba zlepšit?	EU nemá vlastní systém obnovy. Poskytuje finanční výpomoc v případě vybraných pohrom, jestliže jsou splněny požadavky specifického právního předpisu. ČR má zákon č. 12/2002 Sb., který upravuje obnovu po živelních a jiných pohromách, ale plán obnovy, který specifikuje zásady a postupy obnovy (jako má třeba FEMA [80,365,366]) nemá.
Která sledovaná pohroma může způsobit kritické situace v EU? Která sledovaná pohroma může způsobit kritické situace ve vaší zemi?	Nadprojektová jaderná havárie. Dlouhodobý výpadek elektrické energie. Dlouhodobý výpadek dodávek pitné vody. Dlouhodobý výpadek dodávek potravin. Dlouhodobé selhání finanční infrastruktury.
Která sledovaná pohroma může způsobit krizové situace v EU?	Masivní selhání finančního trhu. Nadprojektová jaderná havárie.

Která sledovaná pohroma může způsobit krizové situace ve vaší zemi?	Dlouhodobý výpadek elektrické energie. Dlouhodobý výpadek dodávek pitné vody. Dlouhodobý výpadek dodávek potravin.
Pro které krizové situace v EU není úroveň krizového řízení dostatečná? Pro které krizové situace ve vaší zemi není úroveň krizového řízení dostatečná?	Nedostatky se projeví ve všech krizových situacích, kdy bude třeba aplikovat strategické, systémové a proaktivní řízení, protože současné krizové řízení uvedené parametry nemá.
Které zranitelnosti lidské společnosti v EU mohou způsobit změnu kritické situace na extrémní situaci? Které zranitelnosti lidské společnosti ve vaší zemi mohou způsobit změnu kritické situace na extrémní situaci?	Nedostatek technických prostředků, nedostatečné znalosti a výcvik řídících pracovníků, špatné řízení odezvy a nedostatek financí.
Máme spolehlivé metody pro určení scénářů všech sledovaných pohrom očekávaných v EU? Máme spolehlivé metody pro určení scénářů všech sledovaných pohrom očekávaných ve vaší zemi?	Metody používané v EU, členských zemích EU i v ČR jsou založené na deterministických a stochastických přístupech a na předpokladu, že každý systém je stále ve stacionárním stavu nebo blízko něho [1,10,11]. Poučení z Fukushimy [80] ukazuje, že je třeba vylepšit metody spojené se stanovením zadávacích podmínek pro projekt, výstavbu i provoz technologických objektů a infrastruktur.
Známe pro všechny sledované pohromy v příloze úspěšná opatření a činnosti pro prevenci, zmírnění, odezvu a obnovu? Jaké slabiny jsou ve znalostech o opatřeních a činnostech pro prevenci, zmírnění, odezvu a obnovu?	Teoreticky jsou opatření a činnosti pro prevenci, zmírnění, odezvu a obnovu známé [2,365,366]. Konkrétní opatření a činnosti jsou místně specifické. Jejich určení je provedeno jen pro případ důležitých objektů.
Co je nutné vylepšit?	Systém řízení území a objektů.
Jaký výzkum je nejefektivnější pro zlepšení řízení bezpečnosti v EU? Jaký výzkum je nejefektivnější pro zlepšení řízení bezpečnosti ve vaší zemi?	Řízení integrálního rizika. Dosud aplikované postupy nezvažují průřezová rizika, která jsou příčinou kaskádovitých selhání složených systémů.
Jaké principy, legislativa a pravidla spolupráce v EU jsou nutné pro bezpečí a udržitelný rozvoj lidí?	Respektování zásad pro řízení integrální bezpečnosti [2].
Můžete navrhnout opatření pro odvrácení sociálních krizí v EU?	Respektování veřejného zájmu a zásad pro řízení integrální bezpečnosti [2].

Na základě údajů v tabulce 62 je posouzena úroveň řízení věcí veřejných EU z pohledu řízení havárií spojených s technologiemi a infrastrukturami. Na základě posouzení jsou identifikovány základní nedostatky spojené s řízením sledovaných pohrom a jsou identifikovány oblasti, ve kterých je třeba přijmout opatření (tabulka 63). Z výsledku vyplývá, že nedostatků je mnoho. Je to způsobeno tím, že v současném řízení pohrom všeho druhu chybí zacílení na prioritní problémy.

Tabulka 63. Návrh oblastí řešení identifikovaných nedostatků. Tučně jsou vyznačeny oblasti, které jsou zvláště důležité pro řešení uvedených nedostatků. Ve sloupci „jiné“ M označuje nutnost monitoringu a K nutnost sestavit plán kontinuity a přežití lidí.

Pohroma	**Seznam nedostatků**	**Typ opatření a činností na odstranění nedostatků**				
		legislativa	**specifické řízení**	**výzkum**	**vzdělání**	**jiné**
Ztráta obslužnosti území (selhání některé z infrastruktur)	Chybí koncept pro vytvoření jak robustní kritické infrastruktury, tak robustních dílčích infrastruktur; zvláště pak kybernetické infrastruktury.	**Ano**	**Ano**	**Ano**	**Ano**	**K**
Nadprojektová havárie s přítomností radioaktivních látek	Řízení bezpečnosti vychází z předpokladu, že vícenásobně zálohované bezpečnostní systémy zajistí bezpečnost vždy. Poučení z Fukushimy [363] však ukazuje, že předpoklad není oprávněný.	**Ano**	**Ano**	Ano	Ano	**K**
Nadprojektová havárie s přítomností nebezpečných látek mutagenních, karcinogenních	Řízení bezpečnosti založené na řízení integrální bezpečnosti je vyžadováno jen ve specifikovaných případech.	**Ano**	**Ano**	Ano	Ano	**K**
Zneužití látek CBRNE	Chybí účinný systém řízení nakládání s látkami CBRNE.	**Ano**	**Ano**	Ano	Ano	M
Zneužití nanotechnologií	Neřeší se.	**Ano**	**Ano**	**Ano**	**Ano**	M
Zneužití genetického inženýrství	Neřeší se.	**Ano**	**Ano**	**Ano**	**Ano**	**M**
Zneužití IT technologií	Neřeší se.	**Ano**	**Ano**	**Ano**	**Ano**	**M**

Z tabulky 63 vyplývá, že řada existujících nedostatků není řešena ani v jedné důležité oblasti.

Na základě analýzy nástrojů EU pro řízení věcí veřejných je posouzena úroveň řízení pohrom spojených s technologiemi a infrastrukturami. Vysoce byla oceněna tvorba databáze MARS, která vytváří základnu pro tvorbu vysoce kvalifikovaných podkladů pro řízení bezpečnosti. Na základě šetření založeného na specifickém kontrolním seznamu jsou identifikovány základní nedostatky spojené s řízením sledovaných pohrom a jsou

identifikovány oblasti, ve kterých je třeba přijmout opatření. Z výsledku vyplývá, že nedostatků je mnoho. Je to způsobeno tím, že v řízení chybí zacílení na prioritní problémy.

Nutné je, aby se řízení rizik a s ním spojené odpovědnosti skutečně zavedly do praxe (tak, jak je např. v ČR uloženo zákonem č. 262/2006 Sb.) a byly integrální součástí všech procesů v organizaci, včetně strategického plánování a všech procesů spojených s řízením projektů a změn. Je třeba upravit i požadavky na množství komodit, které skutečně zajistí přežití lidí, např. zabezpečení dodávek ropy a zemního plynu se upravuje na základě výpočtu přidané hodnoty projektu z hlediska krátkodobé a dlouhodobé odolnosti systému a zvýšení zbývající flexibility systému umožňující vyrovnat se s narušením dodávek podle různých scénářů a další kapacity získané v rámci projektu stanovené ve vztahu ke standardu pro infrastrukturu (pravidlo N-1) [367].

K tomu je však nezbytné kvalitní zázemí, které by měl připravit výzkum. Bez kvalitního zázemí budou řešeny jen momentální kritické situace, což obvykle vede k nerovnoměrnému čerpání zdrojů, sil a prostředků.

5.10.9. Nástroj pro bezpečnostní audit v technickém díle

Archiv [12] obsahuje řadu kontrolních seznamů, které jsou zacílené na identifikaci rizik a hodnocení rizik; např. pro chemické a fyzikální laboratoře, provoz souboru zařízení, postup odezvy aj. Dále ukážeme příklad použití nástrojů rizikového inženýrství ve strojírenství, a to pro ocenění rizik při testu tlumení nárazu podvozku letounu v okamžiku přistání. Výsledek testu ukazuje, zda testované přistávací zařízení je či není bezpečný výrobek. Výsledek je důležitý pro bezpečnost letového provozu a hlavně pro lidi, které k přepravě letadla používají.

Bezpečnosti leteckého provozu je v jednotlivých zemích i na mezinárodní úrovni věnována značná pozornost, neboť případné selhání techniky nebo lidského faktoru v předmětné oblasti může vést jak k velkým materiálním škodám, tak ke ztrátám na životech a zdraví značného počtu lidi. Proto jsou všechny činnosti související s leteckým provozem celosvětově poměrně přísně regulovány. Většina zemí má pro danou oblast vytvořen soubor zákonů, směrnic a standardů, které usměrňují všechny činnosti s touto oblasti související.

Speciální místo v souborech dokumentů mají předpisy stanovující technické požadavky na konstrukci letecké techniky a zejména požadavky na její bezpečnost. Dokumenty mají zpravidla závazný charakter a každý výrobce, který chce leteckou techniku vyrábět, je musí akceptovat a jejich dodržení stanoveným způsobem prokazovat [368]. Znalost příslušných dokumentů a požadavků, které jsou v nich specifikovány, je nevyhnutným předpokladem pro úspěšnou realizaci předvýrobních (vývojových) etap u každého výrobků leteckého průmyslu. Testování letadel a jeho jednotlivých částí je dnes rozsáhlým vědním oborem, který souvisí s rychlým rozvojem letectví. Jednou z nejdůležitějších částí letadla je přistávací zařízení, které je zejména při přistání vystaveno značnému zatížení. Letecká názvoslovná norma ČSN 31 0001 definuje pojem „Přistávací zařízení“ jako část letadla umožňující vzlet, přistání, popř. pojíždění. Podvozek je v dané normě definován jako základní konstrukční skupina přistávacího zařízení [368]. Jeho porušení může mít za následek poškození až zničení celého letadla, včetně ohrožení bezpečnosti cestujících. Z uvedených a mnoha dalších důvodů se od přistávacího zařízení požaduje velká bezpečnost a vysoká spolehlivost po celou dobu životnosti letounu, která u některých letounů může znamenat až desítky tisíc vzletů a přistání. Proto je potřeba jak při návrhu nového přistávacího zařízení, tak i při jeho pravidelných kontrolách a revizích věnovat patřičnou pozornost bezpečnosti, a to hlavně řízení jednotlivých rizik vyplývajících z konstrukce, funkce a způsobu řízení, montáže a údržby. Musí být provedena taková opatření, aby se závažná rizika eliminovala nebo snížila na úroveň, která je akceptovatelná.

Jedno z prvních skutečných přistávacích zařízení na letadlech (jednoduchý a spolehlivý tříbodový podvozek, často s příďovým kolem) bylo použito v roce 1903, kdy byl k pohonu

letounu použit spalovací motor. Do té doby byly používány většinou lyže a starty byly realizovány z kolejnic za pomoci katapultu (bratři Wrightové). V průběhu 1. světové války se z důvodu vpředu umístěné vrtule velkého průměru ustálila koncepce dvoukolového hlavního podvozku a jednoduché ostruhy v zadní části letadla. Tlumení přistávacího rázu bylo řešeno pomoci gumového lana omotaného kolem osy hlavního podvozku a podvozkové nohy [368].

S rostoucí rychlostí letadel ve 20. letech 20. století se začínají vyrábět první zatahovací podvozky, které měly snížit aerodynamický odpor letounu. Koncem 2. světové války se začaly vyrábět první letouny vybavené reaktivním pohonem a při stále se zvyšujících rychlostech se začal opět používat podvozek s příďovým kolem, který usnadnil vzlet a hlavně přistání. I když konstrukce letadel od této doby prošla celou řadou změn, tak k žádným výrazným změnám v koncepci podvozků nedošlo. Podvozky s ostruhou lze vidět na některých amatérských konstrukcích a na moderních letounech stavěných speciálně pro leteckou akrobacii [368].

Speciální místo v souborech dokumentů zajišťujících bezpečnost letectví mají předpisy stanovující technické požadavky na konstrukci letecké techniky a zejména požadavky na bezpečnost a spolehlivost letecké techniky po celou dobu životnosti. Předmětné dokumenty mají zpravidla závazný charakter a každý výrobce, který chce leteckou techniku vyrábět, je musí akceptovat a jejich dodržení stanoveným způsobem prokazovat. Znalost příslušných dokumentů a požadavků, které jsou v nich specifikovány, je tedy nevyhnutelným předpokladem pro úspěšnou realizaci předvýrobních (vývojových) etap u každého výrobků leteckého průmyslu.

Testování letadel a jeho jednotlivých částí je dnes rozsáhlým vědním oborem, který souvisí s rychlým rozvojem letectví. Jednou z nejdůležitějších částí letadla je přistávací zařízení, které je zejména při přistání vystaveno značnému zatížení. Jak již bylo uvedeno, jeho porušení může mít za následek poškození až zničení celého letadla, včetně ohrožení bezpečí cestujících. Z těchto a mnoha dalších důvodů se od přistávacího zařízení požaduje vysoká bezpečnost a spolehlivost po celou dobu životnosti letounu, která u některých letounů může znamenat až desítky tisíc vzletů a přistání [369]. Proto je potřeba jak při návrhu nového přistávacího zařízení, tak i při jeho pravidelných kontrolách a revizích věnovat patřičnou pozornost bezpečnosti, včetně posouzení jednotlivých rizik vyplývajících z konstrukce, funkce a způsobu řízení, montáže a údržby. Musí být provedena taková opatření, aby se různá rizika eliminovala nebo snížila na takovou úroveň, aby byla akceptovatelná [369-371].

Nejzávažnější zatížení letounu bývá od přistání. Přistávající letadlo se přibližuje k zemi klouzavým letem. Při plavání letadla blízko nad zemí nastane ustálený stav, kdy aerodynamický vztlak vyváží sílu tíže letadla a zvýšený aerodynamický odpor zabrzďuje pohyb, až nastane částečná ztráta vztlaku, propadání letadla a náraz na přistávací plochu. Tato fáze přistání je nejdůležitější pro přistávací zařízení, neboť vytváří počáteční podmínky pro jeho funkci [371]. Při ideálním přistání se letoun v okamžiku „podrovnání“ a ztráty vztlaku již dotýká koly podvozku země. Klesací rychlost je téměř nulová a přistávací náraz je minimální. Toto je ideální případ. Prakticky ale dochází k tomu, že letoun má při dotyku se zemí jistou nezanedbatelnou klesací rychlost, nebo v případě brzkého podrovnání dojde ke ztrátě vztlaku ještě před dotykem se zemí. Konstrukce podvozku musí přenést a utlumit zatížení i od těchto mimořádných přistání, ke kterým zejména dochází u méně zkušených pilotů, případně za zhoršených podmínek viditelnosti [368,371].

Dynamické zkoušení leteckých podvozků

Ve stavbě letadel je dnes hlavním cílem zvyšování životnosti leteckých podvozků [368,369]. Proto se soustavně studují skutečné poměry v provozu a usiluje se o co nejvěrnější napodobování jejich namáhání v leteckých zkušebnách. To platí i o zkoušení přistávacích zařízeni, především podvozků, které jsou při rozjezdu a zejména při přistání velmi namáhány. Pro laboratorní zkoušky podvozků byl v ČR vyvinut v padesátých letech minulého století a

uveden do provozu v Aeru Radotín (později Technometra Radotín) první „Padostroj“ PS-1, který umožňoval provádět první dynamické zkoušky na pohlcení mechanické práce (pádové zkoušky) leteckých podvozků na dopadovou plošinu [368].

V šedesátých letech minulého století byl uveden do provozu ve Výzkumném a zkušebním leteckém ústavu v Praze Letňanech (VZLÚ) nový víceúčelový zkušební stroj. Jedná se o univerzální padostroj, na němž lze se samotným podvozkem napodobit přistání skutečného letadla, za působení hlavních činitelů, které přistání ovlivňuji, jako je dopředná rychlost letadla, jeho hmota, rychlost klesání, vztlaková odlehčující síla atd., a to pro případy symetrického i nesymetrického přistání. Relativní pohyb letadla vůči zemi se simuluje pádem vozu s podvozkem na roztočený buben setrvačníkového zařízení, sleduje se převzetí kinetické energie svislého pohybu letadla prací tlumicí soustavy podvozku a zabrzdění dopředné složky pohybu letadla až do jeho zastavení přeměnou kinetické energie v teplo, dané prací brzd na kolech podvozku při zanedbání aerodynamických, event. jiných (např. brzdicí padáky) odporů [368,371], který dovoluje komplexní vyšetřování přistávacích zařízení.

Data použitá pro sestavení kontrolního seznamu

Pro zajištění bezpečnosti každého strojního zařízení a bezpečí obsluhy je velice důležité identifikovat všechna možná nebezpečí vyplývající z konstrukce nebo způsobu předpokládaného používání daného zařízení [372]. Proto je třeba mít nástroj a postup pro identifikaci nebezpečí a stanovení rizik, abychom včas identifikovali, že něco je nesprávné a určili místo, kde je třeba pro dosažení správného výsledku provést opatření. Předmětný nástroj je třeba správně použít tak, aby ve sledovaném případě byl test kvalitní a dal správné výsledky. Proto jsme zvolili nástroje, a to postup ve formě bezpečnostního auditu podle nástroje kontrolní seznam [5,15], které jsou nástroji rizikového inženýrství [11].

Cílem je zajistit, aby testy podvozků byly správné a spolehlivé a aby měly dobrou vypovídací hodnotu. Proto byly použity jak teoretické znalosti [1,5,15,368,372], technická dokumentace a postupy pro provádění zkoušek na Padostroji PS 1 s nohou hlavního podvozku levou/pravou (nebo příďového, kde se uvažuje předepsané vztlakové vyvážení) včetně úplného kola za daných klimatických podmínek (20°C +/-5°C), tak experimentální data z prováděných testů na Padostroji PS-1 [368]. Pro civilní letouny je test stavu podvozku prováděna podle požadavků předpisu EASA CS-23/FAR (letouny kategorie normální, cvičná, akrobatická a pro sběrnou dopravu) Part 23, AMDT. 23-55, § 23.725, § 23.726, §23.727 [369,370]. Pro vojenské letouny je zkouška prováděna podle požadavků technických podmínek vydaných výrobcem na základě požadavků zadavatele [368].

Pomocí kontrolního seznamu je možno jednoduše ověřit stav sledovaného objektu a zajistit tak, že nejsou přehlédnuty žádné neshody. Jednou z možných činností je kontrola strojního zařízení a lidského faktoru. V našem případě se jedná o postup prací na Padostroji PS-1 při testu tlumení nárazu podvozku letounu v okamžiku přistání. Kontrolní seznamy se mohou také značně lišit, co se týče úrovně detailů, a mohou být využívány k označení splnění standardů a zvyklostí. V případě navrhovaného kontrolního seznamu je snahou vyhovět v rámci jednoho dokumentu jak obsluze stroje, tak řídícím a kontrolním orgánům.

Při sestavení kontrolního seznamu pro sledovaný proces jsme dbali na splnění požadavků uvedených v pracích [5,15], tj. kontrolní seznam musí být jasný, stručný a srozumitelný pro všechny strany a musí být zamezeno i jakékoliv dvojsmyslnosti. Analýza rizik pomocí kontrolního seznamu dva zásadní kroky a to: odpovědi na otázky; a celkové vyhodnocení, tak jsme pro bezpečnostní audit testu navrhli následující postup:

- odpovědi na otázky kontrolního seznamu ANO či NE,
- v případě, že se vyskytne odpověď NE, tak žádat dohlížejícího kontrolora o posouzení důležitosti činnosti, tj. o rozhodnutí: zda lze dále pokračovat v auditu a procesu testu, anebo je nutné provést nápravná opatření, aby požadavek byl splněn.

Vytvořený kontrolní seznam je uveden v tabulce 64.

Tabulka 64. Kontrolní seznam pro prověření stavu padostroje před testem podvozku [368].

Pořadové číslo	**Otázka**	**ANO**	**NE**
1. Administrativní úkony			
1	Je platné povolení úřadů k provádění testů podvozků? (platnost Oprávnění vydaného ÚCL a Osvědčením ke zkoušení vydaným OVL MO)		
2	Jsou splněny podmínky uvedené v Příručce podnikové jakosti? (Příručka jakosti rozpracovává a popisuje systém řízení jakosti a uvádí jeho základní úroveň)		
3	Je podepsán předávací protokol testovaného podvozku?		
4	Je vydáno zadání (metodika, technické podmínky a specifikace) pro zkoušku podvozku daného typu?		
5	Je vydán postup instalace senzorů na podvozek daného typu pro zkoušku?		
6	Je testovaný podvozek správně upevněn, aby nedošlo k ovlivnění výsledků testů?		
7	Souhlasí výrobní číslo zkoušeného podvozku se zadáním?		
8	Je přítomen osvědčující pracovník (kontrolor), který průběh testu sleduje?		
2. Bezpečnost práce			
9	Jsou při obsluze Padostroje PS-1 dodržovány zásady bezpečnosti práce?		
10	Je pracovní prostředí vhodné k provádění příslušných zkušebních prací z pohledu znečištění zkušebních prostor?		
11	Je pracovní prostředí vhodné k provádění příslušných zkušebních prací z pohledu dostatečného osvětlení?		
12	Je pracovní prostředí vhodné k provádění příslušných zkušebních prací z pohledu hladiny hluku?		
13	Byla provedena kontrola teploty pracovního prostředí, zda odpovídá podmínkám pro provádění zkoušky? (20°C +/-5°C)		
3. Kontrola Padostroje PS-1 před vlastní zkouškou			
14	Byla provedena kontrola knihy údržby Padostroje PS-1 zda má platný interval do další kontroly?		
15	Byla provedena vizuální kontrola stavu stroje?		
16	Byla provedena kontrola olejoznaku hydraulického systému na olejové nádrži v horní části stroje?		
4. Instalace senzorů na testovaný podvozek			
17	Jsou k dispozici senzory určené k instalaci na testovaný podvozek?		
18	Je testovaný podvozek řádně a bezpečně upevněn na transportním přípravku?		
19	Je provedena instalace senzorů na podvozek daného typu pro zkoušku podle vydaného postupu a průvodky práce?		
20	Jsou řádně připevněny konektory senzorů a propojovací kabeláž k testovanému podvozku?		

5. Instalace přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1, za předpokladu, kdy není instalováno závaží a pohyblivý stůl je spuštěn na bezpečnostní podpěře			
21	Má přípravek sloužící k upevnění testovaného podvozku k Padostroji PS-1 platnou revizi?		
22	Je vertikálně pohyblivý vůz podepřen bezpečnostní podpěrou?		
23	Byly provedeny úkony potřebné k instalaci přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1? (prodloužení manipulační délky hydraulického systému)		
24	Je přípravek bezpečně ustaven na manipulačním vozíku?		
25	Je přípravek ustaven a spojen s danou soustavou vhodnými svorníky dle technické specifikace a průvodky práce?		
26	Je vertikálně pohyblivý vůz spuštěn s nainstalovaným přípravkem na bezpečnostní podpěru?		
27	Byly provedeny zpětné úkony potřebné k instalaci přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1 ? (zkrácení manipulační délky hydraulického systému)		
6. Naložení závaží na pohyblivý stůl			
28	Je vertikálně pohyblivý vůz pomocí hydraulického systému zdvižen do horní krajní polohy Padostroje PS-1 k zásobníku závaží? (kontrola volného chodu pohyblivého vozíku)		
29	Je potřebný počet závaží - desek (dle technické specifikace a průvodky práce) uvolněno na vertikálně pohyblivý vůz?		
30	Je zbylé závaží v horní části stroje řádně zajištěno v nosných tyčích zajišťovacími kolíky? (pozor - řádně překontrolovat, nebezpečí úrazu!!!)		
31	Je vertikálně pohyblivý vůz pomocí hydraulického systému spuštěn do dolní polohy a opřen o bezpečnostní podporu? (kontrola volného chodu pohyblivého vozíku)		
32	Jsou desky závaží zajištěny na pohyblivém stole sponami?		
33	Je vertikálně pohyblivý vůz se závažím dovážen pytli s olověnou drtí podle technické specifikace zkoušeného podvozku a průvodky práce?		
7. Instalace podvozku do přípravku na pohyblivém stolu			
34	Je do přípravku instalován testovaný podvozek včetně kola, případně brzdy dle průvodky práce?		
35	Je zkontrolován plnící tlak v tlumiči a v pneumatice testovaného podvozku pomocí kalibrovaných manometrů?		
36	Je spojeno měřící lanko celkového propérování podvozku s unášečem pásového měřítka?		
8. Seřízení polohy „nula“ celkového propérování			
37	Je seřízená poloha lanka a pásového měřítka celkového propérování nastaveného na hodnotu „nula“ okamžiku dotyku kola a dopadové desky?		
9. Simulace vztlakové síly pomocí pružných provazců			
38	Jsou instalovány držáky lan do vodících trubek ve vztlakových křídlech a nasunuty na dvojice vodících tyčí?		

39	Je potřebný počet lan stejnoměrně rozdělen a zaháknut do ok držáků pružných lan? (pozor - lana nesmí být překřížena!!!),		
40	Jsou v „nulové“ poloze podvozku (dotyk kola s dopadovou deskou) zajištěny držáky na vodících tyčích maticemi?		
10. Předpětí pružných provazců			
41	Je provedena změna předpětí pružných provazců v horní části padostroje? (pozor - provádět při uvolněných lanech!!!)		
11. Kontrola hmotnosti zkoušené soustavy			
42	Je připojen měřící zesilovač k senzoru síly?		
43	Je provedeno zahřátí, řádné nastavení a vynulování měřícího zesilovače síly?		
44	Je připojen senzor síly k měřící aparatuře, včetně senzorů umístněných na zkoušené podvozkové noze (senzor propérování a statického přetížení), senzor celkového propérování (senzor absolutního lineárního odměřování)?		
45	Jsou propojovací kabely mezi měřící ústřednou a senzory uspořádány tak, aby nebránili při vlastním měření a aby nedošlo také k jejich poškození?		
46	Je zapnuté napájení měřící ústředny a obslužný software PC pro sledování měřených parametrů, v tomto případě hmotnost zkoušené soustavy?		
47	Jsou v případě použití vztlakových lan tato lana odpojena?		
48	Je zkoušená soustava po odstranění bezpečnostní podpěry spuštěna na dopadovou desku?		
49	Je odjištěn zámek dopadového vozíku? („odhoz“ z nulové výšky)		
50	Bylo provedeno odečtení a zaznamenání hodnoty hmotnosti zkoušené soustavy z displeje zesilovače, zda odpovídá požadované velikosti?		
51	Bylo provedeno odečtení a uložení hodnoty hmotnosti zkoušené soustavy z displeje PC, zda odpovídá požadované velikosti?		
52	Je po kontrole hmotnosti zkoušené soustavy vertikálně pohyblivý vůz zdvižen a zajištěn zámek dopadového vozíku?		
53	Je vložena bezpečnostní podpora a vůz spuštěn na tuto podporu?		
54	Je potřeba soustavu dovážit a opakovat vážení zkoušené soustavy?		
55	Jsou v případě použití vztlakových lan tato lana znovu připojena?		
12. Pádová zkouška			
56	Je zkoušená soustava zdvižena na předepsanou pádovou výšku dle technické specifikace a průvodky práce?		
57	Je řádně nastaven měřící zesilovač pro měření dopadové síly?		
58	Je správně nastaveno měřící lanko celkového propérování?		
59	Je zapnuté napájení měřící ústředny a obslužný software PC pro sledování měřených parametrů?		
60	Je vynulována poloha celkového propérování prostřednictvím software – proveden reset?		

61	Je odstraněna bezpečnostní podpora?		
62	Je spuštěna ochranná klec do dolní polohy?		
63	Je odjištěn zámek odhozu zamáčknutím žlutého tlačítka na ovládacím pultu?		
64	Je spuštěn záznam měřící aparatury software - PLAY?		
65	Je proveden odhoz s následnou vizuální kontrolou celé soustavy, zda nedošlo k nepředvídatelným událostem ohrožující bezpečnost obsluhy Padostroje PS-1?		
66	Je vyzdvižena ochranná klec do horní polohy?		
67	Je proveden odečet měřených parametrů a jejich zápis do tabulky naměřených hodnot?		
68	Je vypnut záznam měřící aparatury a provedena kontrola naměřených dat s následným vyhodnocením testu?		
13. Zpětné zapojení pohyblivého stolu			
69	Je otevřen regulační ventil hydraulického systému a spuštěn vůz ke stolu?		
70	Jsou čelisti zámku řádně zapadnuty za ozuby na trnu vozu?		
71	Je zámek zajištěn zamáčknutím stříbrného tlačítka?		
72	Je provedena kontrola zapadnutí západky zámku?		
73	Je uzavřen regulační ventil hydraulického systému umožňující spouštění vozu?		
74	Je zdvižena zkoušená soustava do patřičné výšky v případě pokračování zkoušky?		
75	Je v případě ukončení zkoušky vložena bezpečností podpora a vůz je spuštěn na tuto podporu?		
14. Odstranění simulace vztlakové síly pokud byla použita			
76	Jsou v nulové“ poloze podvozku (dotyk kola s dopadovou deskou) odstraněny držáky na vodících tyčích sejmutím matic?		
77	Jsou odstraněny držáky lan vodících trubek ve vztlakových křídlech?		
78	Jsou vysunuty dvojice vodících tyčí vztlakové síly?		
15. Demontáž podvozku			
79	Je odpojeno měřící lanko celkového propérování s unášečem pásového měřítka?		
80	Jsou odpojeny vodiče od senzorů umístněných na zkoušené podvozkové noze (senzor propérování a statického přetížení?		
81	Je z přípravku vyjmuta testovaná podvozková noha dle průvodky práce?		
16. Sejmutí závaží (desek) z pohyblivého stolu			
82	Jsou odstraněny pytle s olověnou drtí, jsou-li použity?		
83	Jsou sejmuty zajišťovací spony desek na pohyblivém stolu?		
84	Je vertikálně pohyblivý vůz pomocí hydraulického systému zdvižen do horní krajní polohy Padostroje PS-1 k zásobníku závaží? (kontrola volného chodu pohyblivého vozíku)		
85	Jsou řádně zajištěny desky závaží v nosných tyčích zajišťovacími kolíky? (pozor - řádně překontrolovat, nebezpečí úrazu!!!)		

86	Je prázdný stůl bez závaží spuštěn do dolní polohy a opřen o bezpečnostní podporu?		
87	Je při spouštění zkontrolován volný chod vozíku?		
17. Demontáž přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu			
88	Je vertikálně pohyblivý vůz podepřen bezpečnostní podpěrou?		
89	Byly provedeny úkony potřebné k vyjmutí přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1? (prodloužení manipulační délky hydraulického systému)		
90	Je přípravek rozpojen s danou soustavou vyjmutím svorníků dle technické specifikace a průvodky práce?		
91	Je vertikálně pohyblivý vůz spuštěn bez přípravku na bezpečnostní podpěru?		
92	Byly provedeny zpětné úkony vedoucí ke zkrácení manipulační délky hydraulického systému a uvedení Padostroje PS-1 do výchozího stavu pro další možné práce?		
18. Provedení zápisu do evidenční knihy zkoušek			
93	Je do evidenční knihy proveden záznam pádové zkoušky se všemi náležitostmi?		
19. Vyhodnocení zkoušky			
94	Je zpracován záznam a vyhodnocení zkoušky dle technické specifikace a průvodky práce?		
95	Je vystaven protokol o provedené zkoušce?		

Kontrolní seznam a předmětný postup bezpečnostního auditu je takový proto, že otázky sledují lineární proces, ve kterém jednotlivé úkony na sebe navzájem navazují a nelze je obsluhou samovolně vynechat bez souhlasu nadřízených orgánů. Tato podmínka vyplývá z dokumentu „Příručky zkušebny přistávacích zařízení“ [373], pro kterou se nástroj vytvářel, a ve které se říká, že jakákoliv změna postupů, metodik aj. je možná pouze za souhlasu dozorových podnikových a státních orgánů, a to formou dodatků k platným povolením prováděných zkoušek daného pracoviště, což mimo jiné představuje nemalou administrativní zátěž a časovou prodlevu. V daném případě se hodnotový systém zužuje pouze na hodnocení vynikající, neboť následující krok v kontrolním seznamu může následovat pouze za podmínky splnění předchozího kroku. Případnou výjimku může jednorázově schválit pouze řídící pracovník při potřebných konstrukčních úpravách, a to pouze v rámci podnikových testů, a to za předpokladu řádného dodržování bezpečnosti při práci.

5.11. Výsledky studia rizik dodavatelských řetězců a návrh ochranných opatření

Bezpečná komunita je v současné době globalizace velmi závislá na úrovni bezpečnosti dodavatelských řetězců zajišťujících obslužnost území základními komoditami nutnými pro život lidí. Řada událostí v posledních letech spojených s dodavatelskými řetězci ukázala jejich velkou důležitost v době, kdy princip JUST in TIME v procesním řízení firem je běžný. Např. nedávné přerušení dodávek ropy do střední a západní Evropy z důvodů neshod mezi Ukrajinou a Ruskou Federací odhalilo vysokou zranitelnost postižených států na dané komoditě a vedlo k otevření nového problému, který musí EU řešit v rámci svého bezpečí a rozvoje.

Moderní dodavatelský řetězec se značně proměnil od doby, kdy se zboží dopravovalo na trh na voze taženém koněm, ale k zásilkám v kyberprostoru má stále ještě dlouho cestu před sebou. Ale i za pouhých dvacet let bude dodavatelský řetězec budoucnosti přesnější, přístupnější, spolehlivější, udržitelnější a ziskovější než kdykoliv předtím.

Dodavatelský řetězec se skládá z dodavatelů, výrobců, distributorů, prodejců a zákazníků. Jde o vícestupňové provázané systémy, u kterých mezi jednotlivými stupni v obou směrech proudí materiálové, finanční, informační a rozhodovací toky [194]. Materiálové toky zahrnují toky surovin, meziproduktů a hotových produktů směrem od dodavatele k zákazníkům. Opačně orientované jsou toky produktů určených k opravě, recyklaci nebo likvidaci. Finanční toky zahrnují různé druhy plateb, úvěry, toky vyplývající z vlastnických vztahů atd. Informační toky propojují systém informacemi o objednávkách, dodávkách, plánech apod. Rozhodovací toky jsou posloupnosti rozhodnutí účastníků ovlivňujících celkovou výkonnost řetězce. Finální dodavatel a všichni jeho poddodavatelé, kteří se podílí na kompletaci a plnění dodávky podle smlouvy mezi finálním dodavatelem a objednatelem dodávky. Dodavatelský řetězec může obsahovat více kooperačních stupňů a vztahuje se vždy k plnění jedné dodávky.

Vzájemné vztahy mezi jednotlivými kooperačními stupni jsou založeny na smluvním základě [374-380]. Z metodického pohledu je každý dodavatelský řetězec systém systémů. V inženýrských disciplínách zaměřených na riziko v současné době používáme dvě disciplíny [194,376], které u dodavatelských řetězců dělíme na soubor disciplín, jejichž cílem je zajistit:

- bezpečí dodavatelského řetězce, tj. bezpečí systému bez ohledu na okolí (řízení bezpečí – systémová bezpečnost = security management),
- bezpečnost dodavatelského řetězce, tj. bezpečí a rozvoj jak dodavatelského řetězce, tak jeho okolí.

S ohledem na bezpečnost lidského systému sledovat dodavatelské řetězce, které zajišťují:

- suroviny, materiály a výrobky, které slouží k výrobě energie,
- elektrickou energii v požadovaném množství a kvalitě,
- dodávky nafty v požadovaném množství a kvalitě,
- dodávky zemního plynu v požadovaném množství a kvalitě,
- dodávky pitné vody v požadovaném množství a kvalitě,
- dodávky léků energie v požadovaném množství a kvalitě,
- dodávky potravin v požadovaném množství a kvalitě,
- dodávky surovin pro strategický průmysl v požadovaném množství a kvalitě,
- dodávky ochranných prostředků,
- dodávky surovin pro základní průmysl pro výrobu předmětů denní potřeby v požadovaném množství a kvalitě,
- dodávky informací důležitých pro řízení bezpečnosti lidského systému,
- odstranění odpadů tak, aby nedošlo ke škodám a ztrátám v lidském systému.

Aplikace poznatků systémové teorie na dodavatelské řetězce znamenala nejen významný posun ve vědeckém zkoumání v nejrůznějších oblastech vědy, ale při důsledném uplatnění přináší významné efekty i v praxi. Dodavatelský řetězec je síť organizací, které jsou zapojeny, po i proti směru materiálového toku do různých procesů a aktivit, které přinášejí hodnotu ve formě výrobků a služeb podle požadavků konečného zákazníka [374], tj. dodavatelský řetězec zahrnuje všechny kroky, které je třeba přímo nebo nepřímo uskutečnit pro splnění požadavků konečného zákazníka.

Dodavatelský řetězec nezahrnuje jen výrobce a dodavatele, ale i přepravce, sklady, prodejce a zákazníky. Prostřednictvím všech organizací, např. výrobců, obsahuje dodavatelský řetězec všechny funkce, které jsou nutné pro splnění požadavků zákazníků. Uvedené funkce - a nejen ty – zahrnují vývoj nových výrobků, marketing, distribuci, financování a služby zákazníkům [376].

Podle [376] je dodavatelský řetězec síť partnerů, kteří kolektivně transformují komodity ve finální produkty s přidanou hodnotou pro konečného zákazníka a kteří na každém kroku realizují nezbytné zpětné toky. Každý partner přitom odpovídá za procesy přinášející hodnotu výrobkům … partneři uskutečňují procesy jako dobývání surovin, dopravu…

Definic dodavatelského řetězce je řada; např. organizace British Institute of Logistics z r. (1999 uvádí, že dodavatelský řetězec je posloupnost událostí zaměřených na splnění požadavků zákazníka. Patří k nim nákup, výroba, distribuce a likvidace odpadů, které jsou spojené s adekvátní dopravou, skladováním a využitím informačních technologií. Obdobnou koncepci dodavatelského řetězce nacházíme u Pernici [378], který spojuje pojem dodavatelský řetězec s integrovaným procesním logistickým řetězcem vedoucím od dodavatelů až ke konečnému zákazníkovi resp. k recyklaci, tj. jde o posloupnost kroků přidávajících hodnotu, vedoucí k uspokojení konečného zákazníka, zprostředkovaných informačními technologiemi, dopravou, sklady atd.

Je třeba připojit pohled mezinárodní organizace Supply-Chain Council, která v rámci konceptu srovnávacího modelu dodavatelského řetězce navrhuje jeho dekompozici na 5 skupin aktivit: plánování, získávání zdrojů, transformace (výroba, manipulace.), dodávky a realizace zpětných toků, které se v řetězci opakují v různém rozsahu u všech spolupracujících partnerů v řetězci.

Pernica [378] pak definuje logistický systém jako „uspořádaný soubor technických a lidských prvků a vazeb mezi nimi, které spolupracují při plánování a výkonu logistických řetězců“. Obdobné pojetí lze najít i v [379]. Přesto, že lze najít u obou skupin formulací řadu společných prvků, např. orientaci na konečného zákazníka nebo důraz na zvyšování hodnoty služeb a výrobků pro zákazníky, výrazně se liší v tom, že zatímco prvá skupina vyjadřuje dodavatelský řetězec jako posloupnost, síť, množinu organizací, které jsou nositeli funkcí nutných pro realizaci požadavků zákazníků, druhá ho vyjadřuje jako sled kroků, událostí, aktivit, procesů. V existujících pojetích je i řada nedůsledností, kdy při uvádění příkladů aktivit jsou mezi činnostmi řazeny i organizace.

Ač není jednoznačná definice, je s ohledem na ochranu lidí jisté, že po kritické infrastruktuře přibyly do krizového řízení také problémy dodavatelských řetězců, na nichž záleží přežití lidí při kritických situacích a zachování funkčnosti životně důležitých infrastruktur. V práci [194,376] byly identifikovány dále uvedené jevy, které představují vysoká rizika pro dodavatelské řetězce:

- tradiční pohromy, které poškozují majetek – požáry, přírodní pohromy velkých rozměrů, výpadky elektrizační soustavy a výpadky zařízení,
- sociální pohromy jako krádeže, násilí a terorismus,
- poruchy v řízení lidské společnosti, jakými jsou politická nestabilita, výkyvy v kurzu měn, výpadky dodávek energií a surovin v důsledku politických problémů v zemi dodavatele,
- podvodná jednání a důsledky chyb v centrálním plánování v ekonomické oblasti,
- výpadky počítačových a telekomunikačních sítí,
- požadavky velmi náročných zákazníků (precizní a rychlé dodávky) s ohledem na krátkou životnost některých výrobků,
- požadavky na zajištění komplexní shody u výrobků dle právních předpisů jednotlivých zemí,
- výpadky v komunikaci mezi odpovědnými činiteli v základních sektorech dodavatelského řetězce,
- možnost použití některého zboží jako zbraně.

Nároky na dodavatelské řetězce jsou ze strany výrobců, zákazníků i dopravců. Např. stále více pozorujeme zvýšené nároky zákazníků na bezpečnost, kontinuitu a spolehlivost distribuce vstupních surovin, meziproduktů i hotových výrobků. Motivace výrobců je určena konkurenčním tlakem. Dopravci jsou vystaveni různým tlakům, které závisí jak na konkurenci,

tak na rozmanitých požadavcích při přepravě zboží, např.: zajistit plynulé zásobování; efektivnost zásob; specifické požadavky na přepravu zboží s krátkou dobou trvanlivostí; specifické požadavky na přepravu velmi cenných komodit; specifické požadavky na přepravě nebezpečného zboží atd.

Aplikace standardů ISO 28000 a organizace TAPA zvyšuje bezpečnost dodavatelských řetězců, nejen ve smyslu ošetření rizik typicky spojených s přerušením dodávek způsobených úmyslnou či neúmyslnou ztrátou zboží včetně trestně-právních deliktů a škodných událostí, ale i zvýšením ochrany před terorismem, pašeráctvím a nelegální migrací. Z pohledu systémové teorie řeší jen dílčí úseky. Protože se jedná o soubor několika vzájemně propojených systémů, aplikujeme dále přístup založený na integrální bezpečnosti.

V práci [380] jsou studována specifika spojená s dodavatelskými řetězci soustředěnými na nebezpečné látky, které navíc při přepravě mohou ohrozit okolí, když dojde k dopravní nehodě. Proto je sestrojen model řízení bezpečnosti dodavatelského řetězce [376]. V předmětné práci je též uveden postup, jak vytvářet program na zvyšování bezpečnosti dodavatelského řetězce.

Pro firmu, která se zabývá dodavatelskými řetězci, je důležité jednak obstát v stále rostoucí konkurenceschopnosti a jednak být ziskovým subjektem. Důležitou roli hraje stát, který jednak dovoluje (nebo také nedovoluje) a jednak zřizuje vhodné podmínky pro fungování dodavatelských řetězců. Všichni účastníci v dodavatelském řetězci (výrobce, vývozce, dovozce, dopravce, skladovatel, celní zástupce, přepravce, zasílatel) by měli znát svá rizika a snažit se je eliminovat, resp. nejdůležitější rizika zabezpečit.

5.12. Výsledky studia rizik kritické infrastruktury a návrh ochranných opatření

Je si třeba uvědomit, že pro zajištění bezpečí a rozvoje lidí je nutná na každé úrovni (tj. od jednotlivce přes rodinu, obec až po stát či uskupení států) je nezbytná kromě jiného i materiálně technická základna. Historie ukazuje, že osvícení panovníci ji vždy budovali a že každá chyba v jejím zabezpečení v kritických chvílích znamenala porážku ve válkách nebo velké ztráty na lidských životech (viz velké hladomory). Dnes v předmětné souvislosti mluvíme o kritické infrastruktuře. Kritické infrastruktuře jsou věnovány publikace [10,11], a proto se zabýváme problematikou stručněji a uvádíme především jen nové výsledky.

V textu je pod pojmem kritická infrastruktura chápány dva základní typy systémů, a to objektově orientované systémy (object-oriented systems) a síťově orientované systémy (network-oriented systems); které jsou zpravidla provázané. Síťově orientované systémy mají vyšší zranitelnost vůči mnohým pohromám, např. útokům, protože jejich topologie neumožňuje použít v celém rozsahu ochranu založenou na fyzických bariérách.

5.12.1. Kritická infrastruktura a její úkoly

V nejobecnějším smyslu slova znamená pojem infrastruktura množinu položek, které propojují strukturální prvky systému, které udržují celou strukturu (systém) pohromadě [11]. Z daného pohledu je každá infrastruktura základnou organizovanosti systému. Tvoří ji základní zařízení a služby, které jsou nezbytné pro fungování komunity / společnosti. Je souborem vzájemně propojených skladebných prvků, které tvoří rámec podpory celé struktury. Šedé infrastruktury jsou člověkem vytvořené systémy, které poskytují některé nebo všechny veřejné služby. Proto existuje velmi úzká vazba mezi člověkem a infrastrukturou, tj.: člověk potřebuje infrastrukturu, poněvadž bez jejich služeb by se výrazně zhoršila úroveň a kvalita jeho žití; a infrastruktura potřebuje člověka, jelikož bez jeho přičinění by nevznikla, nevyvíjela se, nebyla

by udržitelná a neustále by selhávala. Člověk – lidský faktor, je tedy řídícím, tj. i kontrolním prvkem každé infrastruktury.

Výše uvedená fakta jsou založená na systémovém pojetí, tj. každá infrastruktura má prvky, které jsou propojené přirozenými vazbami a sítěmi, jimiž se realizují různé toky (energie, materiál, peníze, informace apod.) mezi prvky systému.

Cílem základních infrastruktur a technologií v každém území je zajistit obslužnost území, tj. určitou kvalitu a hierarchii veřejných služeb. Obslužnost území je ovlivněna přímo i nepřímo různými skutečnostmi. Obecně to jsou přírodní podmínky, pragmatický historický vývoj osídlení území a nové aktivity politiky koheze EU. Zranitelnost infrastruktury je míra selhání infrastruktury (tj. infrastruktura přestane fungovat nebo bude fungovat nesprávně) v území a čase. Předmětnou míru lze měřit např. normovaným souhrnným rizikem od všech očekávaných pohrom v daném území nebo pravděpodobností výpadků infrastruktury, ke kterým dojde v důsledku očekávaných pohrom, do nichž se zahrnují i vnitřní problémy infrastruktury samotné. V uvedených souvislostech jsou významné dva faktory, a to důležitost a zranitelnost infrastruktury, z jejichž skórování zjistíme kritičnost infrastruktury [11] (pozn.: čím větší kritičnost infrastruktury, tím menší je její bezpečnost). Jde o doplňující (komplementární) veličiny.

Důležitost infrastruktury v území lze např. ocenit souhrnným oceněním dopadů selhání infrastruktury, tj. ztrát, škod a újmy na chráněných aktivech (zájmech), a to veřejných a v případě vlastníka i privátních, při zohlednění doby trvání vzniklé nouzové situace, která zahrnuje jak dobu nutnou pro obnovu funkčnosti infrastruktury, kdy vznikají přímé škody i dobu, kdy se vyrovnávají nepřímé škody způsobené kauzálním řetězcem dopadů, vyvolaných selháním infrastruktury v území. Uvedené skutečnosti znamenají, že při všech akcích spojených se základními infrastrukturami, tj. i při obnově, musí být zvažována relevantní rizika a při jejich vypořádání veřejný zájem, kterým je bezpečí a rozvoj lidí v daném území. Z hlediska řízení infrastruktur je třeba u každého kritického prvku sledované infrastruktury znát, zda může být jeho činnost přerušena nebo ne, a když ano, tak na jak dlouho – minuty, hodiny, dny atd. [11].

Určení kritické infrastruktury v území závisí na chápání slova „KRITICKÝ“. Slovo „kritický“ se v odborném jazyce používá ve smyslu „mezní“, které označuje, že při překročení určené hranice dochází k nežádoucím jevům. Je proto zřejmé, že do kritické infrastruktury v daném území nepatří všechny infrastruktury každého typu, ale jen ty důležité pro přežití lidí za kritických situací. Proto vzniká otázka vymezení kritické infrastruktury. Příkladem v praxi využitelné metodiky pro výběr územní kritické infrastruktury v USA je Směrnice pro ochranu kritické infrastruktury (Guide for Critical Infrastructure Protection) z roku 2005 [59]. Směrnice představuje určitý návod pro hodnocení jednotlivých prvků kritické infrastruktury z hlediska různých kritérií. Kritéria jsou rozdělena do dvou základních skupin, které jsou dále děleny.

Podle kritérií hodnocení náležících do první skupiny se posuzuje: úroveň dopadů selhání prvků pro územní infrastrukturu; úroveň dopadů selhání prvků na funkčnost infrastruktury; časové možnosti obnovení předepsaných funkcí; úroveň zajištění fyzické ochrany prvků infrastruktury; a stupeň informovanosti veřejnosti o existenci infrastruktury. Podle kritérií hodnocení náležících do druhé skupiny se posuzuje: citlivost infrastruktury na selhání daných prvků; „přitažlivost“ prvků jako cíle potenciálních teroristických útoků; význam hrozby z hlediska nebezpečnosti zařízení, látek; úroveň dopadů dle počtu osob zasažených v areálu zařízení; úroveň dopadů dle počtu osob zasažených v okolí zařízení; a efektivita aplikace právních norem (jejich respektování apod.). Z obou částí je proveden součet bodového hodnocení, který se poté promítne do určité matice (tzv. matice kritičnosti), ve které dojde ke sloučení bodových hodnot z obou částí. Z této matice je poté zřejmé, které prvky by měly být zařazeny do kritické infrastruktury.

Vypracováním konkrétních metod pro výběr opatření k zajištění bezpečnosti prvků kritické infrastruktury se zabývají specializované skupiny v Sandia National Laboratories. Jedním

z metodických postupů je příručka Vital Area Identification [61], kterou lze využít při stanovení způsobu ochrany důležitých prvků, objektů nebo systémů proti provedení teroristického útoku nebo jiného kriminálního činu. Jde o sofistikovaný postup pro stanovení životně důležitých zón a následné zabezpečení těchto zón proti případným útokům. Postup využívá stromy poruch, ze kterých vyplývá, jaké prvky jsou klíčové pro funkci celého systému. V postupu jsou v určitých fázích jako podpora rozhodování využívány rozhodovací matice. Metoda zohledňuje mimo bezpečnostních parametrů také aspekty ekonomické a nabízí určité kompromisy. Příručka pracuje v praktické oblasti s hypotetickými zařízeními a klade důraz na spolupráci odborníků z různých oblastí. To znamená nejenom z oblasti fyzické ochrany, ale také specialisty provozu, technické bezpečnosti a v případě jaderných zařízení také z oblasti jaderné bezpečnosti.

Každá dílčí infrastruktura se skládá z fyzických prvků a z procesů, které používají tyto prvky pro plnění úkolů dílčí infrastruktury. Jestliže se podíváme na dílčí infrastruktury, které jsou v České republice zahrnuté pod pojem „kritická infrastruktura“, tak zjistíme, že jsou propojené. Podle prací [11,381-383] propojitelnost znamená závislost mezi aspoň dvěma dílčími infrastrukturami. Prostřednictvím tohoto spojení stav jedné dílčí infrastruktury ovlivňuje nebo koreluje se stavem jiné dílčí infrastruktury. Tuto definici lze ještě rozšířit o podmínku vzájemného sdílení některých fyzických prvků nebo procesů, přičemž tyto prvky nebo procesy mohou být situovány v určité územní oblasti. Tato vzájemná závislost v území může být fyzická, kybernetická, logická a územní. Přitom platí:

1. Dílčí infrastruktury jsou fyzicky vzájemně závislé, jestliže stav jedné z nich je závislý na materiálním výstupu dílčí infrastruktury druhé.
2. Kybernetická vzájemná závislost znamená, že stav jedné dílčí infrastruktury závisí na informacích z jiné dílčí infrastruktury. Kybernetická vzájemná závislost předpokládá existenci informační (dílčí) infrastruktury.
3. Dílčí infrastruktury jsou územně vzájemně závislé, jestliže události v území mohou měnit stavy dílčích infrastruktur.
4. Logická vzájemná závislost znamená, že stav jedné dílčí infrastruktury závisí na stavu jiné dílčí infrastruktury, přičemž mechanismus propojení není fyzický, kybernetický nebo územní. Jedná se o závislosti přenášené přes toky, kterými jsou předpisy, finance, legislativa apod., např. se může jednat o finanční trhy.

V práci [11] jsou charakteristiky dílčích infrastruktur doplněny ještě o další položky, jako jsou typy poruch a selhání (kaskádní a eskalující poruchy, porucha ze stejných příčin – například živelní pohroma), provozní stav (normální, abnormální a kritický provoz), míra těsnosti vztahů a propojení (volné, těsné, složité) a charakteristiky kritické infrastruktury (časové, územně prostorové, organizační, vlastnické a institucionální).

V důsledku vzájemné závislosti porucha či selhání jedné dílčí infrastruktury způsobí poruchu či selhání dílčí infrastruktury druhé. Tento fakt přispívá ke kritičnosti souboru infrastruktur v území / objektu / státu, který jsme nazvali kritická infrastruktura. Proto nestačí zajišťovat dílčí infrastruktury odděleně, ale je třeba zajišťovat celý soubor dílčích infrastruktur, tj. kritickou infrastrukturu, což v praxi znamená hledat řešení problému BEZPEČNOST SYSTÉMU SYSTÉMŮ [382,383].

Z výše uvedeného vyplývá, že každá dílčí infrastruktura i celý soubor infrastruktur je složitý dynamický systém s určitou úrovní přizpůsobivosti. Pro zajištění jeho funkčnosti se musí znát prahová hodnota – kritičnost, která určuje stav, při kterém systém neposkytuje služby v požadovaném čase a v požadované kvalitě. Ke kritičnosti každé dílčí infrastruktury lze přistupovat ze dvou hledisek z teleologického a systémového [11]:

1. Z teleologického hlediska plyne, že kritičnost je důsledkem role a funkcí dílčí infrastruktury ve společnosti. Tento koncept umožňuje pracovat s nesíťovými a netechnickými objekty a procesy.

2. Dílčí infrastruktura je ze systémového hlediska kritická v důsledku svého postavení v systému nebo vazby na jiné dílčí infrastruktury.

Z obou přístupů plyne, že na kritičnost dílčí infrastruktury má také vliv lidský systém jako lidská / sociální dílčí infrastruktura, kterou tvoří veřejná správa, podnikatelské subjekty, vzdělávací a vědecké instituce a občanská sdružení.

Při aplikaci poznatků z řízení bezpečnosti systému systémů [1,10,11] je soubor dílčích infrastruktur v území kritický, když je pouze schopný zajistit obslužnost, při které je ještě zajištěno přežití lidí v území. Ve světě se k tomuto účelu dělají analýzy sektorů, do kterých jednotlivé dílčí infrastruktury patří, sledují se závislosti mezi sektory a ochrana potom respektuje jak podmínky funkčnosti pro jednotlivé dílčí infrastruktury, tak podmínky nutné pro funkčnost souboru infrastruktur, tj. souhrnné infrastruktury.

Stanovení kritičnosti se důsledně vztahuje k velikosti dopadů ztráty funkčnosti každé infrastruktury na společnost. Při stanovení kritičnosti [11] se zvažuje:

1. Koncentrace lidí a aktiv.
2. Odvětví hospodářství (sektorová analýza).
3. Typy vzájemných závislostí mezi dílčími infrastrukturami / odvětvími:
   - na čem závisí aktiva (chráněné zájmy) daného odvětví?
   - jaká je závislost aktiv mezi odvětvími?
4. Typy služeb veřejnosti:
   - jak dlouho bude trvat obnova poskytování služeb?
   - jaké náhrady / substituty mohou být dostupné a použitelné?
5. Důvěra veřejnosti v instituce veřejné správy:
   - může poškození aktiv / veřejných služeb vést ke snížení morálky obyvatel,
   - může poškození aktiv / veřejných služeb vést ke ztrátě národní prestiže, panice, vzpouře nebo občanským nepokojům?
   - může poškození aktiv vyvolat nějaké dopady / změny na životní prostředí?

Stanovení kritičnosti v obslužnosti území vychází z analýz ohrožení od pohrom možných v daném území, ze zvážení zranitelností dílčích infrastruktur v území, ze zvážení vzájemných propojení dílčích infrastruktur v území, tj. teoreticky má stejný princip jako analýza a hodnocení rizik v území, při které se respektuje více chráněných zájmů. Proto se dá předpokládat, že v obecné rovině se proces stanovení kritičnosti může popsat následovně:

1. Charakteristika aktiv (zvažují se aktiva fyzická, kybernetická a lidská).
2. Stanovení kritičnosti (provádí se analýza ohrožení, které souvisí s pohromami a zvážení zranitelností).
3. Hodnocení dopadů na aktiva (zvažuje se koncentrace lidí a aktiv, ekonomické dopady, vzájemné závislosti, spolehlivost).
4. Hodnocení důsledků ztrát, obětí, škod a poškození aktiv.
5. Priorizace aktiv podle zadaných pravidel.

Analýza sledované literatury ukázala, že většina postupů odpovídá výše zmíněnému obecnému postupu a kritičnost se stanovuje většinou skórováním, tj. pomocí rozhodovací matice [10,11].

Interpretace výsledků pro danou infrastrukturu či technologii (i pro soubor infrastruktur) se odvozuje od polohy bodu, jehož souřadnice tvoří vypočtené hodnoty míry obslužnosti (vlastně míry důležitosti pro území) a míry zranitelnosti. Jestliže bod spadá do sektoru:

- „vysoká zranitelnost a vysoká obslužnost“ je stav infrastruktury či technologie (či souboru infrastruktur) považlivý, tj. kritický, pro dané území a z hlediska zajištění bezpečí a udržitelného rozvoje je třeba situaci řešit zálohováním a zodolněním dané infrastruktury,
- „nižší zranitelnost a nižší obslužnost“ je stav infrastruktury či technologie (či souboru infrastruktur) uspokojivý a je třeba čas od času provést kontrolu stavu v území,

- „vysoká zranitelnost a nižší obslužnost“ je stav infrastruktury či technologie (či souboru infrastruktur) podmíněně uspokojivý a je třeba zajišťovat připravenost na sofistikovanou odezvu v případě selhání infrastruktury či technologie (či souboru infrastruktur) a prevenci soustředit na preventivní a zmírňující opatření vedoucí ke snížení zranitelnosti infrastruktury či technologie (či souboru infrastruktur) vůči možným pohromám, které mohou její selhání způsobit,
- „nižší zranitelnost a vysoká obslužnost“ je stav infrastruktury či technologie (či souboru infrastruktur) podmíněně uspokojivý a je třeba zajišťovat připravenost na sofistikovanou odezvu v případě selhání infrastruktury či technologie (či souboru infrastruktur) a prevenci soustředit na snižování kritičnosti, tj. na vytvoření dalších objektů infrastruktury či technologie (či souboru infrastruktur) v území či na vytvoření záloh stávajících objektů infrastruktury či technologie (či souboru infrastruktur).

Je pravdou, že výše popsaný postup ukazuje, že posouzení infrastruktury nebo technologie (či souboru infrastruktur) podle dvou kritérií, a to míry obslužnosti a míry zranitelnosti není výsledkem objektivního výpočtu nebo procesní analýzy, ale je spíše výsledkem subjektivních odhadů, což lze tolerovat v případě stanovení základního rámce. Složitější by to bylo v případě stanovení kritičnosti nějakého procesu.

Při skórování zranitelnosti a obslužnosti (někdy se v literatuře používá přímo důležitosti) infrastruktur a technologií je nutné zvažovat [18] dále uvedené položky: doba trvání obnovy infrastruktur a technologií; dopad selhání infrastruktur a technologií na životy a bezpečí lidí; způsobené újmy a ztráty; dopady na životní prostředí; a vyvolaný nepříznivý zájem.

Z hlediska bezpečnosti lidského systému (tj. bezpečí a udržitelného rozvoje lidské společnosti) je nutné zajistit kvalitní obslužnost území, která je podmíněna provozní bezpečností kritické infrastruktury

V práci [384], která hledala odpověď na otázku „Jak bezpečná kritická infrastruktura je dostatečná (tj. jaká úroveň bezpečnosti je dostatečná) “ byly odvozeny tolerovatelné velikosti pravděpodobnosti výskytu selhání infrastruktur, tabulka 65.

Tabulka 65. Tolerovatelné velikosti pravděpodobnosti výskytu selhání kritických infrastruktur dle [384].

Položka	**Tolerovatelná pravděpodobnost výskytu selhání za celou dobu životnosti**
Základní požadavek	723×10^{-7}
Únava	0.0668×10^{-7}*
Obslužnost	0.0668

* Velikost pravděpodobnosti podstatně závisí na stupni inspekcí, oprav a toleranci poruch.

Na základě výsledků vlastního studia i výsledků v literatuře, např. [18,59,60,382-385] jsou zzásady pro zajištění bezpečnosti kritické infrastruktury následující:

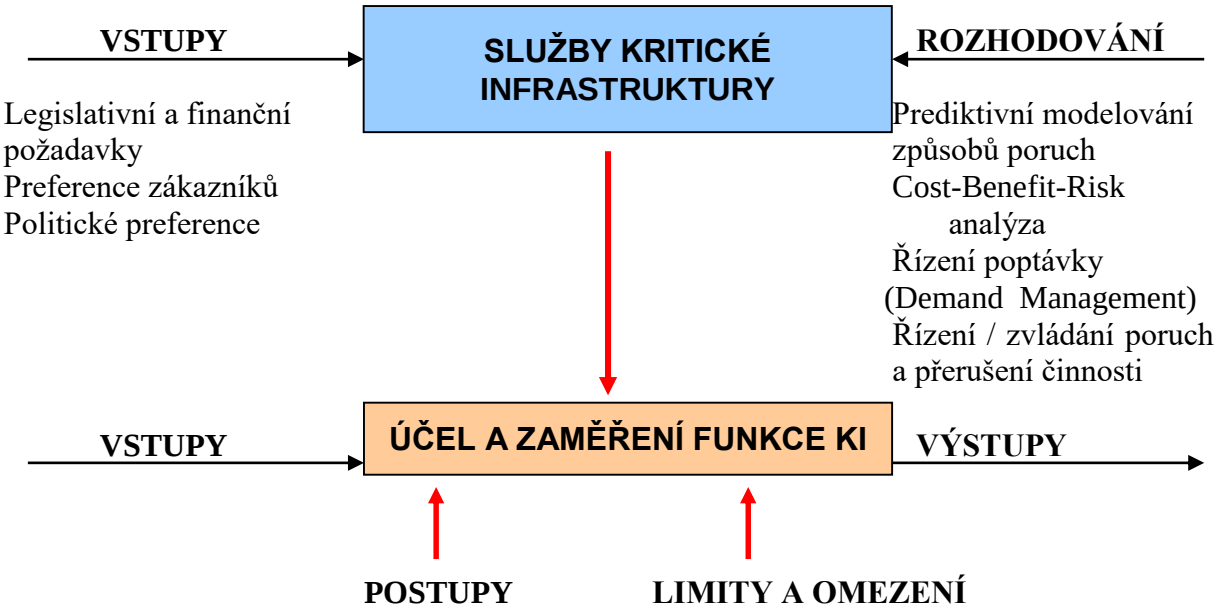
1. Kvalitní projekt, umístění, kvalifikovaná výstavba a údržba, včasné opravy a modernizace.
2. Identifikace opatření preventivních a zmírňujících vůči možným očekávaným živelním a jiným pohromám, tj. včetně havárií a jiných škodlivých jevů; připravenost složek, zdrojů, zařízení a pomůcek na zvládnutí dopadů pohrom včetně cílených útoků na kritickou infrastrukturu a technologie; a vytvoření schopností zvládnout kritické situace a zajistit rychlou obnovu prioritních infrastruktur a technologií v území.
3. Koncepce zabezpečení ochrany kritické infrastruktury a technologií vychází z faktu, že každý systém se skládá z prvků, vazeb a toků, z nichž některé tvoří kritická místa, která způsobují, že systém neplní funkci, ke které je určen, anebo k tomu významně přispívají.

Tj. jejich zranitelnost přispívá výrazně ke zranitelnosti celého systému. Na tato místa se zaměřují opatření plánů kontinuity a krizových plánů a provádí se zálohování v území.

4. Pro strategii ochrany je nutné vymezit minimální cíle, které musí systém zajistit za každé situace (tj. za normálních, abnormálních i kritických podmínek) a dopady ztráty funkčnosti systému na stát a jeho jednotlivé chráněné zájmy, a poté vymezit minimální rozsah systému, který zajistí minimální cíle.
5. Provést hodnocení rizik s ohledem na chráněné zájmy tak, že se za pohromu považuje ztráta funkčnosti kritické infrastruktury nebo technologie a komplexně se hodnotí všechny jevy, které tuto ztrátu mohou vyvolat a pro zajištění bezpečnosti se vytváří soubor opatření na jejich odstranění, minimalizaci či zmírnění.

Z analýzy a vyhodnocení poznatků v literatuře a ve zprávách z hodnocení rizik a bezpečnosti konkrétních infrastruktur, shromážděných v [12] vyplývají dále uvedená doporučení pro praxi:

1. Plány kontinuity musí vycházet z metodiky procesní / funkční analýzy, která se konceptuálně zabývá vztahy uvedenými na obrázku 72. Je však nezbytné zformulovat vhodnou a přiměřenou metodiku procesní analýzy pro různé typy infrastruktur, které náleží do kritické infrastruktury.

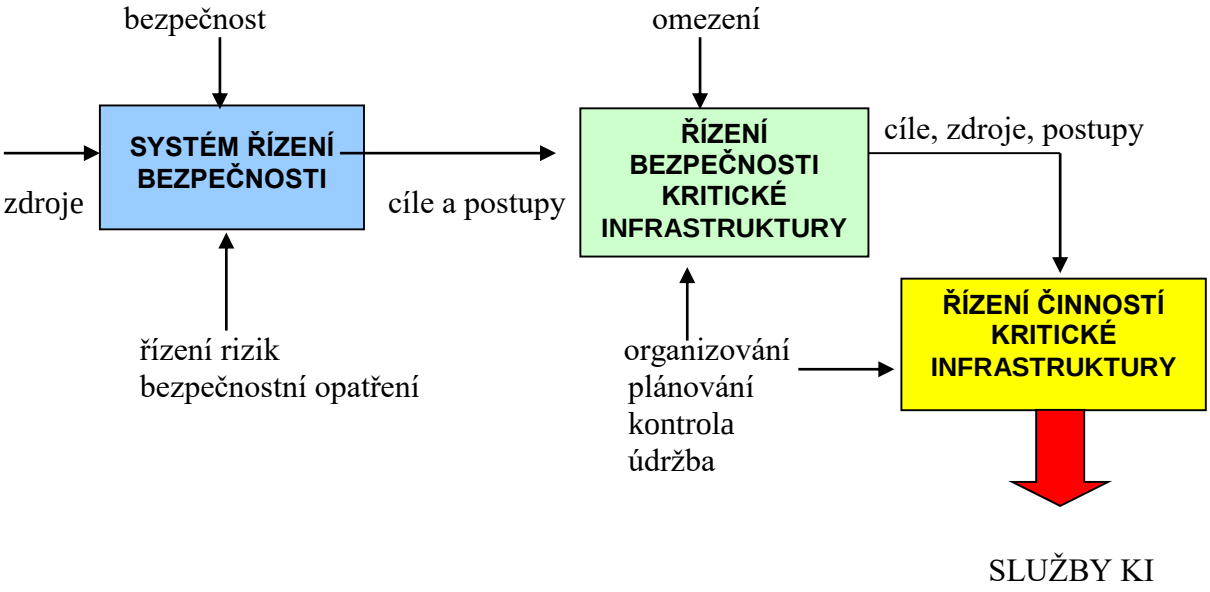


Účel a zaměření funkce	– co se má vykonat / realizovat
Postupy	– typy akcí položek nutných k realizaci účelu a zaměření funkce
Limity a omezení	– slouží k dohledu nebo restrikci účelu a zaměření funkce (přírodní zákony, organizace práce, ochranné systémy apod.)
Vstupy	– nezbytné podmínky realizace účelu a zaměření funkce

Obr. 72. Model procesní analýzy kritické infrastruktury (KI) [11].

2. Infrastruktura a technologie se musí hodnotit z hlediska kritičnosti funkcí nejprve jako celek, a pak podle vztahu k určitému území. Kritičnost infrastruktury se musí stanovit na základě analýzy významných a nebezpečných poruch a selhání, ztrát a škod způsobených neprovozuschopností funkce, vnějších pohrom, zmírňujících opatření, reakcí a látek v daném zařízení, úniků či vytékání látek (produktovody) apod.

3. V rámci plánování kontinuity je žádoucí zabývat se vztahy mezi systémem řízení bezpečnosti, systémem řízení provozu kritické infrastruktury a výkonností provozu kritické infrastruktury, obrázek 73.



Obr. 73. Vazby mezi jednotlivými systémy řízení kritické infrastruktury (KI) [11].

4. Je třeba určit v návaznosti na služby požadované od kritické infrastruktury a podle typu pohromy zařízení vyžadující bezprostřední odezvu, odezvu v prvních dvou až šesti hodinách, odezvu v prvních šesti až dvanácti hodinách a odezvu na vyžádání.

Bezpečí a rozvoj území a jeho komponent, tj. i infrastruktur, zajišťuje především bezpečnostní plánování, územní plánování, dodržování standardů, norem a předpisů při projektování, výstavbě a provozování občanských i technologických objektů a infrastruktur, ekologických, zdravotních, společenských a sociálních norem, standardů a předpisů. V případech, ve kterých dojde k narušení v důsledku pohromy, jsou v rámci nouzového a krizového plánování připraveny postupy na odvrácení či nápravu nepřijatelných, a tudíž nežádoucích dopadů.

V rámci politicko-vojenských a organizačních opatření přijímaných na mezinárodní úrovni vznikl v listopadu 2005 evropský dokument - Zelená kniha o Evropském programu na ochranu kritické infrastruktury (EuropeanProgrammeforCriticalInfrastructureProtection – EPCIP) [86]. Cílem dokumentu byla: „komunikace, koordinace a spolupráce na vnitrostátní úrovni a na úrovni EÚ mezi všemi zainteresovanými: majiteli a provozovateli infrastruktury, regulátory, profesními orgány a průmyslovými sdruženími ve spolupráci se všemi úrovněmi od vlády až po veřejnost.“

Na národní úrovni byly postupně přijaty „Národní programy na ochranu nejdůležitější infrastruktury“. Z [86] vyplývají následující úkoly:

1. Vypracování specifických kritérií, na určení nejdůležitější infrastruktury EU.
2. Postupné určování a ověřování nejdůležitější kritické infrastruktury EÚ.
3. Členské státy a Komise EÚ analyzují mezery současné bezpečnosti ve vztahu k nejdůležitější infrastruktuře EÚ podle jednotlivých sektorů.
4. Členské státy a Komise se dohodnou na prioritních sektorech/infrastruktuře
5. Pravidelné monitorování zabezpečují členské státy a Komise.

Následujícím legislativním krokem EÚ v rámci problematiky KI, bylo přijetí Směrnice rady EÚ č. 787/2006, „o identifikaci a označení evropské kritické infrastruktury a hodnocení potřeby zlepšit její ochranu“.

Definice kritické infrastruktury je stanovena ministerstvem vnitra České Republiky. Jedná se o výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva. Ze společenského hlediska se kritickou infrastrukturou rozumí vzájemně propojené sítě či systémy poskytující spolehlivý tok produktů a služeb. Bezpečnost kritické infrastruktury závisí na procesech, dějích a jevech, které v kritické infrastruktuře a jejím okolí probíhají [11]. Aby mohl být konkrétní objekt zařazen jako prvek kritické infrastruktury, musí být důležitý pro některou z oblastí bezpečnosti státu a zároveň musí podle evropských směrnic a zákonů České republiky splňovat aspoň jedno z následujících kritérií: generalizace; jedinečnost prvku pro fungování systému anebo služby; zjištěná úroveň neakceptovatelného rizika; a významná pravděpodobnost, že prvek může být cílem teroristického útoku, resp. může být ohrožen jinými rizikovými faktory.

V úvodní etapě je potřebné posoudit hlavně:

1. Rozsah – možná ztráta prvků infrastruktury se hodnotí podle velikosti zeměpisné oblasti, která by mohla být jejich ztrátou anebo nedostupností postižena. Pokud postižené území překračuje hranice České republiky, může se jednat o prvek evropské kritické infrastruktury. Pokud rozsah postižené oblasti je území státu, potom uvedený prvek definujeme jako prvek kritické infrastruktura ČR. Při regionálním, příp. místním postižení můžeme též hovořit o regionální kritické infrastruktuře, příp. místní kritické infrastruktuře (tyto pojmy v právních normách dosud nebyly definovány) a je možné je používat jen v případě exaktního odborného nadefinování. Úroveň možného rozsahu je vždy určující. Pokud pro evropskou kritickou infrastrukturu jsou rozhodující prvky, které mají vliv na fungování evropských systémů a služeb, tak pro národní, případně regionální úroveň je rozsah ztráty prvků vždy významně menší. Na místní úrovni je správnější hovořit o významných objektech (prvcích) na regionální a místní úrovni (bez pojmu kritická infrastruktura).
2. Závažnost – stupeň dopadu anebo ztráta funkce, která může být hodnocena jako žádná, minimální, mírná a velká. Mezi kritéria závažnosti, která je možné použít k hodnocení, můžeme hlavně zařadit: dopad na obyvatelstvo; dopady a životní prostředí; hospodářský dopad; politické dopady, příp. synergické jevy.
3. Časový faktor je závažnost dopadů na jednotlivé subjekty v závislosti na čase: okamžik začátku – okamžitě, do 24 hodin, do 48 hodin, …; doba působení – krátkodobě, střednědobě, dlouhodobě, …

Směrnice Rady 2008/114/ES sjednotila terminologii a postupy tak, aby byly měřitelné a porovnatelné v jednotlivých členských zemích. Jednotnost postupu je založena na tom, že všechny členské státy identifikují svoji národní a evropskou kritickou infrastrukturu na základě průřezových a sektorových kritérií.

5.12.2. Nároky na řídící personál vlastníků kritické infrastruktury

Na základě výsledků analýz selhání kritických infrastruktur, a to vlastních i publikovaných v odborné literatuře, shromážděných v [12], management kritických infrastruktur pro zajištění jejich spolehlivé funkce musí respektovat dále uvedené zásady:

- činnost zaměřovat vždy na podstatné aspekty,
- včasné varování obyvatel, zaměstnanců, návštěvníků před blížící se pohromou považovat za základ úspěchu, za základ snížení ztrát na životech,

- cíl řízení stanovovat tak, aby byl prozíravý a upřednostňoval ochranu životů, zdraví a bezpečí lidí tím, že primární pozornost vždy soustředí na snižování zranitelnosti infrastruktury, jejich technologií a objektů,
- pozornost vždy věnovat tomu podsystému, který je nejzranitelnější,
- zvládání nouzových situací zaměřit na potřeby a priority, přičemž základní prioritou je ochrana lidí a ochrana kritických zdrojů a systémů, na nichž závisí existence společnosti,
- podporovat kulturu bezpečnosti a maximální pozornost věnovat prevenci,
- zajištění připravenosti na zvládnutí nouzových situací zahrnovat do programu rozvoje území,
- občané mají právo na pomoc (asistenční službu) a pomoc se musí poskytovat konzistentně bez ohledu na ekonomické a sociální okolnosti a územní lokalizaci,
- občané patří do systému odezvy na nouzové situace nejen jako potenciální oběti, ale i jako aktivní prvky odezvy,
- zajišťovat, aby občané věděli, co jsou krizové plány a plány odezvy na nouzové situace a co přinášejí, jaká je jejich odpovědnost, jak mohou napomoci v prevenci vzniku pohromy či nouzových situací, jak mají reagovat, a proč, apod.,
- systém řízení bezpečnosti i krizové řízení musí být transparentní i pro občany a musí být přizpůsobeny místním podmínkám,
- systém řízení bezpečnosti i krizové řízení musí mít legitimitu, musí být udržitelné a přijatelné a musí být založeny na systémovém přístupu.

5.12.3. Kritická místa prvků infrastruktur

Každá infrastruktura se skládá z objektů a z liniových prvků. Zajistit bezpečnost liniových prvků je obvykle složité; fyzická ochrana a fyzická ostraha [28] mají omezené možnosti. Proto se dbá především o objekty, např. ustanovení zákona č. 240/2000 Sb., o krizovém řízení ve znění pozdějších předpisů v ČR. Kritickými objekty jsou elektrárny, rozvodny, přehrady, čistírny vod, komunikační centrály, průmyslové podniky apod. Některé příklady kritických objektů a jejich selhání jsou uvedeny výše, další uvedeme dále.

V chemickém podniku jsou kritickými místy ta místa, ve kterých může dojít ke ztrátě soudržnosti zařízení, které vede k uvolnění nebezpečných látek do okolního prostředí. V tabulce 66 jsou uvedena kritická místa stanovená pomocí vyhodnocení příčin minulých havárií, uvedených v pracích [1,5,6,10,11,304-308,309-315,321-329].

Tabulka 66. Kritická místa v chemickém podniku.

I.	Kritická místa v zařízeních s „otevřeným koncem“ cesty do atmosféry, ve kterých může dojít ke ztrátě soudržnosti.	
	A.	Místa, ve kterých soudržnost může být porušena v důsledku tzv. odlehčení procesu nebo na základě požadavku vypustit zařízení.
	B.	Místa, ve kterých soudržnost může být porušena v důsledku chybné operace nebo poruchy zařízení, např. nesprávnou činností pojišťovacího ventilu nebo poruchou pojišťovací membrány, atd.
	C.	Místa, ve kterých soudržnost být porušena v důsledku chyby operátora, např. ponechání otevřeného odvzdušňovacího nebo odkalovacího ventilu, špatné směrování přesunu materiálu, přeplnění zásobníku, otevření natlakované jednotky, atd.
II.	Kritická místa v zařízeních, ve kterých v důsledku vady zařízení může dojít ke ztrátě soudržnosti při úkonech v provozu provedených v mezích provozních podmínek zařízení.	

	A.	Místa, ve kterých soudržnost může být porušena v důsledku vad, které vznikly před uvedením do provozu a nebyly objevené před zahájením provozu (v důsledku špatných inspekčních nebo zkušebních procedur).	
		1.	Zařízení, které nebylo správně navržené pro zamýšlený výkon, např. určen špatný materiál, neadekvátní jmenovitý tlak nádob nebo potrubí, neadekvátní jmenovitá teplota, atd.
		2.	Místa, ve kterých vznikají defekty během výroby v důsledku, např. použití špatného materiálu, nízké zručnosti pracovníků, nízké úrovně kontroly kvality, atd.
		3.	Místa, ve kterých došlo k poškození zařízení nebo zhoršení jeho stavu při dopravě nebo skladování.
		4.	Místa, ve kterých došlo k poruchám při stavbě a konstrukci, např. defekty při svařování, porušení souososti, špatně přizpůsobená těsnění, atd.
	B.	Místa, ve kterých soudržnost může být porušena v důsledku vady, která zhoršuje stav zařízení při provozu a nebyla zjištěna včasně, tj. dříve, než se její vliv stal významným (např. nevhodné monitorovací procedury v případech, kdy zhoršování je postupné).	
		1.	Místa zeslabení a trhlin v ucpávkách čerpadel nebo míchadel, těsnění ventilů, těsnění přírubových spojů, atd.
		2.	Místa interní, anebo externí koroze, včetně popraskání vlivem pnutí z koroze.
		3.	Místa eroze nebo zeslabení.
		4.	Místa, ve kterých se projevuje únava kovů nebo na která působí vibrace.
		5.	Místa, která byla podrobena hrubému zacházení v předchozím údobí, např. provoz pece při teplotách převyšujících konstrukční teplotu trubek („creep“ neboli tečení materiálu).
		6.	Místa zkřehnutí v důsledku působení vodíku.
	C.	Místa, ve kterých soudržnost může být porušena vadami vzniklými při rutinní údržbě nebo při malých změnách neprovedených přesně v důsledku nízké zručnosti pracovníků, použití špatných materiály, atd.	
III.	Kritická místa v zařízeních, ve kterých v důsledku externích činitelů může dojít ke ztrátě soudržnosti při dodržení provozních podmínek zařízení.		
	A.	Místa, ve kterých soudržnost může být porušena poškození nárazem, např. pád jeřábu, silniční vozidlo, rypadlo, strojní dílna přidružená k procesní jednotce, atd.	
	B.	Místa, ve kterých soudržnost může být porušena ohraničenou explozí následkem nahromadění a vznícení hořlavých směsí vzniklých z malých úniků, např. výbušné prostředí vytvořené v analyzátorových domkách, v uzavřených kanalizacích, okolo obestavěných zásobníků, atd.	
	C.	Místa, ve kterých soudržnost může být porušena sesedáním stavebních podpěr následkem geologických nebo klimatických faktorů nebo vady stavebních podpěr následkem koroze, atd.	
	D.	Místa, ve kterých soudržnost může být porušena poškozením silničních cisteren, železničních vagónů, kontejnerů, atd. během přepravy materiálu do a z místa.	
	E.	Místa, ve kterých soudržnost může být porušena požárem.	
	F.	Místa, ve kterých soudržnost může být porušena dopady tlakové vlny z okolních explozí (exploze neohraničeného oblaku par, vybuchující nádoby, atd.), jako je přetlak v čele vlny, úlomky, poškození staveb, atd.	
	G.	Místa, ve kterých soudržnost může být porušena přírodními pohromami, vichřice, zemětřesení, povodně, blesky, atd.	

IV.	Kritická místa v zařízeních, ve kterých může dojít ke ztrátě soudržnosti v důsledku výskytu podmínek, které leží mimo limity provozních podmínek zařízení.				
	A.	Místa, ve kterých soudržnost může být porušena přetlakováním zařízení			
		1.	Místa propojení se zdrojem tlaku:		
			a.	Místa zdroje tlaku plynu:	
				1)	Místa, ve kterých může dojít k prudkému proniknutí plynu do nízkotlakého zařízení v důsledku poruchy kontroly tlaku, chybně otevřeného oddělovacího ventilu, atd.
				(2)	Místa, ve kterých může dojít k tlakovému zpětnému toku do nízkotlakového zařízení, např. v důsledku poruchy kompresoru.
			b.	Místa zdroje tlaku kapalina:	
				(1)	Místa, ve kterých může dojít k načerpání blokovaných (ucpaných) plynových prostorů,
				(2)	Místa, ve kterých může dojít k hydraulickému přetlakování jako následek blokování (ucpání) na odtokové straně,
				(3)	Místa, ve kterých může dojít k nadměrnému rázu, např. při náhlém uzavření ventilu na transportním potrubí kapaliny.
		2.	Místa, ve kterých může dojít k růstu teploty při procesu:		
			a.	Místa, která může vážně poškodit ztráta chlazení:	
				(1)	Místa, ve kterých může dojít k ztrátě průtoku chladiva, např. do chladiče reaktoru, do kondenzátoru destilační kolony, atd.
				(2)	Místa, ve kterých může dojít ke zvýšené teplotě chladiva, např. výpadek ventilátoru chladící vody, atd.
				(3)	Místa, ve kterých může dojít k nánosu nečistot v chladičích, kondenzátorech, výměnících,
			b.	Místa, která může vážně poškodit nadměrný vstup tepla	
				(1)	Místa, ve kterých může dojít k poruše kontroly vařáku, zejména u systémů vytápěných parou nebo horkým olejem,
					Místa, ve kterých může dojít ke vstupu horkého materiálu z vnějšku, např. přetok,
			c.	Místa, která může vážně poškodit nadměrný vznik tepla při chemické reakci	
				(1)	Místa, ve kterých může dojít k ujetí reaktoru, např. následkem nedostatku reakčního rozpouštědla, vysoké rychlosti přívodu surovin, vysokého molárního poměru, nashromáždění nezreagovaných chemikálií při nevhodném míchání nebo dočasné ztrátě reakce následně vedoucí k ujetí reaktoru, atd.
				(2)	Místa, ve kterých může dojít k samozahřívání následkem vstupu katalytických nečistot, např. zpětný tok ze spotřebitelské jednotky ethylenoxidu do napájecího zásobníku,
				(3)	Místa, ve kterých může dojít k samozahřívání následkem smíchání reagujících chemikálií, např. H_2SO_4 s NaOH,
				(4)	Místa, ve kterých může dojít k exotermnímu rozkladu tepelně nestabilních nebo explozivních materiálů, jako jsou peroxidy, např. následkem vzrůstu teploty, překoncentrováním nebo uložením na horké povrchy.
		3.	Místa, ve kterých může dojít k vytvoření a zapálení směsí hořlavých plynů, aerosolů nebo prachů v důsledku vnitřní exploze		
			a.	Místa, která může vážně poškodit vnik ovzduší např. následkem neadekvátního vyčištění zařízení před najetím, následkem ztráty proplachu	

				dusíkem v hlavách faklí, skladových zásobníků, odstředivkových systémů, sušáren, atd.
			b.	Místa, která může vážně poškodit nepřítomnost kritického inertního zřeďovadla, např. dusíku ve skladových zásobnících s ethylenoxidem, výpadek dusíku ve směšovacích sekcích transportních systémů pevných látek, atd.
			c.	Místa, která může vážně poškodit nedostatek prostředků tlumících explozi,
			d.	Místa, která může vážně poškodit hořlavá odchylka v oxidačních procesech, např. následkem vysokých podílů ovzduší nebo kyslíku nebo při zastavení konverze.
		4.	Místa, ve kterých může dojít k poškození následkem fyzikálně nebo mechanicky indukovaných sil nebo pnutí:	
			a.	Místa, která může vážně poškodit expanze při změně stavu, např. zamrznutí vody v potrubí,
			b.	Místa, která může vážně poškodit tepelná expanze zablokovaných kapalin, např. ve výměnících tepla nebo v dlouhých potrubích,
			c.	Místa, která může vážně poškodit vnik cizích fází, např. porucha plynového kompresoru následkem protlačení kapaliny sáním stroje, pulsování kondenzátu v parovodech, atd.
	B.	Místa, ve kterých soudržnost může být porušena podtlakováním zařízení (neschopného odolat vakuu):		
		1.	Místa, ve kterých může dojít k přímým připojením k ejektoru nebo k zařízení normálně provozovanému pod vakuem:	
			a.	Místa, která může vážně poškodit selhání zařízení, způsobené např. ztrátou kapalinového uzávěru následkem poruchy hlídače hladiny a tím způsobeným spojením s vakuovým prostorem,
			b.	Místa, která může vážně poškodit chyba obsluhy, např. otevřený oddělovací ventil, atd.
		2.	Místa, ve kterých může dojít k pohybu nebo přemístění kapalin:	
			a.	Místa, která může vážně poškodit vyčerpání zásobníků nebo nádob,
			b.	Místa, která může vážně poškodit vyprázdnění nebo gravitační odtok ze zvýšených zablokovaných zařízení.
		3.	Místa, ve kterých může dojít k ochlazení plynů nebo par:	
			a.	Místa, která může vážně poškodit kondenzace kondenzovatelných par, např. zablokování nádoby po vypařování,
			b.	Místa, která může vážně poškodit chlazení nekondenzovatelných plynů a par, např. skladový zásobník při silném dešti v létě.
		4.	Místa, ve kterých může dojít k rozpustnosti, např. rozpouštění plynů v kapalinách.	
	C.	Místa, ve kterých soudržnost může být porušena vysokou teplotou kovů (způsobující ztrátu pevnosti):		
		1.	Místa, ve kterých může dojít k požáru pod zařízením, např. následkem výtoku, prosakování čerpadel, atd.	
		2.	Místa, ve kterých může dojít k plamenovému nárazu, který způsobí lokální přehřátí, např. v pecích následkem nesouososti nebo špatným seřízením hořáků.	
		3.	Místa, ve kterých může dojít k přehřátí elektrickými topidly, např. následkem poruchy vysokoteplotních pojistek.	
		4.	Místa, ve kterých může dojít k neadekvátnímu průtoku tekutiny vytápěným zařízením, např. porucha trubky pece při ztrátě průtoku horkého oleje.	

		5.	Místa, ve kterých může dojít k vyšší průtokové rychlosti nebo vyšší teplotě páry nebo jsou limity pro průtokovou rychlost nebo teplotu páry výměníkem tepla.
	D.	Místa, ve kterých soudržnost může být porušena nízkou teplotou kovů (způsobující zkřehnutí a přepnutí):	
		1.	Místa, ve kterých může dojít k podchlazení chladící jednotky, např. následkem poruch kontroly, použitím špatného chladiva, atd.
		2.	Místa, ve kterých může dojít k neúplnému odpaření, anebo neadekvátnímu ohřátí materiálu před převedením do zařízení s určenou jmenovitou teplotou, např. následkem poruchy kontroly odparky kapalného ethylenu.
		3.	Místa, ve kterých může dojít ke ztrátě tlaku v jednotkách zpracovávajících kapaliny o nízkém bodu varu.
	E.	Místa, ve kterých soudržnost může být porušena špatným zpracováním materiálů nebo abnormálním znečištěním (způsobujícím větší korozi, chemické působení na ucpávky a těsnění, trhání korozním pnutím, zkřehnutí, atd.)	
		1.	Místa, ve kterých může dojít ke změně složení par mimo přípustné hranice.
		2.	Místa, ve kterých může dojít k abnormálnímu znečištění způsobenému surovinami nebo nevhodnými surovinami.
		3.	Místa, ve kterých může dojít ke vzniku vedlejších produktů nežádoucích chemických reakcí.
		4.	Místa, ve kterých může dojít k hromadění kyslíku, chlóru nebo jiné nečistoty zůstávající v zařízení při najíždění následkem neadekvátní evakuace nebo dekontaminace.
		5.	Místa, ve kterých může dojít k hromadění nečistot z atmosféry, obslužných médií, úniků z potrubí, atd. během provozu.

Z práce [11] vyplývá, že dopady selhání prvků kritické infrastruktury jsou jak okamžité, tak mající jistou dobu trvání. Z inženýrské praxe vyplývá, že čím déle trvá nouzová situace, tím jsou její dopady na aktiva krutější. To je zapříčiněno vznikem nejen primárních dopadů, ale i dopadů sekundárních, terciálních, atd. Proto při zajištění bezpečnosti kritické infrastruktury je nutné zvažovat čas a snažit se, aby doba trvání nouzové situace byla co nejkratší. Ze zdroje [11] vyplývá, že rozhodujícími faktory pro posouzení závažnosti selhání kritické infrastruktury jsou:

- množství lidí postižených ztrátou nebo nedostupností služeb, které zajišťuje kritická infrastruktura,
- výše ekonomických ztrát,
- výše nákladů na přežití lidí,
- pravděpodobnost výskytu kaskádovitých selhání v kritické infrastruktuře,
- velikost nákladů na obnovu.

V každém objektu, tj. území, podniku či infrastruktuře z hlediska bezpečnosti je třeba sledovat charakter objektu a chráněná aktiva. Na základě panelové diskuse s pěti experty (pracovník veřejné správy odpovídající za ochranu obyvatelstva, pracovník veřejné správy odpovídající za obslužnost území, pracovník provozovatele energetické infrastruktury odpovídající za technickou bezpečnost, pracovník provozovatele dopravní infrastruktury odpovídající za technickou bezpečnost, zástupce krizového řízení IZS) [12], tabulka 67.

Tabulka 67. Objekty kritické infrastruktury a jejich chráněná aktiva.

Objekt kritické infrastruktury	**Charakter**	**Chráněná aktiva**	**Poslání**

Obytná zástavba	Plošný	Veřejná aktiva	Sociální a společenské centrum
Zemědělské plochy	Plošný	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Výroba potravin a produktů pro další zpracování
Průmysl	plošný / bodový	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Výroba produktů a zpracování odpadů
Vodní toky, vodní plochy, lesy	plošný / liniový	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Tvorba životního prostředí Umožnění rozvoje technologií
Vodovodní soustava	bodový / liniový / síťový	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Zajistit dodávky pitné a užitkové vody
Kanalizace a odpadové hospodářství	bodový / liniový / síťový	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Zajistit nakládání s odpady
Energetický sektor	bodový / liniový / síťový	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Zajistit dodávky energií
Dopravní sektor	bodový / liniový / síťový	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Zajistit přepravu osob a zboží.
Kybernetický sektor	bodový / liniový / síťový	Veřejná aktiva Majetek Zisk Konkurenceschopnost	Zajistit přenos informací a komunikaci
Nouzové složky	bodový / síťový	Veřejná aktiva Majetek	Zajistit nouzové služby
Správa státu	bodový / liniový / síťový	Veřejná aktiva Majetek	Zajistit samosprávu a správu státu

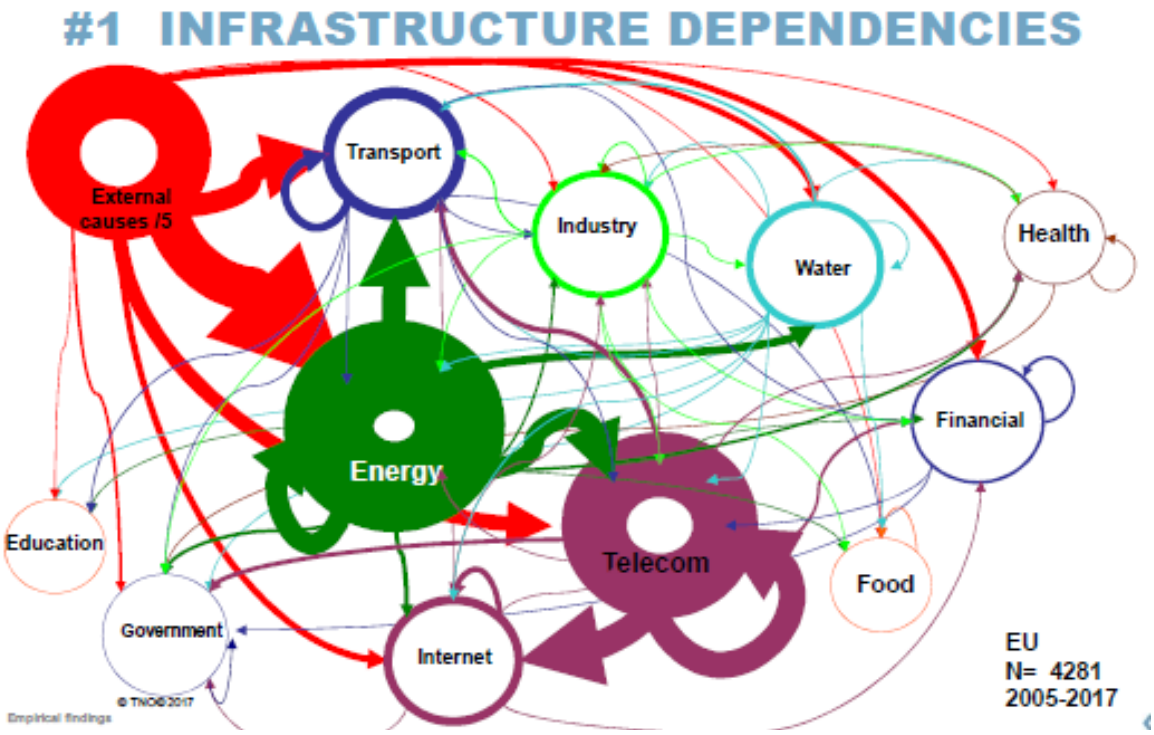
5.12.4. Selhání kritické infrastruktury

Na základě práce [386] má TNO databázi selhání kritických infrastruktur na světě. Z období 2005 – 18. 1. 2017 z období databáze obsahuje 12 706 narušení provozu kritické infrastruktury; z toho 2912 mělo kaskádovitý charakter a 534 z nich mělo společnou příčinu. Zatím pouze 2 kaskádovitá selhání z 9794 pozorovaných selhání zasáhla všechny životně důležité infrastruktury. Obvykle byly zasaženy 4 služby kritické infrastruktury – energetika, doprava, telekomunikace a internet.

Z analýzy právě popsané databáze, uvedené v [386], vyplývá, že dopady selhání kritické infrastruktury na:

- lokální úrovni poškozují veřejné blaho obyvatel obce či několika obcí (působí absenci služeb nebo jejich nedostatečnost či nízkou kvalitu) a většinu z nich lze vypořádat opatřeními na lokání úrovni,
- regionální úrovni poškozují veřejné blaho obyvatel regionu (působí absenci služeb nebo jejich nedostatečnost či nízkou kvalitu) a většinu z nich lze vypořádat opatřeními na regionální úrovni,
- národní úrovni poškozují veřejné blaho obyvatel regionu (působí absenci služeb nebo jejich nedostatečnost či nízkou kvalitu) a většinu z nich lze vypořádat opatřeními na regionální úrovni,
- příčiny selhání jsou různorodé,
- v oblasti telekomunikací jsou nejvíce kritická selhání, která postihnou systémy pro řízení dat.

Příčiny selhání uvedené v práci [386] jsou následující: bouře; vichřice; silný mráz; příval sněhu; led; povodeň; velké horko; zemětřesení; sesuv; sucho; poškození zvířaty; lidská chyba; sociální nepokoje; ekonomické selhání; technická porucha; a propojení. Procentuální zastoupení je následující: technické poruchy a lidský faktor 29-44%; živelní pohromy 17-47%; závislosti v infrastrukturách 13-28%; a úmysl 5-16%. Výsledky týkající se provázanosti infrastruktur uvedené v práci [386] jsou na obrázku 74. Obrázek je komplexní a ukazuje, že stav celé kritické infrastruktury ovlivňují nejvíce selhání dodávek energie, ztráta spojení a vnější příčiny. Zde se nabízí otázka, proč alespoň u energetických a komunikačních infrastruktur nevyžadují předpisy vyšší odolnost vůči vnějším příčinám.



Obr. 74. Provázanosti infrastruktur vedoucí k selhání dalších infrastruktur dle [386].

Příkladem velkého výpadku infrastruktur je např. výpadek dodávek elektřiny, který postihl 40 tureckých regionů dne 31. 3. 2015 [387]. V důsledku toho začal kolaps veřejné dopravy (v

Istanbulu a v Ankaře nejezdilo metro), lidé zůstali dlouhé hodiny uvěznění ve výtazích, byly zavřené obchody, byly přerušeny dodávky vody a spojení.

Na základě přístupu All-Hazard-Approach [8] i údajů z předchozích kapitol, které se opíraly především o výsledky z [1,2,5,10,11] je třeba sledovat škodlivé jevy všeho druhu, tj. živelní pohromy, lidský faktor (chyby fyzické, organizační i úmyslné), technická selhání daného systému i systémů jiných, se kterými je daný objekt propojen nebo je závislý na jeho výsledcích, selhání řídících systémů vyvolané chybou automatiky řízení (poškození PC, chybný software, špatná údržba), narušení spojení mezi řídicím systémem a řízenými systémy, selhání ochranných systémů (fyzických, technických i kybernetických). Přičemž je pravdou, že některé jevy jako elektromagnetické záření mající původ v kosmickém prostoru, anebo v technologiích aplikovaných člověkem vystupuje jako významný zdroj rizika právě u kybernetických systémů závislých na dálkovém přenosu dat. Jejich existence a dopady se podcenily nebo vůbec neuvažovaly v zadávacích podmínkách.

Databáze havárií a selhání technických objektů a infrastruktur analyzované výše, ukazují, že v každém typu dosud vytvořených technických děl (doly, kosmodromy, sklady, překladiště, přehrady, průmyslové a dopravní stavby, nemocnice atd.) se havárie nebo selhání již vyskytlo; v některých typech (chemický a petrochemický průmysl) častěji, jinde méně častěji. Příčiny byly jak vnější a vnitřní podmínky, tak lidský faktor.

Znalosti uvedené výše shrnuté v [1,10,11] i zkušenosti ukazují, že pro zajištění bezpečnosti technických děl ve smyslu socio-kyber-technickém je třeba v každém technickém díle mít

- správně nastaven systém spolupráce uvnitř i vně,
- personál pro zvládání nouzových situací,
- rezervní komponenty, systémy, materiál, technika a finance pro zvládání kritických situací,
- bezpečnostní, nouzové (a to včetně plánování kontinuity kritických objektů) a krizové plánování.

Předmětné nástroje musí být vytvořeny za pomoci systémového myšlení, inženýrských postupů zacílených na bezpečnost a kultury bezpečnosti.

Postup pro technické dílo: stanovit aktiva – vnější (veřejná) + vnitřní (fyzická / technická, kybernetická, personální, organizační, ekonomická); zajistit fyzickou ochranu - technická (plot, senzory,..); zajistit fyzickou ostrahu a režimová opatření a sestavit plán řízení rizik.

5.12.5. Řízení rizik na úrovni procesů v provozech infrastruktur

Jelikož procesy spojené s provozem infrastruktur jsou méně nebo více provázané, tak je nelze jednoduchým způsobem řídit. Podle postupů inženýrství rizika je třeba identifikovat konflikty a určit pravidla pro jejich řešení [26]. Pro řešení možných selhání či havárií zpracovat předem místně specifické plány řízení rizik ve formátu, který je uveden v předchozích odstavcích.

Na základě výše uvedených znalostí a zkušeností je třeba v plánu řízení rizik konkrétní infrastruktury zajistit způsob vypořádání poruch a příslušné odpovědnosti v jednotlivých vrstvách systému řízení bezpečnosti:

1. V oblasti celé infrastruktury jde především o zajištění zvládnutí:
   - slabin v zabezpečení vůči vnějším vlivům,
   - výskytu vnitřních náhodných poruch systému,
   - výskytu vnitřních systémových poruch zařízení,
   - poruch v procesech, lidských chyb, nedostatku zdrojů,
   - konfliktů mezi požadavky na bezpečnost a zabezpečení,
   - chybné nebo nedostatečné identifikace ovlivňujících činitelů,
   - chybná práce s riziky, volba metody, definice stupnic, ohodnocení rizik,
   - neodpovědnosti, nekompetence, závislosti a nedůvěryhodnosti řešitelských subjektů.

2. V oblastech, kde jsou nadřazené systémy propojeny toky či vazbami s podřízenými či vedlejšími systémy 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,
   - poruchám okolních systémů a realizaci relevantních pohrom.
3. V oblastech propojení mezi jednotlivými vrstvami systému řízení bezpečnosti 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,
   - nedodání vstupní informace.
4. Na rozhraní infrastruktury s okolním prostředím jde o zabránění nepředvídatelným událostem a útokům:
   - změna podmínek pro provoz ze strany státu,
   - úmyslná poškození,
   - cílené útoky.

5.12.6. Zásady obnovy důležitých technických infrastruktur z pohledu ochrany obyvatelstva

Jestliže mluvíme o obnově, tak musíme mít vždy na paměti, že nikdy po pohromě nejsme schopni provést akce tak, abychom dosáhli stejného stavu jako před pohromou; dosáhneme vždy nového stavu, který vyhovuje více či méně požadavkům řídícího subjektu. Pro řešení praktických úkolů je velmi důležité chápání obnovy infrastruktury, protože právě ono určuje způsoby stanovení, řízení a vypořádání rizik. Postupy obnovy i jejich softwarové podpory se liší: způsobem hodnocení (přijímání) rizika, posuzování a zvládání rizika; metodologií rizikové analýzy a operačního výzkumu; nástroji řízení bezpečnosti včetně nástrojů krizového managementu; specifickými zvláštnostmi kybernetické infrastruktury; hrozbou konvenčního a nekonvenčního terorismu; způsobem určování priorit zranitelnosti systému; a povědomím obyvatelstva a vlastnostmi post-moderní společnosti.

Důvody pro stanovení kritických prvků, kritických procesů, kritických funkcí, kritických částí infrastruktury a kritických technologií v území jsou dány požadavkem na snížení rizik pro lidský systém z pohledu bezpečí a rozvoje lidí v nejširším slova smyslu, tj. požaduje se integrální bezpečnost. Jde o snížení míry zranitelnosti (zvýšení odolnosti) klíčových elementů území chápaného jako lidský systém, které jsou zásadní pro existenci společnosti na všech úrovních organizace a státní správy, zajištění funkčnosti životodárných systémů a racionální ochranu obyvatelstva.

Ochrana životně důležitých infrastruktur je kodifikována zákonem č. 240/2000 Sb., o krizovém řízení. Pro zajištění bezpečnosti území, tj. dennodenního života lidí a jejich přežití při kritických situacích způsobených živelními a jinými pohromami včetně selhání infrastruktur v lidském systému do řízení bezpečnosti území nutně patří obnova životně důležitých infrastruktur po pohromách [2]. To znamená, že obnova infrastruktur zaujímá významné místo v ochraně obyvatelstva.

Obnova je v odborné literatuře a v právních dokumentech chápaná jako zajištění návratu do stabilizovaného stavu a nastartování dalšího rozvoje v rozumném čase a za přijatelných nákladů [2]. Od konce 70 let je ve vyspělém světě základní součástí strategického řízení území (obec, kraj, stát, EU), které je zacílené na bezpečí a udržitelný rozvoj lidí [388]. V oblasti řízení České republiky chybí strategie obnovy a její zásady. V důsledku toho se každá obnova provádí

systémem případ od případu (ad hoc), což má za následek, že jednou se problém řeší jedním způsobem a jindy způsobem zcela protichůdným, a to v závislosti na znalostech a možná i momentální náladě příslušného vedoucího pracovníka. Popsaný přístup je zcela v rozporu se zásadami moderních teorií řízení (managementu) a někdy dokonce může vyvolávat pocity, že jde o záměrné poškozování občanů, společnosti i celého státu. To znamená, že scénáře obnovy, zásady pro obnovu obsahující preventivní opatření, aby se pohromy či jejich nejkrutější dopady v budoucnu buď neopakovaly anebo se opakovaly v mírnější formě, provázání obnovy s rozvojem území apod. upraveny jednotně nejsou.

S ohledem na výše uvedený cíl obnovy, každá obnova, tj. i obnova infrastruktur, musí být prováděna na základě určitých zásad, které nebudou zvyšovat zranitelnost chráněných aktiv (zájmů) státu ani vůči pohromě, po které se obnova provádí a ani vůči předvídatelným možným pohromám dalším. Z hlediska rozvoje je třeba obnovu nechápat jen jako prostou obnovu poškozeného majetku a rozvrácených funkcí, ale je ji třeba dělat podle takového scénáře, aby v budoucnu dopady stejně silné pohromy byly menší. Proto je třeba vycházet z hodnocení ohrožení od pohromy, analýzy rizik a přihlížet k požadavkům udržitelného rozvoje a k principu předběžné opatrnosti – tj. používat nástroj řízení bezpečnosti [1,2,5,10,388]. Je si třeba uvědomit, že v případech, kdy není obnova přesně vymezena zákonem, lze obnovu jakékoliv položky, tj. infrastruktury, chápat rozdílně. Možná chápání obnovy infrastruktury jsou: obnova infrastruktury je prostá oprava poškozených prvků či síťových položek infrastruktury; obnova infrastruktury je proces, kterým se vytvoří odolnější infrastruktura vůči jevu, který ji poškodil (jevem se myslí jak důsledky přirozeného stárnutí, tak i povodeň a jí podobné jevy); obnova infrastruktury je proces, kterým se vytvoří odolnější infrastruktura vůči všem možným pohromám, tj. aplikuje se tzv. All-Hazard-Approach [2,8] a přitom se zvažuje jen aktivum infrastruktura (zde je několik rozdílných postupů – např.: zvažují či nezvažují se organizační havárie; zvažují či nezvažují se teroristické útoky na kritické prvky; atd.); a obnova infrastruktury je proces, kterým se vytvoří odolnější infrastruktura vůči všem možným pohromám, tj. aplikuje se tzv. All-Hazard-Approach [2,8] a přitom se zvažují veřejná aktiva a aktivum infrastruktura (zde je několik rozdílných postupů, např.: zvažují či nezvažují se organizační havárie; zvažují či nezvažují se teroristické útoky na kritické prvky; atd.).

Je nutno také přihlédnout ke skutečnosti, že svět je dynamicky proměnný, což v daném případě znamená, že zdroje, síly a prostředky potřebné na obnovu jsou proměnné. V případě kritických objektů a infrastruktur, na kterých závisí životy lidí se ve strategických materiálech vyspělých zemí a velkých zajišťoven (Swiss Re, Munich Re) doporučuje obnovu a rozvoj nezastavovat, když není dostatek zdrojů, sil a prostředků, ale přejít na variantu realizace, která je méně nákladná a prodlouží realizaci. Aplikovat řízení infrastruktury, které umí daný způsob, je náročné jak na sestavení věcných podkladů (musí se umět dobře pracovat s nejistotami náhodnými i epistemickými), tak na tvorbu jejich software, která podporují jejich aplikaci.

Pokyny pro sestavení plánu obnovy infrastruktury

Základem provedení kvalitní obnovy infrastruktury je sestavení kvalitního plánu obnovy ve formě procesního modelu, jehož realizace je zajištěna po stránce technické, finanční, personální i manažerské, ke kterému se sestrojí softwarové nástroje odpovídající odbornému konceptu. Dle návrhů v pracích shrnutých v [365,388] tvorba plánu obnovy je obvykle chápaná jako vícestupňový proces. Na jeho základě jsou metodou analogie zpracovány následující pokyny pro plán obnovy infrastruktury. Při jeho tvorbě musí být kladen důraz na následující tři kroky: identifikace funkcí a cílů infrastruktury; prioritní položky pro plnění funkcí infrastruktury; a tvorba plánu obnovy infrastruktury.

V prvém kroku jde o identifikaci těch aspektů, které jsou nutné pro udržení / zachování činností infrastruktury po výskytu pohromy a pro přechod z nouzového provozu na provoz normální. Aby se zmírnily škody a / nebo ztráty způsobené snížením nebo zastavením provozu,

tak se vyžaduje, aby předem byly provedeny následující činnosti: identifikace týmu, který bude řídit provádění obnovy infrastruktury; definování a vysvětlení rolí členům týmu; vytvoření souboru nouzových zpráv, které budou použity pro uvědomění členů týmu a dalších zúčastněných; definování postupů pro řízení základních / životně důležitých funkcí infrastruktury; určení alternativních požadavků na budovy a jiné části infrastruktur; zabezpečení záložních / alternativních lokalit pro provoz základních / životně důležitých funkcí infrastruktur; stanovení časových harmonogramů pro obnovu základních / životně důležitých funkcí infrastruktur; odhady a dokumentace ztrát / nákladů na obnovu infrastruktur; zabezpečení nezbytné dokumentace; a definice strategií pro plán obnovy a pro plán na řízení škod, který musí být jeho nezbytnou součástí.

V druhém kroku jde o stanovení základních položek, které jsou nezbytné pro provoz infrastruktur. Tento krok je místně specifický, tj. závisí na tom, z jakých prvků a sítí se infrastruktura skládá, jak jsou uvedené položky odolné a robustní. Jde o stanovení kritických míst, služeb a funkcí v infrastruktuře. Kritická místa v technologických objektech jsou místa, kde probíhají technologické procesy, pro které platí specifické předpisy zajišťující bezpečnost za normálních, abnormálních a kritických podmínek. Kritická místa v objektech jsou schodiště, dveře, východy, výtahy, telefonní a komunikační centrály, elektrické přípojky, topení, bojlery, kamna, sklady, sklady odpadků, střechy. Ze systémů jsou to vnitřní a vnější osvětlení, systémy HVAC (rozvody zajišťující dodávky základních (životodárných) produktů), požární a nouzové detektory včetně sprchových systémů, varovacích a oznamovacích systémů, nouzových elektrických generátorů a bezpečnostních systémů včetně zámků, poplašných zařízení a řídicích systémů. Všechny uvedené položky a systémy musí být vyhodnoceny z hlediska jejich dostupnosti, přístupu a spolehlivosti při pohromě předem. Také musí být vyhodnoceny dopady jejich selhání na zaměstnance a na provoz při a po pohromě.

Kritické služby (dodávky energií, vody, chladících médií apod.), provozy a výrobky při výskytu pohrom souvisí s problematikou bezpečnosti, zdraví, detekce a prevence ohrožení, nouzovým plánováním včetně uvědomění a přemístění, obnovou majetku a výrobků, telekomunikacemi, obnovou výroby, zvládnutím nouzové situace, bezpečím, prevencí a dokumentací ztrát, předcházením nouzovým situacím a s plánováním řízení likvidace škod. Přestože ne všechny uvedené faktory souvisí s kontinuitou provozu, je nutné, je zvážit při volbě strategií alternativ provozu pro případ výskytu pohromy, která vyvolá přerušení provozu. To znamená, že jsou položkami plánu obnovy.

Struktura plánu obnovy z předmětného pohledu je následující: stanovení pravděpodobnosti výskytu pohromy; stanovení potenciálních dopadů pohromy; a identifikace omezení v dostupnosti zdrojů. Základním úkolem je: předcházet zraněním a ztrátám na životech lidí; zajistit bezpečnost zaměstnanců a ostatních zúčastněných; a předcházet ztrátám na majetku a na schopnosti podnikat. Prodlužování přerušení funkce infrastruktury má neblahý vliv na přežití podnikatelského subjektu i lidí v území. Proto se důkladně zvažují všechny možné pohromy, jejichž zdroje leží vně i uvnitř infrastruktury.

Pro potřeby provozovatelů infrastruktur je třeba zpracovat speciální kontrolní seznamy pro identifikaci vnitřních zdrojů pohrom. Identifikace vnějších zdrojů pohrom závisí na: fyzické poloze infrastruktury, tj. jejich prvků a sítích; místních klimatických podmínkách; a na blízkosti a dostupnosti bezpečných míst a míst, ze kterých se odezva na pohromu a obnova řídí. Všechny uvedené faktory se posuzují z pohledu, zda daný faktor nebo některé jeho kombinace zvyšují četnost výskytu pohromy nebo eskalují dopady pohromy. Do identifikace vnitřních zdrojů a schopností patří problémy spojené s personálem, zařízením, objekty, organizační schopností (výcvik, evakuační plány apod.), záložními systémy (komunikace, výroba, nouzové zdroje energie, vody atd.) atd. V uvedených souvislostech je třeba rozlišovat dva případy, a to pouze jedna část infrastruktury v území je postižena pohromou nebo více částí infrastruktury je postiženo pohromou. Zatímco v prvním případě je předpoklad, že lze počítat s činností všech

hasičů, policie, zdravotníků a dalších nouzových služeb, tak v druhém případě je třeba více spoléhat na vlastní síly. Proto je nouzové řízení u provozovatelů infrastruktur kritickou činností, která by se měla především soustřeďovat na prevenci pohrom, kterým mohou zabránit a na zmírňování dopadů pohrom, kterým zabránit nemohou. Provozovatelů infrastruktur musí pomáhat odborné úřady veřejné správy, jakými jsou dozorné a inspekční orgány, protože pro zvládnutí pohrom je nutné kvalifikované řízení založené na správném vyhodnocení odborných fakt, a to mohou poskytnout jen odborníci. Pomoci musí také pojišťovny, a proto legislativa musí specifikovat jejich roli.

V třetím kroku jde o vlastní tvorbu plánu obnovy infrastruktury. V jeho rámci je nutno zvážit problémy lidí, budov, sítí i možné nepředvídané události. Tj. je třeba respektovat, že: naděje zraněných na přežití závisí na kvalitě / kvalifikovanosti zvládnutí rozsahu a krutosti pohromy, která se vyskytne, a proto v plánu obnovy musí být identifikovány jak zdravotní služby, tak pomoc psychologů předem; pro potřebu zajištění nouzového provozu prvků a sítí infrastruktur je třeba předem predikovat rozsah fyzického poškození prvků a sítí infrastruktur a systémů, které zajišťují zásobování vodou, elektřinou, jídlem, kanalizaci apod.; pro zajištění nouzového řízení infrastruktury je nutné zálohování telefonů, telekomunikací, PC apod.; pro nepředvídané události je třeba mít plány nouzových činností sestavené s ohledem na zákazníky a obyvatele území.

Plánování pro nepředvídané situace je proces tvorby místně specifických strategií, které jsou nutné pro zajištění kontinuity základních funkcí infrastruktur. Zajišťuje identifikaci preventivních opatření a činností, které musí být provedeny k tomu, aby se minimalizoval výskyt pohrom a aby se minimalizovaly dopady pohrom na infrastrukturu a její provoz. Při tvorbě místně specifických strategií musí být určena dále zmíněná klíčová fakta: velikost a rozsah možných pohrom; podstata a cíle provozu v místě; časový rámec činností; a náklady. Plánovací tým musí nejprve určit dopady možných pohrom na infrastrukturu, a to zvláště specifické dopady na její provoz a její činnosti. V souvislosti s tím musí být určena opatření, která musí být provedena k tomu, aby se zabránilo výskytu pohrom či aby se zmírnily dopady pohrom. S ohledem na praktické zkušenosti autorka práce doporučuje rozvážit řetězec událostí, které nastanou při přerušení funkce určité infrastruktury (tj. řetězec selhání ostatních infrastruktur a sekundární dopady na veřejná aktiva).

Na základě zkušeností z praxe shrnutých v [1,10,12] je třeba při všech rozhodnutích zvažovat náklady spojené s aktivací plánů pro nepředvídané situace a fakt, že pro obnovu je třeba vybrat takové varianty obnovy, které jsou „cost-effective“. To je v souladu s dalšími pracemi, ve kterých se požaduje, aby náklady na obnovu byly přijatelné, tj. obnova se neprovádí v případech, kdy náklady na obnovu se vyrovnají hodnotě obnovované položky nebo ji dokonce převýší.

V procesu specifikace nákladů na obnovu se musí nejprve identifikovat a určit priority ve funkcích a provozech infrastruktury. Musí být zváženy: dopady možných pohrom (škody, ztráty) na funkce, které jsou určené jako podstatné pro podnik / území; a maximální doby, po které mohou probíhat alternativní postupy vedoucí k zajištění kontinuity činnosti infrastruktury. Z důvodu vnitřní provázanosti faktorů (zvláště těch, které jdou napříč celým systémem) je třeba určit různé varianty postupů. Úloha státu / veřejné správy při obnově infrastruktur spočívá v tom, že musí prosadit, aby veřejné zájmy byly upřednostněny před zájmy soukromými a že se musí poskytnout asistenční služba potřebným, tj. postiženým pohromou.

Prevence ztrát při obnově znamená: vytvořit koncepci prevence ztrát při obnově; identifikovat a vyhodnotit všechny možné pohromy a jejich možné dopady na infrastrukturu; určit priority obnovy; a vytvořit skupiny programů, které minimalizují možné ztráty. Z důvodu použitelnosti v praxi se požaduje, aby koncepce prevence ztrát při obnově a koncepce řízení obnovy byly písemné a aby se jednalo o skutečné plány odezvy na zvládnutí vzniklé situace a ne o pouhé slohové cvičení. Požaduje se, aby: identifikovaly všechny oblasti prevence ztrát;

identifikovaly klíčové úrovně odpovědností a pravomocí pro tvorbu a implementaci programů na prevenci ztrát v každé identifikované oblasti, která bude postižena dopady pohromy a přitom je klíčovou pro provoz infrastruktury; a uvedly vymezení a postupy vynucovacích procedur a / nebo disciplinárních postupů pro odstranění nesouladů v procesech obnovy infrastruktur.

Pro vytvoření koncepce prevence ztrát by odpovědní lidé měli na svém úseku identifikovat a vyhodnotit všechna možná ohrožení předem. Mnoho dopadů pohrom vzniká jako důsledek chování lidí (viz technologické havárie, organizační havárie, požáry atd.), a proto musí být vzat v úvahu lidský činitel. Z pohledu iniciace dalších dopadů nebo eskalace očekávaných dopadů je třeba zvážit velmi mnoho oblastí, např. hasební technika, sváření, údržba, stavba, úklid, kouření, dozor, pojištění, výcvik personálu, hodnocení nebezpečných látek. S ohledem na lidský faktor je také třeba zvážit zranitelnosti v systému odpovědností v organizaci provozovatele infrastruktury. Protože v této oblasti je ještě mnoho neznámých, tak se doporučuje, aby se během obnovy pořizovaly záznamy o pracích, činnostech, opatřeních a jejich účinnosti a řízení, které budou tvořit zdrojový materiál pro vylepšení řízení při budoucích pohromách.

Prevence na úseku infrastruktur je chápána ze dvou pohledů, a to dlouhodobá jako technická opatření v projektu, výstavbě a provozu, a krátkodobá jako opatření při bezprostředním nebezpečí vzniku pohromy (to nelze např. u zemětřesení). Okamžitá prevence nebo bezprostřední ochrana se provádí v postiženém místě také při průběhu pohromy až do jejího odeznění, zde jde o zabránění eskalací situace (např. zhasnutí otevřeného ohně, vypnutí plynu či elektřiny, uzavření přívodů vody, nebezpečných látek, odstavení technologií (zastavení zpracovatelských postupů), použití ochranných pomůcek a prostředků apod.).

Cílem inspekce infrastruktur po pohromě je zajistit bezpečí lidí, bezpečný návrat zaměstnanců do provozů. Při ní se klade důraz na: kontrolu provozuschopnosti hasících systémů a zařízení; posouzení škod na základech budov; škody způsobené odpadky a úlomky; a na záznamy a dokumenty o škodách.

Aby se zamezilo ztrátě zkušeností z odezvy a obnovy a aby se vytvořil materiál pro poučení, je třeba vytvořit záznam o obnově po pohromě, který zahrnuje: popis pohromy; hodnocení škod; plánování a vlastní provedení záchrany; odstranění a zabalení poničených záznamů a dat; uložení záznamů a dat; obnova záznamů; a skladování.

Dobře sestavené plány obnovy nejen redukují náklady na obnovu, ale také minimalizují dopady na funkce, které jsou podstatné pro kontinuitu podniku / organizace / území. V plánech obnovy technologických objektů infrastruktur musí být zváženy dále uvedené činnosti, které jsou možné při průběhu obnovy: oprava a přemístění zařízení technologických objektů infrastruktur; přesun provozů technologických objektů infrastruktur na alternativní místo; a zajištění dočasných kontraktů ve věci provozu infrastruktur, aby nedošlo ke ztrátě trhu, plnily se závazky vůči objednatelům i závazky vůči občanům.

V plánu obnovy infrastruktur je třeba zvážit, že ne všichni pracovníci řízení infrastruktur jsou vždy schopni v řízení pokračovat, a proto pro kontinuitu řízení infrastruktur je třeba alternativně stanovit postupy pro: zajištění řetězu povelů, tj. předávání příkazů; úpravu nadřazenosti a podřízenosti klíčového personálu; a řídícího pracoviště.

Další plány provozovatele infrastruktury či objektu technického díla

Plánování kontinuity infrastruktury je proces, který má za úkol navrhnout a implementovat opatření a postupy, které umožní provozovateli infrastruktury reagovat na pohromu tak, aby kritické činnosti infrastruktury byly zachovány s plánovanou úrovní přerušení. Tj. plánování kontinuity činností je proces proaktivního plánování preventivních (je-li to možné) a reaktivních opatření na pohromu tak, aby se minimalizovaly ztráty na úroveň, kterou si provozovatel kritické infrastruktury může dovolit.

Pro případ, že pomocí plánu kontinuity provozovatel infrastruktury nezvládne nouzovou situaci, se vytváří krizový plán, který obsahuje: kontakty na odpovědné činitele veřejné správy a výkonných složek, kteří zajistí pomoc při zvládnutí dopadů pohromy na chráněná aktiva; předpisy pro zaměstnance, ve kterých je stanoveno, co mají dělat; postup pro jednání s médii; připravené informace pro veřejnost.

Při plánování obnovy infrastruktur je nutno zvážit, že náklady na obnovu závisí i na době trvání obnovy. Při dlouhotrvající obnově jsou velké dopady na společnost. Je třeba také vybudovat systém, aby obnova navazovala na odezvu. K danému účelu je třeba zpracovat zvláštní plán, který má 4 základní části:

1. Stanovení týmu, který propojí činnosti odezvy a obnovy v oblasti technické, právní, organizační, finanční, vzdělání, ochrany zdraví a bezpečí a vytvoří několika úrovňovou strukturu řízení.
2. Vytvoření programu řízení nouzové situace, tj. analýza možných pohrom a velikosti jejich dopadů na chráněné zájmy a posouzení schopnosti disponibilních sil, prostředků a zdrojů zvládnout stanovené dopady na chráněné zájmy (tj. co zvládnou opatření v protipožárních plánech, evakuačních plánech, plánech na ochranu zdraví, bezpečnostních plánech, pojištění apod.) s uvážením nejprve vnitřních sil, zdrojů a prostředků (personál, specifické pomůcky, zařízení a prostředky, zálohování, organizační postupy) a když tyto jsou nedostatečné, tak s využitím vnějších zdrojů (veřejná správa, hasiči, zdravotní ambulance, technické služby, spolupracující organizace, občané apod.) a vyhodnocení jeho spolehlivosti s ohledem na možné problémy plynoucí z historických faktorů, geografických faktorů, technologických faktorů, lidských chyb, selhání dodávek jídla, pití, pohonných hmot, elektřiny apod.
3. Zpracování plánu koordinace odezvy a obnovy, tj. specifikace činností odezvy a činností obnovy, stanovení jejich propojení a zpracování příslušných postupů a dokumentů, seznam zdrojů, na nichž závisí odezva, obnova i jejich propojení, dále pak stanovení cílů a priorit v činnostech, stanovení požadavků a harmonogramů na výcvik, projednání s vnějšími orgány, schválení a distribuce plánu.
4. Implementace plánu (zapracování do provozních dokumentů, cvičení, výcviku, drilu apod.) včetně monitoringu účinnosti plánu a způsobu provádění změn k lepšímu.

Nouzové řízení je pak chápáno jako proces přípravy na zmírnění, odezvu a obnovu pro případ výskytu pohromy nebo nouzové situace. Zahrnuje: usměrnění a řízení odezvy tak, aby se situace zvládla s přiměřenými silami, zdroji a prostředky, tj. upravuje strukturu řízení, seznam povelů, pokyny pro činnost operačního střediska, zásady spolupráce a komunikace; zajištění bezpečí lidí (nezávadné jídlo a pití, ochrana životů a zdraví, evakuace, úkryty, ochrana majetku); a vlastní odezvu a obnovu (oblast technická, finanční, právní, personální, bezpečnostní – např. ochrana nezničeného majetku).

5.12.7. Postupy pro ochranu a bezpečnost kritické infrastruktury

Kritická infrastruktura je z hlediska Směrnice rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu [389] definována jako: „Prostředky, systémy a jejich části nacházející se v členském státě, které jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení nebo dobrých hospodářských či sociálních podmínek obyvatel a jejichž narušení nebo zničení by mělo pro členský stát závažný dopad v důsledku selhání těchto funkcí“. Dle zdroje [11] lze jinými slovy kritickou infrastrukturu definovat jako systémy různé povahy (technické, organizační, kybernetické, územní, vzdělávací atd.), které mohou mít vliv na fungování ekonomiky, státu a na zvládání nouzových a kritických situací.

Objektem neboli prvkem kritické infrastruktury se dle zákona č. 240/2000 Sb., o krizovém

řízení se rozumí stavba, zařízení, prostředek nebo veřejná infrastruktura, určená podle průřezových a odvětvových kritérií. Z hlediska drážního systému je vhodné za objekt kritické infrastruktury považovat například nádraží, stanice metra, významné mosty či tunely, technologická zařízení a informační, materiálové, energetické toky v systémech a to podle metodiky určení kritičnosti objektů dle zdroje [10].

V reálném světě nastávají jevy, nebezpečné události zvané pohromy, které mohou ovlivnit nejen správnou funkci prvku kritické infrastruktury, ale taktéž mohou ohrozit zdraví a majetek lidí. Ochrana zdraví a majetku lidí je předním zájmem základní funkce státu zakotvené v Ústavě České republiky. Každou pohromu lze ve vybraném území klasifikovat na základě velikosti dopadů na chráněná aktiva, včetně objektů kritické infrastruktury a četnosti výskytu dané pohromy v území. Podle kategorie velikosti možných dopadů pohromy se provádí příslušná opatření [2,10].

Pro zajištění bezpečnosti je nutné volit proaktivní přístupy konkrétním řízením bezpečnosti, které vyjednávají s riziky prostřednictvím prevence, anebo alespoň zmírňují jejich dopady při jejich realizaci. Pro zvládnutí nouzových situací se připravují plány odezvy na pohromu, plány obnovy po pohromě a zajišťuje se monitoring. Aby se zajistilo bezpečné území, v našem případě Česká republika, je zapotřebí zavést tzv. vrcholové řízení bezpečnosti založené na principu integrálního rizika a All-Hazard-Approach (přístup zvažování všech možných ohrožení) [1,2,8,11].

Vrcholové řízení bezpečnosti je základním kamenem řízení a spočívá na identifikaci a analýze rizik mezi různými oborovými odvětvími. Analýza a hodnocení rizik počínaje v nejvyšší vrstvě na úrovni celého státu umožní stanovit prioritní rizika a chráněná aktiva státu, a též míru kritičnosti objektů kritické infrastruktury. Výstupy z řízení bezpečnosti vyšší vrstvy slouží jako vstupy pro řízení bezpečnosti na nižších úrovních, tj. konkrétního území, kritické infrastruktury a vybrané kritické objekty. Vrcholové řízení bezpečnosti na úrovni státu, které dle zdroje [11] zahrnuje:

1. Určit seznam relevantních živelních a jiných pohrom.
2. Provést analýzu poznatků a zkušeností spojených s každou relevantní pohromou.
3. Provést hodnocení dopadů každé sledované živelní či jiné pohromy.
4. Provést ocenění resp. klasifikaci sledované živelní či jiné pohromy.
5. Regulovat činnosti v dané oblasti (tj. řízení bezpečnosti v dané oblasti s cílem minimalizovat a zvládat dopady pohromy, zavést preventivní opatření, plány odezvy a obnovy na pohromu).
6. Soustavně ověřovat přijatou metodiku vrcholového řízení bezpečnosti.

Výstupem vrcholového řízení bezpečnosti je stanovení relevantních pohrom pro dané území a určení kritičnosti objektů kritické infrastruktury z hlediska celého státu a krajů jakožto chráněná aktiva státu.

Nižší vrstvou řízení bezpečnosti je řízení bezpečnosti pro konkrétního území využívající výstupů vrcholového řízení státu, které by mělo dle zdroje [10] pracovat s integrálním rizikem. Integrální riziko zahrnuje více chráněných aktiv včetně života, zdraví a bezpečí lidí, majetku a veřejného blaha, životního prostředí i technologií a infrastruktur a zahrnuje i vliv propojení mezi uvedenými chráněnými aktivy (interdependences). Aplikace All–Hazard-Approach [8], tj. přístup zvažování všech možných ohrožení, má za úkol zajistit zvládnutí dopadů na veškeré relevantní pohromy.

Kritické technologické objekty či objekty kritické infrastruktury analyzované v popsaných vyšších vrstvách řízení bezpečnosti by měly splňovat určitá kritéria a požadavky bezpečnosti, která zajistí vyšší bezpečnost objektů samotných a také bezpečnost okolí a vazeb mezi okolními systémy. Řízení bezpečnosti objektů, které nebyly identifikované jako kritické, je zajištěna obecnými nebo oborovými předpisy (stavební zákon, systémy jakosti, drážní normy a předpisy, jiné oborové normy a podobně).

Při specifikaci ochranných opatření pro kritickou infrastrukturu si je třeba uvědomit, že útok na řídicí systém kritické infrastruktury nemusí vyvolat ihned fyzické zničení, ale vyvolá, že řídicí systém neplní funkce, ke kterým je určen (používá se pojem „odepření služby“), což mnohdy má v bližší nebo vzdálenější budoucnosti mnohem větší dopady než okamžité fyzické zničení, protože vyvolá nebo může vyvolat kaskádu nežádoucích jevů.

Odezva v tomto případě není snadná, protože není snadno zjistitelná příčina. Abychom zařídili, že systém bude plnit jen žádoucí funkce, tak se musí data zálohovat, činnost systému monitorovat a neustále porovnávat, zda řídicí systém má žádoucí data. Příkladem je výpadek dodávek elektrické energie v srpnu 2003 v USA a Kanadě a poučení, které z toho vyplynulo, tj. zálohování kybernetických systémů [162].

Oblast řízení v době automatizace je nejcitlivější oblastí. Kybernetický útok tak jako každý jiný útok je neúčinnější, když využije zranitelné místo, tj. v případě IT citlivé informace. Ochranu citlivých informací lze zajistit buď tak, že citlivé informace nejsou veřejně přístupné (kybernetická bariéra nestačí, musí být i fyzická) anebo tak, že se zašifrují moderními metodami kryptologie. V USA hodnotí teroristické útoky na řídicí systémy jako útoky s největší nebezpečností. Proto zabezpečení ochrany řídicích systémů považují za nejvýše důležité. Výzkumné ústavy v Německu a v USA se specializují na poznání a implementaci opatření proti dopadům teroristických útoků na kybernetické (řídící) systémy, např. ISTS (Institute for Security Technology Studies) v Hannoveru a v Darthmouthu [12].

Pro zajištění lidské bezpečnosti je nutné zvažovat nejenom přímé dopady, ale i dopady zprostředkované složitou sítí vazeb v lidském systému. V tomto konceptu musí být také zvažována kritická informační infrastruktura. Problémy spojené s informační infrastrukturou jsou komplexní, protože každý informační systém se skládá z prvků a sítí a ochrana sítí je vždy komplikovaná, viz ochrana rozvodů elektřiny, vody apod. Informační infrastruktury jsou součástí mnoha systémů a tvoří podsystémy ostatních infrastruktur, které patří do lidského systému. Z hlediska jejich ochrany musíme zabezpečit, aby spolehlivě pracovaly nejen za normálních a abnormálních podmínek, které jsou pokryty jejich projektem, ale i za nouzových a speciálně kritických podmínek. Pozornost se musí soustředit, jak na kritické informační infrastruktury, které mají přímé dopady na životy, zdraví a bezpečí lidí, ale i na ty, které mají nepřímé dopady nebo které mohou eskalovat dopady pohrom na životy, zdraví a bezpečí lidí.

S ohledem na velkou rozmanitost typů informačních infrastruktur je nutné pro lidskou bezpečnost a pro bezpečnost lidského systému zmapovat situaci a rozpoznat problémy, tj. určit:

- za jakých podmínek informační infrastruktury selžou a proč?
- které dopady mohou způsobit selhání informačních infrastruktur na životy, zdraví a bezpečí lidí?
- která opatření mohou zabránit selhání informačních infrastruktur nebo která opatření mohou zmírnit dopady selhání informačních infrastruktur na životy, zdraví a bezpečí lidí?

Problémy spojené s ochranou kritické informační infrastruktury se zmapovaly v rámci projektu EU nazvaného CI2RCO [12].

Občané členských států EU očekávají, že národní vlády i EU zajistí bezpečí pro kritické infrastruktury. Proto EU vydala právní předpisy, které obsahují minimální strategie na ochranu infrastruktury a zapadají do různých koncepcí EU. Plán boje EU proti terorismu zpracovaný po útocích v Madridu byl upraven po útocích v Londýně v červnu 2005. Dne 12. července 2005 Rada EU přijala v tomto smyslu deklaraci, ve které je mimo jiné zdůrazněna role standardů na ochranu kritické infrastruktury napříč zeměmi EU. Ochrana kritické infrastruktury je koordinována DG pro spravedlnost, svobodu a bezpečí kvůli tomu, že tato DG je pověřena prevencí proti terorismu, ale věcně patří i do DG pro dopravu a energetiku a do DG pro informační společnost. Přijaté směrnice a nařízení pro ochranu kritické infrastruktury jsou např.:

- The Universal Service Directive 2002/22/EC – pro zajištění integrity veřejné telefonní sítě při velkých pohromách.
- The e-Privacy Directive 2002/58/EC – pro zajištění bezpečnosti veřejných elektronických komunikačních sítí.
- Regulation 725/2004 – nařízení pro zajištění bezpečnosti přístavů.
- Regulation 884/2005 – nařízení obsahující pravidla pro bezpečnostní kontroly pro potřebu bezpečnosti letecké dopravy.
- Směrnice na regulaci vážných narušení v pohybech vlaků po EU.

Dne 24. 11. 2005 byla přijata tzv. Zelená kniha EU [86]. Tato studie upozornila na to, že v případě nebezpečí bude třeba v části nebo v celé EU přijmout společnou úroveň ochrany, tj. jistý soubor koordinovaných opatření. Navrhla rámec Evropského programu pro ochranu kritické infrastruktury (European Programme for Critical Infrastructure Protection – EPCIP). Cílem tohoto programu je definovat pojem kritická infrastruktura, určit klíčové principy pro ochranu kritické infrastruktury na úrovni EU, najít propojení na národní kritické infrastruktury, zřídit síť pro zajištění varování v oblasti kritické infrastruktury pro případ vážných narušení a selhání a instalovat monitoring kritické infrastruktury.

Náklady na infrastrukturu nejsou jen náklady na její projekt a výstavbu, zahrnují také náklady na její provoz, údržbu, opravy a modernizaci. Proto rizika spojená s každou infrastrukturou musí zahrnovat i rizika z právě uvedených oblastí a řízení území se musí s nimi umět vypořádat. Tj. je třeba hodnotit i rizika pohrom, která lze označit např. jako selhání finančního trhu a s nimi spojeného selhání financí na údržbu, provoz, opravy a modernizaci objektu kritické infrastruktury. Je to proto, že kritičnost infrastruktury roste také tím, že není řádná údržba a řádné opravy, v jejichž důsledku dochází k růstu zranitelnosti.

Protože nic není bezporuchové, tak musí být připraven plán obnovy infrastruktury, a to především kritické. Uvedený plán musí být proaktivní, správně vyhodnocen, mít transparentně vypořádaná rizika a obsahovat odpovědi na otázky:
- co udělat?
- jak to udělat?
- v jakém časovém intervalu?
- nezvýší to rizika pro jiné chráněné zájmy?

apod.

Otevřené problémy spojené s bezpečností kybernetické kritické infrastruktury jsou:
- stejné jako u jiných infrastruktur a u celé kritické infrastruktury, viz údaje výše,
- specifické pro kybernetickou kritickou infrastrukturu, které pramení z: neexistence standardů a norem, protože doba užití je krátká; a skutečnosti řešení jejich problémů je prováděno na nízké znalostní úrovni. Většinou se řeší dílčí úkoly, a to přístupem ad hoc, takže jednotlivá řešení nelze propojit na vyšší úrovni a hledat systémová proaktivní řešení problémů, jak je to běžné v ostatních oblastech, které jsou historicky známy a prošly určitým vývojem, který stanovil jejich vysoké standardy.

5.13. Řízení státu a bezpečnost technických děl

Na základě vize zajistit bezpečnou Evropu Evropská unie zavedla do hodnocení projektů, které by měla financovat ze svého rozpočtu specifická rizika, která se musí hodnotit. Jedná se o: stavebně-technologická a projekční rizika; kreditní rizika; tržní rizika; vnější rizika; provozní rizika; a rizika spojená s řízením a rozhodováním [5]. Celkem je třeba sledovat 55 dílčích rizik. Z pohledu sledované problematiky si pozornost zasluhují rizika zařazená do skupin:
- provozní rizika, která zahrnují rizika související se zařízeními (tj. riziko související se zařízením, se vstupy, tj. materiálem, spojené s údržbou, opravami, modifikacemi a

adaptacemi a s nízkou zůstatkovou hodnotou); s lidmi (tj. riziko související s neodpovídajícími pracovními silami, s nezastupitelností, s nedostatkem lidských zdrojů, pracovně právními spory a se selháním lidského faktoru); a s jednáním lidí (tj. riziko související s podvodným jednáním, s nelegálním jednáním, s bezpečností technologických systémů, s poškozením, krádeží apod.),

- vnější rizika, která zahrnují rizika politická (tj. riziko související s národní či mezinárodní situací, se selháním vlády a s nadnárodními povinnostmi státu), vyšší moc (tj. riziko související s přírodní pohromou rozměru katastrofy, s terorismem a s válkou) a ostatní vnější rizika (tj. riziko související se změnou legislativy jako změna daní, potřeba dodatečných povolení, s poklesem poptávky a se stávkou),
- rizika spojená s řízením a rozhodováním, která zahrnují rizika smluvní (tj. riziko související s odpovědností třetím stranám, se změnou smlouvy a s porušením obecně závazných předpisů) a ostatní rizika spojená s řízením a rozhodováním (tj. riziko související se strategickým rozhodnutím a s reputací).

Příkladem realizace politického rizika, které se nazývá „selhání vlády“, je finanční krize, která je důsledkem špatného řízení finanční oblasti státu, tj. aplikace špatného nebo žádného scénáře řízení finanční oblasti, nedodržování finanční disciplíny v důsledku zneužití pravomoci či korupce. Dalším příkladem předmětného selhání je vládnutí, ve kterém u všech rozhodnutí hraje hlavní roli korupce. Příkladem realizace rizika spojeného s řízením a rozhodováním je metylová aféra, která odhalila slabiny v legislativě, v konání odpovědných orgánů a nedostatečné spolupráce odpovědných orgánů. Její příčiny jsou: špatné vnímání (podcenění) rizika; nedostatečná kontrola; špatný dohled a legislativa; normy tolerující porušování předpisů apod.

Šetření provedená v rámci projektu Evropské unie FOCUS ukázala, že organizační havárie v EU i v členských státech jsou důsledkem použití špatných dat, špatných scénářů či špatných odhadů při rozhodování o věcech veřejných, korupce a zneužití pravomoci [19]. Proto závěry projektu doporučují EU zavést strategické, systémové a proaktivní řízení bezpečnosti, které bude respektovat veřejný zájem, dynamické změny podmínek a bude pod kontrolou občanů EU.

Jelikož řízení lidského systému i jeho podsystémů je značně závislé na chování lidí; jejich nesprávné chování vede k organizačním haváriím, tak je třeba věnovat pozornost způsobu řízení lidské společnosti. Proto byla provedena simulace možných dopadů dlouhodobého selhání státní správy na veřejná aktiva. Byla použita metoda What, If a data od 142 respondentů z veřejné správy, kteří řeší bezpečnostní otázky [12]. Jejich vyhodnocení ukazuje:

1. Možné dopady na životy a zdraví lidí: důsledky selhání služeb, které vykonávají veřejné sbory, např. Policie ČR, HZS a ZZS; oběti na životech a zdraví obyvatel v důsledku ztráty řízení území; selhání sociální péče o děti, staré a nemocné lidi a v důsledku zastavení činnosti krajských hygienických stanic apod.
2. Možné dopady na bezpečí lidí: selhání armády a dalších bezpečnostních složek (Policie ČR, HZS, ZZS, vězeňské služby aj.); ztráta pocitu bezpečí lidí; rabování, násilí; zvýšení kriminality; desorientace lidí aj.
3. Možné dopady na majetek: devastace obydlí nebo jiných materiálních statků od kriminálních živlů či v důsledku neřešení věcí veřejné správy a občanských záležitostí; výpadek finanční správy → snížení daňových výnosů → dlouhodobé ztráty pro území; materiální škody způsobené sníženou reakcí na mráz, sníh, povodně, pohromy velkého rozsahu, požáry; škody na objektech způsobené požáry v důsledku snížené akceschopnosti hasičů apod.
4. Možné dopady na veřejné blaho: zastavení mezinárodního obchodování a služeb občanům; zastavení společenských a kulturních akcí; snížení úrovně zdravotnické péče; zastavení činnosti krajských hygienických stanic; nestabilita, panika, chaos ve společnosti apod.

5. Možné dopady na životní prostředí: znečištění vod a ovzduší v důsledku výpadku řízení území; narušení ekosystémů v důsledku výpadku řízení území; onemocnění či úhyn zvířat v důsledku výpadku řízení území; zastavení ochrany přírody, chráněných území, chráněných rostlin a živočichů v důsledku výpadku řízení území; zastavení přílivu peněz do sféry ochrany životního prostředí apod.
6. Možné dopady na infrastruktury a technologie, které se dále člení na:
   - možné dopady na dodávky energií (elektřina, teplo, plyn): v důsledku selhání řízení věcí veřejných špatná regulace dodávek elektřiny, vody a plynu; výpadky v dodávkách; pomalé nápravy v opravách rozvodů a dodávek energií apod.
   - možné dopady na systém dodávky vody: v důsledku selhání řízení věcí veřejných špatné dodávky vody; zhoršení kvality pitné vody (nefunguje inspekce) apod.
   - možné dopady na kanalizační systém: v důsledku selhání řízení věcí veřejných nefunkčnost systému; nedostatečný chod čističek a odkalovacích zařízení; kanalizace se dostane do podzemních a povrchových vod apod.
   - možné dopady na přepravní síť: v důsledku selhání řízení věcí veřejných nefunkčnost veřejné dopravy a systému organizace dopravy apod.
   - možné dopady kybernetickou infrastrukturu (komunikační a informační sítě): v důsledku selhání řízení věcí veřejných: nefunkčnost komunikačních sítí, pošty, přenosu dat apod.
   - možné dopady na bankovní a finanční sektor: v důsledku selhání řízení věcí veřejných porušení finančního trhu; finanční machinace s veřejnými prostředky apod.
   - možné dopady na nouzové služby (policie, hasiči, zdravotníci): v důsledku selhání řízení věcí veřejných nefunkčnost dopravní policie, tzn. možnost dopravních kolapsů a velké množství nevyřešených nehod, rozpad systémů nouzových služeb apod.
   - možné dopady na základní služby v území (zásobování potravinami, likvidace odpadů, sociální služby, pohřební služby), průmysl a zemědělství: v důsledku selhání řízení věcí veřejných: nefunkčnost obchodů, …všech základních služeb; zastavení provozu škol, školek, a dalších sociálních zařízení; zastavení výroby průmyslových podniků (podniky ve vlastnictví státu);
   - možné dopady na státní správu a samosprávu: v důsledku selhání řízení věcí veřejných: ztráta provozu úřadů práce; neplnění úkolů vyplývajících z odpovědností stanovených zákony o státní správě i samosprávě (např. nevydání občanských průkazů nebo cestovních pasů apod.) v důsledku selhání řízení věcí veřejných; ztráta správy území; ztráta činnosti profesních komor (např.: Notářská komora ČR, Česká lékařská komora, Česká advokátní komora, Česká stomatologická komora apod.); nečinnost pozemkových úřadů, inspektorátů Státní energetické inspekce atd.; lidé nedostanou např. podporu v nezaměstnanosti, přídavky na dítě apod.; selhání ČNB → nejsou k dispozici kurzy měn, není regulován oběh peněz, není přehled o finančním trhu domácím i zahraničním; státní podniky nemají přístup k účtu v ČNB; ztráty ve finančním sektoru ve vlastnictví státu apod.

Jelikož výstavba a provoz technických děl vyžadují finanční prostředky, je třeba pojednat o finančním systému. Finanční systém je soubor trhů, institucí, zákonů, regulací a technik, s jejichž pomocí jsou obchodovány obligace, akcie a jiné cenné papíry, určovány úrokové sazby a poskytovány finanční služby po celém světě. Jeho primárním úkolem je přemístit zápůjční kapitál na spotřebu a investice. Finanční systém je nedílnou součástí ekonomického systému a nemůže být posuzován odděleně. Všichni, tj. spotřebitel, investor, podnikatel, politik i občan jsou závislí na rychlosti, efektivitě a kvalitě služeb, které poskytuje finanční systém. Proto je součástí kritické infrastruktury každého státu i celé EU. Důkazem je i skutečnost, že Rada Evropské Unie s ohledem na Smlouvu o založení Evropského společenství zřídila finanční nástroj pro civilní ochranu (2007/162/ES, Euratom). Nástroj je zřetelným vyjádřením evropské

solidarity vůči zemím postiženým závažnými pohromami, protože usnadňuje poskytování pomoci prostřednictvím mobilizace zásahových prostředků členských států.

Finanční systém peněžních a kapitálových trhů je závislý na ekonomice a na společnosti, která jej obklopuje. Ekonomické poklesy a vzestupy, technologické inovace, politické převraty, války, sociální změny i živelní pohromy ovlivňují rozhodnutí na finančních trzích a mají často ničivé důsledky. Problémy systému jsou spojené jak se škodlivými jevy všeho druhu (viz přístup All Hazard Approach [8]), tak se špatným řízením systému, tj. i se špatnými reakcemi na problémy a s nezvládnutím předvídatelných rizik [2]. Proto byla provedena simulace možných dopadů dlouhodobého selhání finančního sektoru na veřejná aktiva. Byla použita metoda What, If a data od 142 respondentů z veřejné správy, kteří řeší bezpečnostní otázky [12]. Jejich vyhodnocení ukazuje:

1. Možné dopady na životy a zdraví lidí: ztráta přístupu k peněžním prostředkům a tím i k nákupu potravin a všeobecně k uspokojování základních lidských potřeb; kvůli neplacení ztráta osvětlení, vytápění, možnosti přípravy jídla, nájmů; kvůli nedostatku financí na ošetření lidí, selže lázeňská péče, péče o zdravotně postižené, duševně nemocné, dojde ke snížení úrovně veřejně dostupné péče; kvůli nedostatku financí zdravotnická zařízení budou provádět pouze neodkladné případy, sníží se hygienické standardy, nebudou peníze na benzín do vozidel záchranářů; lidé z nedostatku hygieny a dalších závažných nedostatků postupně onemocní a dojde k epidemiím; zastaví se rehabilitační a pečovatelské služby; na duševní zdraví obyvatel bude působit pocit beznaděje (uložené peníze v bance ztrácí hodnotu a všechny úspory, spoření přichází vniveč); dojde ke skupování potravin a šmelině; lidé nedostanou půjčky na základní potraviny kvůli nemožnosti splácení dluhů a nemožnosti vyplacení mzdy apod.
2. Možné dopady na bezpečí lidí: vznik paniky, chaosu, ztráta pocitu bezpečí obyvatelstva; strach z celkového vývoje situace mohou vést k agresi a panice lidí; sociální nepokoje; v případě ztráty peněžních prostředků pocit strachu, nebezpečí, nejistoty, deprese; růst kriminality – ke zločinům se uchýlí i normální lidé mající hlad; nerespektování zákazů, příkazů a samotných zákonů; vznik baretu (směna zboží za zboží) s tím souvisí vznik černého trhu apod.; závislost na případné pomoci ze zahraničí; nedůvěra občanů ve stát – možnost případu „převzetí problému / správy do vlastních rukou“; úplatkářství (ne peněžní, to nemá hodnotu); rabování; kriminální činy; vznik mafií; při dlouhodobějším výpadku pracovní demotivace lidí; nedostatek peněz na léky apod.
3. Možné dopady na majetek: nemožnost dohledu a kontroly majetku v elektronické podobě a hospodaření s ním; ztráta přístupu k informacím týkajících se peněz, měny a kapitálu; nemožnost zvyšování majetku; ztráta majetku související s nutností získání peněz (rozprodávání např. vnitřního vybavení bytu, dědictví, šperků); exekuce majetku v důsledku nezaplacení v daném termínu; ztráta domácích a chovných zvířat (lidé budou muset především uspokojovat vlastní potřeby a nebudou mít finanční prostředky na krmiva pro zvířata); ohrožování majetku vzrůstajícím rabováním, krádežemi atd.; firmy nebudou mít finanční prostředky na ochranu a ostrahu majetku; postupné znehodnocení majetku - lidé si nebudou moci vzít hypotéku na přestavbu či postavení nového bydlení apod.
4. Možné dopady na veřejné blaho: zastavení společenských a kulturních akcí; masivní propouštění státních zaměstnanců (např. platy úředníků zatěžují finanční prostředky, jejich služby při déletrvajícím výpadku finančního sektoru ztratí na důležitosti, nebudou potřeba a nebudou využívány); problémy udržet pracovníky nouzových služeb (zdravotnických zařízení, hasiči, policie, armáda); nezaměstnanost pracovníků bankovního sektoru; zastavení obchodování a služeb občanům; nedostání všech svých závazků z důvodu finančních problémů; pokles ekonomické úrovně obyvatelstva; zpomalení společenského rozvoje; nefunkčnost hromadné dopravy; uzavírání těch částí infrastruktury, které nebudou mít takovou prioritu (např. školek), jejichž provoz odčerpává finanční prostředky státu;

znehodnocení potravin, které nebude moci nikdo koupit; kavárny, restaurace, hospody, bary – existenční problémy; veškeré služby volného času (plavecký bazén, sauny solária, fitcentra, kadeřnictví, kosmetiky, masáže, pedikúry) přijdou nazmar; omezení turistického ruchu, nedostatek finančních prostředků na nákup letenek, jízdenek; nemožnost splácení dluhů mezi občany → msty, násilí, krádeže apod.

5. Možné dopady na životní prostředí: pozastavení ekologických aktivit dlouhodoběji závislých na finančních zdrojích; finanční problémy při řešení akutních rozsáhlých ekologických havárií; lidé budou uspokojovat základní potřeby a nezbydou jim peníze na např. odvoz odpadků (s tím souvisí zvyšování počtu černých skládek); firmy se budou snažit udržet alespoň základní výrobu, tudíž budou šetřit např. na čističkách, odlučovačích, tzn., že dojde ke zvýšení tepelných a kapalných emisí; firmy nebudou mít dostatek peněz na výzkum nových systémů chránicích životní prostředí; zastavení výstavby i provozu čističek a jiných různých ochranných zařízení životního prostředí; nebudou peníze na uhlí, zemní plyn → lidé budou topit odpadky, což znečistí ovzduší; nebudou peníze na vysazování nových stromků; nebudou jezdit popeláři, uklízet metaři (všude nepořádek); nemožnost financování různých čističek, separátorů odpadů, chladících zařízení apod.; ekologické havárie v důsledku lidské nečinnosti; znečištění vod v důsledku nečinnosti čističek; škody na životním prostředí v důsledku snazšího přístupu k přírodním zdrojům; ztráta sponzorských finančních aktiv na zlepšení životního prostředí apod.
6. Možné dopady na infrastruktury a technologie, které se dále člení na:
   - možné dopady na dodávky energií (elektřina, teplo, plyn): ztráta funkčnosti dodávek v související s finančními prostředky; selhání činnosti kybernetické infrastruktury a ostatních systémů, které jsou závislé na elektrické energii; selhání centrálních dodávek zemního plynu a ropy do státu (neschopnost státu za dodávky platit); šetření dodávek energie do domácností, firem apod.
   - možné dopady na systém dodávky vody: ztráta funkčnosti dodávek vody související s finančními prostředky; ztráta řízení sítí v čase apod.
   - možné dopady na kanalizační systém: v důsledku platební neschopnosti malá funkčnost a snížené uspokojování potřeb obyvatel apod.
   - možné dopady na přepravní síť: zvýšení počtu nehod v důsledku selhání řízení signalizace špatně placené; v zimě kvalita cest velmi omezená – silničáři nemají peníze na posypový materiál a provoz strojů; postupný rozpad dopravní sítě; značné omezení a totální kolaps v městské hromadné dopravě, u Českých drah, na autobusových linkách, v osobní a nákladní dopravě (nejsou peníze na nákup nafty, benzínu a opravu vozidel → zvyšování cen přepravy apod.
   - možné dopady kybernetickou infrastrukturu (komunikační a informační sítě): kvůli neplacení služeb kaskádové efekty a dominové efekty v systémech a sítích, zhroucení telekomunikační sítě, selhání internetu; snížení rozsahu rozhlasového a televizního zpravodajství, časopisů, provozu informačních systémů apod.
   - možné dopady na bankovní a finanční sektor: selhání bankomatů a e-bank; zhroucení internetového bankovnictví; ztráta přehledu o situaci na finančním trhu; ztráty na finančním trhu v důsledku sankcí za neprovedené transakce a za promarněné příležitosti; banky přestanou vydávat peníze a poskytovat úvěry; ČNB v případě České republiky nebude moci kontrolovat peníze v oběhu, výši kurzů peněz a jiné platební transakce se zahraničím; dojde k znehodnocení peněz v bankách, ztrátě kupní síly peněz; zvýšení inflace, hyperinflace; pokles měnového kurz; nedostatek peněz v oběhu; zastavení dovozu a vývozu; ztráty dopravců, sektorů služeb (zejména těch co nabízejí nadstandardní služby); zhroucení burzy; neschopnost zaměstnavatelů vyplácet mzdy; omezení sociálních dávek; nevyplácení důchodů, mezd a platů a tím zastavení prací závisejících na platbách, a to jak v tuzemsku, tak v zahraničí; dominový efekt

z nedostatků informací v bankovnictví; ztráty na finančním trhu v důsledku sankcí za neprovedené transakce a za promarněné příležitosti; pokuty z prodlení v důsledku nemožnosti zaplatit včas; finanční ztráty věřitelů bank; zvyšování cen zboží; vzestup šedé ekonomiky; chudnutí; nemožnost splácení závazků (druhotná platební neschopnost, nemožnost splácet hypotéky, leasing apod.); nemožnost disponovat s penězi v bance; nemožnost placení faktur; zhroucení obchodu apod.

- možné dopady na nouzové služby (policie, hasiči, zdravotníci: kvůli problémům ve finančních trzích omezena činnost policie, hasičského záchranného sboru, armády a nemocnic vynucena zákonem (chybí pohonné hmoty do vozidel nouzových služeb aj.; ztížená činnost zdravotnických zařízení apod.
- možné dopady na základní služby v území (zásobování potravinami, likvidace odpadů, sociální služby, pohřební služby), průmysl a zemědělství: dojde k útlumu zásobování; omezení poštovních služeb; snížení úrovně pečovatelské služby; celkové narušení dodávek zboží; zavřou se restaurace, jídelny, které nebudou mít na zaplacení zásobování apod.
- možné dopady na státní správu a samosprávu: nemožnost dostát všem úkolům vyplývajícím z odpovědností stanovených zákony o státní správě i samosprávě; neschopnost udržet situaci v území pod kontrolou; lidé nebudou moci odvádět sociální a zdravotní pojištění a tedy ani stát nebude mít prostředky na garanci těchto služeb; výpadek škol; zpomalení vědy a výzkumu apod.

Finanční krize v letech 2008-2014 ukázala velkou důležitost finančního sektoru, jak pro kvalitu života lidí, tak pro ekonomickou úroveň státu. Na základě analýzy údajů v práci [390] jsou hlavní příčiny bankovních krizí: makroekonomický vývoj; špatné řízení; trestná činnost (tzv. tunelování); a laxní bankovní dohled (i když není primární příčinou). Vedlejší příčiny bankovních krizí jsou: neefektivní činnost bank; nadměrný počet pracovníků; tlak akcionářů na získání výhodnějších podmínek; nedostatečné účetnictví bank nebo klientů; a vylepšování výsledků. Důsledkem je pak pokles ekonomické aktivity, spočívající v úvěrové kontrakci (credit crunch), kdy se snižuje dostupnost úvěrů. Následkem je pak bankrot i jinak životaschopných podniků a v konečném důsledku to má dopad na: pokles růstu HDP; a absolutní pokles HDP.

Finanční krize v bankovním sektoru mohou být v první úrovni jejich klasifikace rozděleny podle dvou základních faktorů jejich vzniku: finanční krize v bankovním sektoru plynoucí z podnikatelské činnosti, tj. v důsledku realizace bankovních rizik, do kterých patří: úvěrové riziko, tržní riziko, likvidní riziko a obchodní riziko; a finanční krize v bankovním sektoru způsobená výskytem škodlivých jevů všech druhů [5], tj. realizací operačních (provozních) rizik. V praxi je nutno zvažovat ještě systémové riziko, k jehož pochopení si je třeba uvědomit řetězec událostí, který může odstartovat realizace jakékoli z pěti výše zmíněných rizik. Jejich realizace (individuálně či v kombinaci) způsobí bance potíže, které mají nepřijatelný dopad na mnoho dalších subjektů či v krajním případě i na větší část finančního systému. Systémové riziko je ve své podstatě rizikem přenosu potíží, kdy neschopnost jedné instituce splnit své splatné závazky způsobí, že jiné instituce nebudou schopny splnit své závazky. Předmětné selhání může způsobit značné likvidní problémy a problémy se splácením úvěrů bankám a v důsledku toho může ohrozit stabilitu bankovního systému jako celku. Ochrana před systémovým rizikem je součástí činnosti regulátorů finančních trhů (včetně institucí bankovního dohledu) a centrálních bank. Je velmi důležitá pro výstavbu a provoz technických děl, jelikož problémy ve finančním sektoru dopadnou na veřejná aktiva dříve nebo později.

Shrnutí

Protože vytvoření kompletního seznamu dopadů a všech možných řetězců dopadů primárních, sekundárních, terciárních apod., tj. scénářů pohromy v každém konkrétním místě

je základem hodnocení rizik a pochopitelně i základem řízení bezpečnosti, je třeba provést důkladné expertní šetření v této záležitosti v obecné poloze a potom pro každé území expertní došetření, které vezme v úvahu místní podmínky. Na základě těchto analýz je možno dále přikročit k navrhování místních preventivní a zmírňujících opatření, zajistit připravenost provozovatelů, správních úřadů i občanů a vyhotovit scénáře odezvy, které budou procvičeny za účasti všech složek podílejících se na odezvě.

Je si třeba uvědomit, že v souvislosti s technickými díly je role státu i role finančního sektoru velmi významná. Každé opatření spojené s technickým dílem něco stojí, a proto musí být činěno na základě rozhodování ve prospěch veřejného zájmu tak, jak to stanoví ústava ČR. Realizace každého opatření vyžaduje také disponibilní znalosti a dovednosti, čas a motivaci tvůrců a provozovatelů technického díla, a proto stát musí zajistit příslušnou vzdělanost, legislativu, dobré pracovní a společenské podmínky pro odborníky a realizátory, kteří vytváří a provozují technická díla.

5.14. Shrnutí údajů o lidském faktoru a problematice hodnocení havárií

Podniky, tj. velké provozy a systémy jsou víc než jen množinou technických částí zařízení a součástek. Jsou odrazem organizační struktury, managementu, provozních předpisů a kultury konstrukčních organizací, které je vytvořily a také jsou zpravidla i odrazem společnosti, ve které byly vytvořené [1,2,26]. Havárie a nehody, tj. události doprovázené škodami, újmami a ztrátami na chráněných aktivech jsou pořád ještě často svalované na chyby operátorů nebo zařízení, bez rozlišení technických, organizačních a manažerských faktorů, které způsobily, že se předmětné chyby a nedostatky staly nevyhnutelnými.

Člověk je myslící bytost, která by neměla být „ponechána na milost“ řadě designovaným, organizačním a momentálním faktorům, které mohou vést k jednání, na které může být vnějším pozorovatelem nahlíženo (i když často neoprávněně) jako na lidskou chybu. Není vůbec jednoduché stanovit, kdy se přiklonit k variantě, že chyba byla způsobena opravdu člověkem, a kdy k ní byl donucen okolnostmi. Schopnost rozhodovat se správně, uvážlivě a včas patří k základním předpokladům praktické činnosti a tvořivého myšlení a je zároveň důležitou složkou lidské osobnosti.

5.14.1. Lidský faktor a havárie technických děl

Lidský faktor je pozitivní, když rozhodnutí člověka vede k zisku a k posílení aktiv, které člověku zajistí vyšší bezpečí, zisk a rozvoj. Je negativní, když člověka oslabí nebo poškodí. Zdrojem chyb v druhém případě je neznalost, nerespektování zákonitostí přírodních, technických, ekonomických a sociálních a machrovství (nejčastější chyba manažerů při hodnocení technických, přírodních a ekonomických podkladů) [28]. V odstavci 3.4.1. jsou uvedeny zdroje chyb roztříděné na: podmínky, které působí vznik chyb; podmínky, které působí porušení předpisů a pravidel; a dovolené porušování předpisů a pravidel. Z analýzy shromážděných dat v [12] vyplynulo, že selhání systému řízení přispělo k příčinám více než 85% nahlášených havárií.

Provedené analýzy havárií potvrdily příčiny havárií v nedostatcích řízení a v nevhodné struktuře práce. Ve většině velkých havárií byly technické informace o potřebné prevenci havárií dopředu známé a často i implementované. Při analýze téměř každé havárie, ke které bylo dostatek údajů, se ukázalo, že technické informace a řešení nebyly využity v důsledku nedostatků v organizaci a v jejím řízení. Ukázaly se závažné chyby při rozhodování a to zejména v situacích, kdy všechny alternativy, mezi kterými se rozhodujeme, jsou nežádoucí, a

jde jen o to, zvolit nejmenší zlo, byla odhalena řada zkratkovitých řešení, což odpovídá faktům uvedeným v práci [391].

Zde se ukázala nutnost připravit nástroje pro rozhodování pod tlakem, které: zajistí odpovědný přístup k problému a k výsledkům jeho řešení s ohledem na veřejné či jiné zájmy; umožní uplatnit morální vlastnosti jako rozvážnost, smysl pro povinnost a důslednost; zachovají schopnost: analyzovat problém či situaci, kreativně přistupovat k řešení problému; umožní anticipovat další vývoj, využívat analogie apod.; a umožní uplatnit zkušenosti a sociální dovednosti, umožňující mu regulovat činnost a jednání podřízených. Právě takové nástroje navrhuje a používá inženýrství rizika: All-Hazard- Approach, Defence-In-Depth, scénáře pro různé podmínky, scénáře odezvy pro různé podmínky, plány pro řízení rizik apod., a proto je třeba je zavést do praxe.

Na základě současného poznání, které je shrnuté v knize [28], a bylo již zmíněno, omezování rizik v rámci řízení bezpečnosti podniku pokrývá několik okruhů: 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 modelu organizační havárie. V odstavci 3.6.1 je uvedeno, že příčiny organizačních havárií se hledají ve třech základních oblastech, a to hlavně v organizačních procesech. Proto, jak již bylo vícekrát zmíněno, pro odvrácení rizik je nutno do řízení podniků zabudovávat proces řízení bezpečnosti PSM (Process Safety Management), který koordinuje všechny další procesy, a to od stanovení cílů v rámci hospodářské a sociální situace podniku; organizace podniku pro splnění stanovených dlouhodobých strategických cílů; řízení provozních činností; organizační procesy; podmínky, které působí vznik chyb nebo porušení předpisů; a chyby a/nebo porušení předpisů.

5.14.2. Problematika hodnocení havárií

Je skutečností, že popisy příčin havárií často zahrnují subjektivitu a filtrování zjištěných informací. Pouze ojediněle jsou příčiny havárií vnímané identicky vedením společnosti, inženýry, představiteli odborů, operátory, zaměstnanci v pojišťovnách, soudci, policisty, novináři, státem a oběťmi. Ukazuje se, že každá specifikace možných příčin havárií nevyhnutelně nese znaky střetu zájmů [1,28,304].

Některé podmínky mohou být považované za nebezpečné jednou skupinou, přičemž druhá skupina je má za perfektně bezpečné a nevýznamné. K uvedeným střetům dochází často v situacích, při kterých jsou potřebná normativní, etická a politická posouzení. Navíc, rozhodnutí o příčině nehody mohou být ovlivněná hrozbou možných soudních sporů.

Opravdu, každý dotazovaný člověk může přisoudit k dané havárii či nehodě různou příčinu. Jedna studie ukázala, že dělníci, kteří byli spokojeni se svou prací a byli včleněni do podnikání, přisuzovali událostem hlavně osobní příčiny [28,304]. Naopak, pracovníci, kteří nebyli spokojení, měli na podnikání jen malý podíl, uváděli daleko častěji neosobní příčiny, které dokazovaly, že za události odpovídá podnik. Dalším faktorem subjektivity může být pracovní postavení v organizaci. Čím nižší je hierarchické postavení, tím větší je tendence svádět události na faktory spojené s organizací a naopak, jednotlivci, kteří mají vysoké postavení v hierarchii, mají tendenci obviňovat dělníky. Uvedený fakt odporuje údajům z hlášení o „skoro nehodách“, která dokazují, že příčinami vzniklých událostí jsou v převážné míře technické a organizační závady (často mající kořen v rozhodnutích špičkových řídících pracovníků). Je tedy zřejmé, že určení příčiny závisí na určitých charakteristikách oběti a na analýze postavení oběti (hierarchické postavení, míra zainteresovanosti a spokojenost s prací) na vztazích mezi obětí a analytikem a na stupni závažností havárie [304].

Identifikování příčiny nehody a z ní vyvinuté havárie může být ovlivněno i metodami sběru dat. Většinou jsou údaje o haváriích shromažďované ve formě textových popisů časového

průběhu události s tendencí soustřeďovat se na běžné okolnosti bezprostředních jevů (které časově těsně předcházely vzniklé události). Na jedné straně, formuláře pro zaznamenání jevů, které jsou předem připravené jen na bezprostředně související jevy, většinou ani neumožňují zaznamenat i jiné související jevy. Na druhé straně, podrobněji vymezené formuláře mohou omezit kategorie podmínek, které mají být zvažované při vyšetřování příčin události [304].

Dalším problémem při identifikování příčin havárií je nepřiměřené zjednodušování. Mnohokrát se při nehodách zdůrazní pouze některé faktory jako příčina, a to přesto, že všechny zjištěné faktory byly stejně nevyhnutelné pro vznik události. Např. při smyku auta za deště může působit mnoho faktorů, jako např.: mokrá vozovka, nedostatek zkušenosti řidiče, nevybavení auta protismykovým brzdovým systémem a pod. Ani jeden z uvedených faktorů není dostatečnou příčinou smyku, ale jakýkoliv z nich je často uváděný jako jediná příčina smyku. Určitá podmínka / faktor může být vybraná jako příčina čistě proto, že se naplnila jako poslední před vznikem události, nebo se zdá být nejnápadnější, nebo analytik má svůj vlastní motiv pro její výběr. Mnoho odborníků zastává názor, že přestože často izolujeme jednu podmínku a nazveme ji příčinou, přičemž ostatní podmínky považujeme za přispívající, nemá takové odlišování žádný všeobecný základ [304].

Přílišné zjednodušování příčinných faktorů u havárií může být obzvlášť škodlivé pro ochranu před haváriemi v budoucnosti. Společným typem přílišného zjednodušování je úřední, formálně zákonný přístup, kterým se nehody připisují jen selháním člověka, nebo technickým chybám, přičemž se ignorují organizační faktory a hledají se jednoduché zjevné příčiny.

Právníci a pojišťovací agenti často příliš zjednodušují příčiny havárií a obyčejně identifikují bezprostřední, resp. přímou příčinu nehody. Je jim jasné, že se na havárii podílelo více faktorů, ale z praktických důvodů, obzvlášť pro určení viny a odpovědnosti za škodu, identifikují podstatný faktor jako příčinu. Jejich cílem je určit, která ze zúčastněných stran má ze zákona odpovědnost zaplatit škody. Předmětné určování může být ovlivněné platební schopností zúčastněných stran nebo politickými úvahami [28,304,305].

Všeobecně neexistuje žádné objektivní kritérium pro upřednostnění jednoho faktoru před druhým, z množiny těch, které se podílely na havárii. Právnický přístup ke kauzalitě má výhodu jen pro určení viny a odpovědnosti. Pro technický pokrok, u kterého cílem je porozumět a zabránit havárii, má právnický přístup pouze malý užitek. Může být dokonce přímo škodlivý, protože většina relevantních faktorů z hlediska prevence budoucích havárii může být u něj ignorovaná [28,305].

Opatření proti nehodám a haváriím, které z nich vznikají, by neměla být určovaná podle relativního významu příčinných faktorů. Naopak, priority musí být dány takovým opatřením, které bude co nejefektivněji redukovat ztráty. Zjednodušené vysvětlení nehod často neposkytuje nevyhnutelné informace pro zabránění dalším nehodám v budoucnosti a kromě důvodů souvisejících s odpovědností, je vynakládání času na určení relativních příspěvků jednotlivých faktorů k předmětným událostem neproduktivní.

Nejčastěji vyskytujícím přílišným zjednodušením je podle zpráv o nehodách svalení viny na člověka (operátora, pilota, řidiče, dělníka). V každém systému, do kterého je včleněný člověk, může být hypoteticky příčina nehody vždy přiřazená člověku, ať už za jeho zásahy, nebo za nedostatečnou prevenci havárií. I v případech, když je chyba člověka bezprostředně spojená s nehodou, je chybou považovat člověka za jedinou příčinu nehody systému a snažit se ho proto v budoucnosti z něho vyloučit, protože to má jen omezený účinek pro identifikaci toho, co má být změněno, aby se efektivně zvýšila bezpečnost. Lidský faktor totiž v řadě případů je jediný, který dokáže zvládnout díky intelektu složité situace [28], např. zkušený operátor odvrátil při povodni v r. 2002 přelití hráze na přehradě Orlík, zkušený pilot přistál v r. 2012 na řece Hudson, když přestaly fungovat motory letadla v důsledku nasátí hejna hus atd.

Všeobecně se selhání člověka udává jako příčina nehody a uvádí se „vinen je lidský činitel“. Analytici často zastaví rozbory při chybě člověka a nevěnují náležitou pozornost jiným nevyhnutelným okolnostem, které musely spolupůsobit, aby k chybě člověka došlo.

Protože objektivně můžeme o každé havárii říci, že ji způsobila chyba člověka, je uvedená fráze demotivující pro konstruktivní přístup k akcím potřebným pro zabránění opakovaným selháním člověka. Je velmi jednoduché říci někomu: „Buď opatrnější.“ Asi bude vhodnější přestat se zjišťováním, jestli chyba člověka byla příčinou nehody a místo toho začít zkoumat a aplikovat prevenci proti selháním člověka.

Obdobně přílišným zjednodušováním je i zaměření jen na technické chyby a bezprostřední fyzikální jevy. Předmětný typ převládajícího úzkého zaměření může vést k přehlédnutí některých nejdůležitějších faktorů nehody.

V souvislosti se sledovanou problematikou si je třeba uvědomit, že pro vyšetřování příčiny havárií nestačí jen osvojení technik, jako FTA, HAZOP apod. [5,15], kterými nelze zjistit příčiny havárií, které jsou důsledkem emergentních interdependences, tj. jevů, které se projevily jen za jistých podmínek. Podle teoretického rozboru autorky a podle jejich zkušeností z praxe ***zmíněné techniky jsou schopny odhalit jen příčiny, které leží v nastavených procesech a nevidí spouštěcí jevy (triggery), které tkví v náhlých propojeních*** (přeskočení jiskry mezi sousedními obvody navzdory izolaci, reakce vyvolané nezvyklými meteorologickými podmínkami, neočekávaně velká vnější pohroma apod.). Proto je třeba šetření velkých havárií provádět v kontextu SoS [1,10,11] metodami rizikového inženýrství.

Na základě získaných znalostí a zkušeností [305,306] je třeba následující běžné cíle vyšetřování velkých havárií:

- identifikovat to, co se stalo, jak se to stalo a proč se to stalo,
- systematické zkoumání lidských a technických faktorů,
- sběr informací pro možné legislativní a pojistné nároky,
- tvorba databáze údajů, možných řešení a poučení se z chyb,
- pojmenování příčin provozních obtíží,
- identifikování neodpovídajících výkonových standardů pro zkoumaná a vztažná zařízení,
- určení primární příčiny nehody,
- konstruktivnost (za vinu by se měla dávat pouze úmyslná porušení či přestupky),
- podpora hlášení o skoronehodách a vlastním pozorování,
- splnění zákonných oznamovacích a informačních požadavků,

doplnit o systematické hledání interdependences, které vedly k selhání zabezpečovacích a bezpečnostních systémů, anebo k chybné odezvě na havárii, a teprve na jejich základě provádět zodolnění. Přitom je nutno mít na paměti, že: co není zaznamenáno, nemůže být zkoumáno a vyšetřováno; co není vyšetřováno a zkoumáno, nemůže být změněno; a co nemůže být změněno, nemůže být zlepšeno. Důkladně je třeba prověřovat všechny fyzické důkazy a odpovědnosti jak řídícího týmu, tak jednotlivých zúčastněných.

6. ZÁSADY PRO ŘÍZENÍ RIZIK SLOŽITÝCH TECHNOLOGICKÝCH OBJEKTŮ A ÚZEMÍ, VE KTERÉM SE OBJEKT NACHÁZÍ

Nejprve je třeba konstatovat, že podle vědecké teorie řízení a dle dosavadních zkušeností z praxe je třeba v souvislosti s řešením problémů při stanovení rozdělení úkolů a odpovědností brát v úvahu možnosti, které existují na jednotlivých úrovních řízení. Možnosti jsou totiž dané jak pravomocemi, tak dostupností a množstvím disponibilních zdrojů, sil a prostředků které jsou potřebné k řešení:

- na operativní úrovni managementu technického díla lze úspěšně řešit dobře strukturované problémy,
- na střední úrovni managementu technického díla lze úspěšně řešit strukturované i špatně strukturované problémy, které nejsou spojeny s velkými riziky pro technické dílo,
- na vrcholové úrovni řízení technického díla lze úspěšně řešit složité i nestrukturované problémy, která mají rizika, která lze ovládat za použití nástrojů, které má jen vrcholové řízení technického díla k dispozici,
- jen vzájemnou spoluprací veřejné správy a vrcholového managementu technického díla lze řešit složité i nestrukturované problémy velkého rozsahu s velkými riziky.

U technických děl nadnárodního dosahu je pak ještě nutná mezinárodní spolupráce.

Pro odvození zásad pro řízení rizik složitých technických děl jsou použity znalostí a zkušenosti uvedené v předchozích kapitolách a základní hlediska:

1. Složitý socio-technologický systém musí být bezpečný po celou dobu životnosti, a proto řízení rizik musí být zacíleno na integrální bezpečnost a ve všech aspektech ucelené, systémové a proaktivní.
2. Složitý socio-technologický systém musí po celou dobu životnosti plnit kvalitně úkoly a ani při svých kritických podmínkách nesmí neohrozit sebe ani své okolí, tj. aplikuje All-Hazard-Approach, Defence-In-Depth, má program pro neustálé zvyšování bezpečnosti a kultury bezpečnosti.
3. Složitý socio-technologický systém je důležitý pro zajištění základních funkcí státu (rozvody elektřiny, rozvody vody, kanalizace, jaderné elektrárny, dálnice, velká letiště, dopravní tepny, velké výrobní celky apod.), a některé z nich i EU, a proto se povinnosti při vypořádání rizik se rozdělují mezi všechny zúčastněné.

Proto z pohledu bezpečí a rozvoje lidí je řízení rizik složitých technologických celků důležité ve dvou oblastech:

A. Oblast propojující veřejnou správu a management složitého socio-technologického celku.
B. Oblast věcná zabývající se daty, metodami, materiálovými a technickými záležitostmi, organizačními, právními, finančními a personálními záležitostmi přímo v složitém socio-technologickém celku.

6.1. Obecné zásady řízení rizik, které plní stát i složité složitý technologický celek

Zásady pro řízení rizik na úseku propojení veřejné správy a managementu složitého socio-technologického systému jsou stanoveny pro úrovně:

A1. Politickou (parlament, vláda, veřejná správa) – celkem 4 požadavky.
A2. Strategickou (veřejná správa, vlastník, investor, provozovatel) – celkem 8 požadavků.
A3. Taktickou (veřejná správa, vlastník, investor, provozovatel) – celkem 4 požadavky.
A4. Operativní / funkční (provozovatel) – celkem 5 požadavků.

A5. Technickou (provozovatel) – celkem 19 požadavků.
Jde celkem o 40 požadavků.

A1. Zásady pro řízení rizik složitých technologických zařízení – úroveň politická – pro: parlament, vládu a veřejnou správu:

- vytvářet podmínky pro dlouhodobou stabilitu veřejného prostoru, kterou složitý technologický systém potřebuje pro kvalitní provoz, (jde především o zajištění stabilní vlády, zmírnění korupce, zabránění vytváření netolerantních skupin, zmírňování dopadů terorismu a závažných dopadů národních a nadnárodních konfliktů na složitý technologický systém).
- podporovat veřejný zájem a respektovat fakt, že rizika složitého technologického systému vstupují do veřejné oblasti, tj. jde o externality, které nemohou řešit tržní mechanismy (škodlivé dopady; výpadkem provozu je ohrožena značná část veřejnosti; politické rozhodnutí má potenciál vyvolat událost, při které dojde k realizaci rizika; a nežádoucí jevy, při kterých se realizují nepřijatelná rizika, jsou rozloženy tak, že neberou ohled na politickou spravedlivost),
- respektovat, že časté změny legislativy, daní a požadavků na provozovatele složitých technologických systémů mohou vést ke snížení kvality provozu složitých technologických systémů,
- při rozhodování o složitých technologických systémech brát v úvahu názory specialistů a neupřednostňovat momentální politické zájmy a akce nátlakových skupin.

A2. Zásady pro řízení rizik složitých technologických zařízení - úroveň strategická – pro: veřejnou správu, investora, vlastníka a provozovatele:

- respektovat hodnotové a kulturní souvislosti (pohodlná strategie pojištění a odškodnění není plně spolehlivá, protože při realizaci velkého rizika může dojít k zasažení sociálního systému, a tudíž se musí prosazovat princip předběžné opatrnosti a odpovědnost od všech zúčastněných),
- zabránit použití chybných technologií, technologické nedostatečnosti projektu složitých technologických zařízení a nedostatečné připravenosti lokality na provoz složitých technologických zařízení (dozor, dohled státu),
- zajistit, aby závazky spojené se složitými technologickými zařízeními byly plněny v dobré kvalitě (dozor, dohled státu),
- zajistit vzdělávání personálu pro složitá technologická zařízení, a to především na úrovni technické a technicko - organizační; příslušný výzkum, plánování a legislativu na podporu činnosti složitých technologických zařízení,
- při práci s riziky složitých technologických zařízení prosazovat proaktivní, systémový a strategický přístup,
- dbát na dobrou reputaci složitých technologických zařízení (goodwill) při práci s riziky,
- zajistit, aby nebyly podceněny významné zdroje rizik pro složitá technologická zařízení, kterými jsou: nejistota v oblasti pracovních sil (nevhodná kvalifikace, nedostatek pracovníků, nespolehlivost pracovníků - fluktuace, stávkové hnutí apod.); neurčitost finančních zdrojů (nesolventnost obchodních partnerů, nejistota úvěru, problémy s pojištěním apod.); havárie a velké poruchy na provozovaném zařízení; průmyslové havárie u jiných subjektů; živelní pohromy; a politická nebo hospodářská nestabilita v regionu, kde je složité technologické zařízení lokalizováno,
- zajistit schopnost veřejné správy a složitých technologických zařízení zvládnout dopady extrémní havárie a obnovu složitých technologických zařízení i okolí.

A3. Zásady pro řízení rizik složitých technologických zařízení na úrovni taktické – pro veřejnou správu, investora a provozovatele:

- zajistit, aby v projektu, výstavbě a provozu složitých technologických zařízení byly zváženy a správně vypořádány všechny závažné pohromy možné v lokalitě složitého technologického zařízení
- zajistit, aby projektová dokumentace byla správná a bez chyb; konstrukce a stavba probíhala podle odborných požadavků, tj. bez chyb, překročení stavebních nákladů a zbytečného znečištění životního prostředí v lokalitě složitých technologických zařízení,
- zajistit, aby složitá technologická zařízení byla bezpečná za podmínek normálních, abnormálních a kritických (dohled a dozor státu),
- zajistit spolupráci s místním obyvatelstvem a místními bezpečnostními složkami pro případ havárie i rozvoje okolí složitých technologických zařízení.

A4. Zásady pro řízení rizik složitých technologických zařízení na úrovni operativní / funkční – pro provozovatele:

- zajistit správné vypořádání všech rizik, zvláště pak tržních rizik, jakými jsou snížení poptávky po výrobku, změny měnového kurzu; inflace, deflace a změna úrokové sazby,
- zajistit kvalitní provoz zařízení z pohledu zajištění materiálových vstupů a kvalifikovaného personálu,
- zajistit kulturu bezpečnosti založenou na vzájemné spolupráci, tj. mít nástroje na řízení konfliktů mezi zaměstnanci,
- zajistit zdroje a ochranné prostředky pro zaměstnance i místní obyvatelstvo, včetně informačních zařízení a dokumentů (pro případ havárie),
- zajistit příslušné vzdělání zaměstnanců, kontraktorů i místního obyvatelstva.

A5. Zásady pro řízení rizik složitých technologických zařízení na úrovni technické – pro provozovatele:

- permanentně zlepšovat chápání, řízení a vypořádání rizik,
- zavést kontinuální monitoring zdrojů rizik,
- zvažovat rizika spojená s organizačními haváriemi,
- zvažovat rizika spojená se složitostí technologických celků (protože složitost nejen vytváří nová nebezpečí, ale dělá je i hůře odhalitelnými; nová nebezpečí jsou např.: zvyšování automatizace, růst výrobní kapacity, velké tempo technologických změn),
- počítat s výskytem atypických havárií, jejichž příčinou jsou neočekávané kombinace jevů a mít kvalitní plány odezvy pro více scénářů havárií a také pro havárii způsobenou kombinací řady nepřijatelných jevů,
- připustit, že mohou selhat bezpečnostní systémy,
- zpracovat plán odezvy na extrémní jevy,
- nacvičit odezvy na situace vyvolané extrémními jevy,
- pro případ velké havárie mít zajištěné místo pro řízení odezvy a technické vybavení na odklízení trosek,
- zajistit, aby se odborný top management neustále zajímal o vývoj poznání a vyhodnocoval zkušenosti z tvorby a provozu složitých technologických celků, protože neexistuje žádná předchozí zkušenost, které by mohlo být využito při překonávání nových nebezpečí, a odpovídající zákony a normy pro mnohé z nových inženýrských odvětví a technologií ještě nejsou vypracované,
- zajistit plnění všech úkolů spojených s provozem složitých technologických zařízení, které jsou uvedeny ve věcné oblasti
- zajistit plnění všech úkolů státu (výrobky v požadované kvalitě, obslužnost),

- při řízení složitých technologických zařízení vycházet z kvalifikovaných odborných kritérií pro posuzování rizik (stanovených dle: charakteru a druhu následků, které se mohou při realizaci rizika 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; a možnosti kombinace více rizik),
- zajistit odborné provádění činností, kvalifikovanou údržbu, kvalifikované opravy, včasné modernizace; a včasnou adaptaci na změnu podmínek (mít kvalifikované odborné řízení a vysoce účinnou odbornou kontrolu, a to včetně motivačních prostředků pro zacílení zaměstnanců na bezpečné provádění činností a vzájemnou spolupráci),
- zajistit ochranu a potřebný výcvik kritických zaměstnanců, tj. i ochranné prostředky a pomůcky a další potřebné náležitosti, a to včetně příslušných rezervních zdrojů a chráněných prostor pro ukrytí zaměstnanců,
- zajistit kvalitní provozní předpisy pro normální, abnormální a kritické podmínky,
- zajistit kvalitní monitoring a včasnou reakci na odchylky provozu, poruchy, skoro nehody a nehody (zajistit, aby se včas přijímala potřebná opatření, a to zvláště tam, kde dochází k hromadění velkého množství poruch a skoro nehod),
- zajistit sestavení základních plánů: plán řízení bezpečnosti, který bude zajišťovat bezpečnost v čase po dobu životnosti; plán řízení rizik, ve kterém budou jasné odpovědnosti za jednotlivá opatření a jednotlivé činnosti; vnitřní havarijní plán (ve kterém budou jasné odpovědnosti za jednotlivá opatření a jednotlivé činnosti); plán kontinuity (na překonání vysoce kritických až extrémních podmínek, ve kterém budou jasné odpovědnosti za jednotlivá opatření a jednotlivé činnosti pro zachování a přežití složitých technologických zařízení), vnější havarijní plán a krizový plán (ve kterém budou jasně vymezeny spolupráce a odpovědnosti složitých technologických zařízení a jeho bezpečnostních složek, veřejných bezpečnostních složek a veřejné správy),
- zajistit permanentní zvažování nových poznatků a poučení ze skoro nehod a havárií a jejich zavádění do praxe ve formě vhodné pro složitá technologická zařízení.

6.2. Věcné zásady řízení rizik, které platí pro složitý technologický celek

Zásady pro řízení rizik složitých technologických zařízení ve věcné oblasti je třeba sledovat na úsecích:

B1. Koncepce a způsob řízení složitých technologických zařízení – 21 požadavků.
B2. Požadavky na data, metody a techniky, které zajišťují kvalitní rozhodování a řízení složitých technologických zařízení – 9 požadavků.
B3. Postupy pro správné umístění, kvalitní projekt, výstavbu a provoz složitých technologických zařízení – 13 požadavků.
B4. Zajištění kontinuity provozu složitých technologických zařízení a podpory základních funkcí státu, tj. veřejného zájmu – 23 požadavků.

Jde celkem o 66 požadavků.

Řízení rizik musí respektovat, že zásadní roli hrají: znalosti; respektování fyzikálních a dalších zákonitostí (tj. vlastnosti materiálu, konstrukcí, staveb a prostředí a jejich proměny v čase), tj. existence limitů a podmínek; lidský faktor a s ním spojené provádění kvalitní práce a řádné plnění odpovědností ve všech fázích životního cyklu; dostupnost a způsoby aplikace postupů a technologií apod. Obecné principy pro práci s riziky jsou: být proaktivní; domýšlet možné důsledky; správně určovat priority veřejného zájmu; myslet na zvládnutí problémů; zvažovat synergie; a být ostražitý.

Ve všech fázích životního cyklu složitého technologického zařízení je třeba, aby řízení rizik respektovalo hlavní zásady:

- bylo zacíleno na integrální bezpečnost, používat All-Hazard-Approach, Defence-In-Depth, program na zvyšování bezpečnosti zacílený na integritu bezpečnosti (tj. mít systém řízení bezpečnosti, proces pro řízení bezpečnosti a kulturu bezpečnosti),
- bylo obsaženo v každém procesu rozhodování sledované entity – TQM a jeho ISO normy (Mezinárodní organizace pro standardizaci).
- respektovalo klíčové koncepty bezpečnostního a rizikového inženýrství, tj. zvažovalo kritické atributy kvality a kritické parametry procesu (kvalitní provádění opatření a činnosti prevence, připravenosti, odezvy, obnovy i poučení ze zkušeností),
- používalo: kvalitní data, metody a inženýrský přístup, progresivní typy bezpečnostních přístupů - inherentní, pasivní a aktivní bezpečnost,
- optimálně řídilo faktory o různé podstatě: znalosti; zkušenosti; rozpočet; kompetence, způsob řízení a rozhodování; týmová práce; atd.
- optimálně řešilo konflikty

B1. Zásady pro řízení rizik složitých technologických zařízení z pohledu koncepce a způsobu řízení - pro vlastníka, investora, provozovatele, odborný management, zaměstnance a kontraktory jsou:

- vycházet z nejlepších dostupných informací o chování složitých systémů,
- používat pouze otestované a v praxi ověřené koncepty složitých technologických zařízení,
- ve snaze ovládnout rizika složitých technologických zařízení se pohybovat po ose „anticipace budoucího“ a „zhodnocení minulého“, tj. opírat se o porovnání užitků a nákladů u různých variant rozhodnutí o riziku, a na jeho základě vybrat projekty řízení rizika nebo činnosti, které jsou schopné nejlépe přispět k růstu bezpečí a rozvoje složitých technologických zařízení,
- respektovat logický postup o vypořádání rizik v území o 4 krocích: poznání a sledování území a pohrom, které v něm mají závažné dopady; určení rizik a interakcí složitých technologických zařízení a území; opatření a činnosti pro zajištění bezpečných složitých technologických zařízení za všech podmínek (bezpečný projekt a jeho správná realizace, program řízení bezpečnosti v čase + plán řízení rizik pro prioritní rizika); způsob řešení vysoce nepřijatelných situací (odezva na extrémní pohromy včetně postupů, personálního, materiálního, technického a finančního zajištění),
- zajistit aplikaci zásad řízení a inženýrství orientovaných na bezpečnost složitých technologických zařízení (zdroje rizik jsou jevy všeho druhu uvnitř i vně, vnitřní závislosti všeho druhu a lidský faktor; uplatňuje se princip předběžné opatrnosti a požadavek na koexistenci životního prostředí, lidstva a techniky),
- používat All-Hazard-Approach, tj. zvažovat i plíživé pohromy, spojené např. s: nedostatečnou údržbou složitých technologických zařízení; nedostatečnou modernizací složitých technologických zařízení, která je nutná kvůli stárnutí materiálu i zastarávání přístupů pro zvládnutí problémů; nedostatečnou reakcí na nové zdroje rizik, nedostatečnou výchovou a vzděláváním personálu, korupci, insiders, terorismus atd.,
- zajistit, aby v projektu, výstavbě a provozu složitých technologických zařízení byl správně založen a během času zdokonalován koncept Defence-In-Depth, (Ochrana do hloubky je klíčovým principem využívaným při zajištění bezpečného a spolehlivého provozu složitých technologických zařízení. Aplikuje prevenci založenou na fyzických bariérách a řídí se obecně následujícími principy: konzervativnost při návrhu, konstrukci, výrobě a montáži, dosahovaná používáním ověřených a spolehlivých metod (podporuje kvalitní odezvu na projevy externích jevů, včetně zapojení systémů kontroly a řízení do odezvy); program zajištění jakosti užívaný při všech provozních činnostech (s výrazným pozitivním

preventivním dopadem na kvalitu odezvy na projev externí události vysoké intenzity); uvážení selhání lidského činitele, kdy při všech provozních i speciálních činnostech je počítáno s lidským faktorem a tomu jsou podřízena opatření k zajištění spolehlivosti a bezpečnosti provozu (v oblasti externích událostí často nebyla tato oblast historicky budována ve stejné míře jako pro interní události a je zde velký prostor pro metodický vývoj); spolehlivostní a bezpečnostní rozhodování (s rostoucím uplatněním spolehlivostně a rizikově orientovaného rozhodování u externích událostí); radiační ochrana; zpětná vazba, včetně využití zkušeností z provozu výměnou informací mezi různými zástupci provozované technologie a platforem IAEA či WANO, což je u vzácných externích událostí vysoké intenzity velmi důležitý princip).

- zajistit, aby v projektu, výstavbě a provozu složitých technologických zařízení byly využity progresivní typy bezpečnostních přístupů (aplikovatelné i v rámci odezvy na externí události a mající pro zvládnutí závažných externích událostí vysoké intenzity ještě větší význam než pro "standardní" události interní), a to: inherentní bezpečnost, jež předpokládá využití základních fyzikálních principů fungování dané technologie, které samy a priori vyloučí možnost havárie; pasivní bezpečnost, jež předpokládá využití fyzických zábran, které zmírní následky případných havárií a spolu s bariérami zabrání úniku nebezpečných látek i v případě, že by selhala veškerá aktivní bezpečnostní havarijní technika; a zálohování technických systémů představuje velmi rozmanitou množinu řešení. Již samotný pojem zálohování v sobě obsahuje očekávání, že máme k dispozici něco navíc, co nám umožní překonat kritickou situaci. Při zálohování se setkáváme s pojmem redundance (nadbytečnost) a diverzita (rozmanitost). Každé zálohování vždy představuje redundantnost, ale ne vždy diverzitu, pokud se jedná o použité prostředky zálohování. Při návrhu redundantních systémů je třeba mít na zřeteli celou řadu aspektů, a to např. skutečnost, že zvyšují složitost systému, čímž vznikají možnosti neočekávaných propojení, které jsou příčinou nežádoucích jevů nebo celých kaskád takových jevů).
- cílit na integrální bezpečnost a respektovat vznik atypických i normálních havárií (kritické prvky vybírat s ohledem na bezpečnost, hodnotit a vypořádávat průřezová rizika, která jsou příčinou kaskádovitých selhání či změny podmínek pro procesy, které mohou reagovat na změny podmínek nežádoucím způsobem a být příčinou velkých ztrát a škod; zvažovat všechny existující zranitelnosti: technické, organizační, kybernetické a místní; zavést kvalifikované postupy pro zvládnutí všech dílčích rizik, která přispívají do integrálního rizika a všech průřezových rizik. Uvědomovat si, že je lépe vědět o riziku, které z různých důvodů (jakými jsou nedostatek znalostí, financí, techniky, času, personálu aj. faktorů) není zvládnuté a připravit si plán odezvy na řešení možných kritických situací než si hrát na mrtvého brouka. Z reálného pohledu je zřejmé, že všechna rizika nikdy nezvládneme úplně – viz Perrow – Normální havárie, a proto je třeba respektovat zásady TQM, na kterém jsou založeny normy a standardy, dle kterých je třeba prioritní rizika monitorovat a mít pro ně mít připraven plán odezvy ve variantách, protože jak charakter dopadů, tak disponibilita zdrojů, sil a prostředků se v čase mění. Velkou pozornost je třeba věnovat automatizovaným systémům řízení a dohledu (jako je třeba SCADA). Nerozluštitelnost chování systému spočívá v tom, že systémy: jsou vystaveny skrytým propojením, která mohou neutralizovat zálohování, spojky, firewalls, a tím vytvořit situace, pro které inženýři nepřipravili rozumný postup. Kaskádová selhání mohou akcelerovat ztrátu kontroly, zmást obsluhu a odepřít možnost obnovy normálního režimu.
- postupovat proaktivně, přitom domýšlet možné důsledky a správně určovat priority veřejného zájmu, a respektovat proměnnost procesů v čase,
- cílit na zvládnutí problémů, přitom zvažovat různé synergie a zachovávat ostražitost z důvodu neurčitostí, které vyplývají ze složitosti technologických celků a z proměnnosti okolního světa,

- při stanovení opatření a činnosti na vypořádání rizika (část rizika se sníží, tj. preventivními opatřeními se odvrátí realizace rizika; část rizika se zmírní, tj. zmírňujícími opatřeními a připraveností (zpracování scénářů odezvy, zajištění zásob pro odezvu, instalace a provoz varovných systémů a jiná opatření nouzového a krizového řízení) se sníží nebo odvrátí nepřijatelné dopady; část rizika se pojistí; část rizika, pro kterou se připraví rezervy na odezvu a obnovu; část rizika, která je neřiditelná nebo příliš nákladná nebo málo častá, pro kterou se připraví plán pro nepředvídané situace (contingency plan) postupovat odpovědně a respektovat veřejný zájem,
- v případě, že riziko není přijatelné, provést vhodná opatření či činnosti (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; retence rizika),
- zahrnovat poznatky o rizicích jako nedílnou součást do podkladů pro rozhodování o chování složitých technologických zařízení v čase - propojení technické, operativní, taktické a strategické úrovně v čase musí být průhledné a jasně zacílené (brát v potaz, že existují rizika dvou druhů, a to: rizika spojená s dynamickým vývojem systému, tj. s procesy, které produkují jevy, které mají nepřijatelné dopady na systém, který řídíme; a pak i rizika spojená s aplikací vybraného způsobu hodnocení variant řešení, které v procesu řízení provádíme. Druhý typ rizika vzniká obvykle z dále uvedených důvodů: nepochopení problému a špatná formulace problému; neúplnost dat a nekvalifikované či neúplné vyjádření podstatných vlastností objektu či předmětu hodnocení; způsob tvorby variant řešení; způsob provedení multikriteriálního hodnocení variant; a náhodné okolnosti. Chyby tohoto druhu nelze obvykle vyloučit při konkrétním hodnocení. Lze je snížit pomocí týmu expertů, kteří splňují kritéria kladená na experty. Chyby z této fáze se bohužel přenáší do nouzových a krizových plánů a snižují jejich efektivitu),
- v každém procesu rozhodování o složitých technologických zařízeních zvažovat znalosti o rizicích (musí sledovat priority složitých technologických zařízení i veřejný zájem), tj. při každém rozhodování o rizicích explicitně zvažovat nejistoty a neurčitosti v procesech a podmínkách složitých technologických zařízení a jeho okolí,
- činnosti a opatření identifikované ke snížení či zmírnění rizika provádět systematicky a strukturovaně (a to na všech úrovních – zajistit specifickým procesem pro řízení bezpečnosti (PSM), který má dohled nad všemi procesy v složitých technologických zařízeních),
- zajistit, aby činnosti a opatření identifikované ke snížení či zmírnění rizika byly včasné a vhodně reagovaly na různé změny (stárnutí materiálu, zastarávání zařízení, komponent a postupů, poruchy, skoro nehody, nehody a havárie),
- zajistit, aby při každém návrhu a realizaci opatření a činností ke snížení rizik se přihlíželo k místním podmínkám a úpravám provedeným v minulosti,
- zajistit, aby při vypořádání rizik byl brán zřetel na vliv člověka, tj. lidský faktor (a to jak u provozních operací, tak při rozhodování o provozních procesech na všech úrovních řízení, tj. respektuje tzv. „Zlatá pravidla řízení rizik“),
- zajistit schopnost neustálého zlepšování kvality opatření a činností na snížení rizik (tj. vyžadovat od zúčastněných aktivní přístup k řešení problémů a odpovědnost; zpracovat program na zvyšování bezpečnosti složitých technických děl v čase a postupovat dle něho),
- zajistit odborné rozhodování a odbornou realizaci opatření na vypořádání rizik (musí je provádět systémoví inženýři, kteří nemusí být experty na všechny aspekty systému, ale musí rozumět podsystémům a různým jevům v nich natolik, aby byli schopni popsat a modelovat

jejich charakteristiky, pochopit důsledky a dle toho navrhnout opatření a postup jejich realizace).

B2. Zásady pro řízení rizik složitých technických děl z pohledu nároků na data, metody a techniky, které zajišťují kvalitní rozhodování a řízení - pro vlastníka, investora, provozovatele, odborný management, zaměstnance a kontraktory jsou:

- zajistit, aby při sestavování zadávacích podmínek, provozních předpisů a dalších řídících dokumentů se vycházelo z relevantních souborů dat a z aplikace ověřených metod, které zaručují výsledky se stanovenou vypovídací schopností. Jsou nástroje a techniky pro: lineární procesy; stromové procesy; procesy odehrávající se v síti; a procesy nestrukturované (DSS). (Např. pro řízení složitých technologických zařízení používat model PSA pro řízení rizik zacílené na bezpečnost (tj. nestačí model používaný pro řízení spolehlivosti, který kopíruje architekturu výrobního zařízení, a tím se nevidí interdependences, ani v objektu, ani mezi objektem a okolím; PSA zacílená na bezpečnost ukazuje úroveň kritičnosti provozu, slabá místa v systému, ve kterých je třeba navrhnout opatření a prokázat zvýšení bezpečnosti, a navrhuje způsob více bezpečného provozu pomocí kvalifikovaného programu údržby; stanovení veličin, ze kterých se určuje riziko – např. určení ohrožení, tj. o velikosti pohrom, která představují nepřijatelné dopady na složitá technologická zařízení - musí být použity dostatečně dlouhé časové řady, vysoce konzervativní expertní odhady; při stanovení rizika se musí počítat se selháním bezpečnostních opatření a ochranných systémů). Tj. zajistit, aby při sestavování zadávacích podmínek, provozních předpisů a dalších řídících dokumentů byly používány odpovídající míry rizika, tj. nelze používat indikátory,
- zajistit, aby u každého procesu, který má potenciál způsobit jevy, jejichž důsledkem jsou ztráty, škody a újmy na chráněných aktivech složitého technologického celku nebo okolí, bylo zvažováno, zda jsou či nejsou proměnné v čase,
- zajistit, aby při výběru metod a při interpretaci výsledků zpracování dat byla respektována skutečnost, že řada matematických metod má jisté předpoklady, které musí být splněny, aby výsledky byly správné, když nejsou splněny, tak dochází k chybnému stanovení hodnot rizika, a také k chybám v odezvě (požadavky na homogenitu, správnost a validitu datového souboru; rozmanitost procesů, které vedou k realizaci rizika - v čase to často neplatí. Něco lze opravit aplikací – deterministický přístup – nejméně příznivá hodnota; pravděpodobnostní přístup - medián, medián ± σ, medián ± 2σ, medián ± 3σ; heuristický přístup – několik variant procesu s nestejným rozdělením pravděpodobnosti); praktické uplatnění pravděpodobnostních metod se střetává s mnohými nedostatky, které se postupně odstraňují. Nejdůležitější nedostatky jsou: neurčitosti v charakteristice kritického stavu; nejistoty teoretických modelů základních veličin; a nedostatečný zřetel k následkům poruch),
- zajistit, aby při rozhodování o přijetí, či nepřijetí opatření na zvýšení bezpečnosti složitých technologických zařízení byly zvažovány neurčitosti v periodách opakování závažných pohrom, tj. aby byly používány metody pro posouzení interdependences, tj. multikriteriální přístupy a řešit otázky spojené s konfliktními kritérii,
- zajistit respektování výsledků vývoje poznání o způsobu práce s rizikem,
- zavést do praxe techniky reakce na možné lidské chyby při stavbě, konstrukci, montáži, provozu a řízení; mechanická selhání komponent nebo celého systému; stárnutí prvků, komponent, zařízení, systémů; zastarávání postupů ve světle nových poznatků a poučení z havárií; chyby obsluhy i úmyslné útoky,
- orientovat pozornost na správná kritická aktiva složitých technologických zařízení a na prioritní pohromy, které jsou příčinou realizace závažných rizik, tj. aplikovat kvalifikované metody pro určení: kritických položek složitých technologických zařízení; kritických

pohrom; kritického personálu; kritických činností, a to při provozu, opravách i obnově (Rozlišovat dva typy kritických položek, a to: položky, které pouze způsobují eskalaci dopadů pohrom, buď všech, nebo jen některých, které jsou možné v daném místě; a položky, které zaručují funkčnost systému, tj. bezpečnost a rozvoj chráněných aktiv. Jejich selhání způsobená nějakou pohromou nebo provozními aspekty vedou k závažným dopadům na chráněná aktiva. U prvního typu se při obnově provádí zodolnění položky vůči pohromám, které v daném případě vyvolaly nebo mohou vyvolat nepřijatelné dopady. Provádění jejich obnovy nemá žádnou prioritu z pohledu funkčnosti území / objektu / státu apod. U druhého typu se již v územním plánování, projektování, výstavbě i provozování provádí opatření, která vedou ke zvýšení jejich technické spolehlivosti. Používají se různá opatření i zálohování činností jinými položkami, která vedou k vyšší odolnosti vůči možným pohromám. Proto při obnově je třeba provést opatření jak v oblasti zálohování, tak v oblasti zodolnění. Protože předmětné položky jsou životadárné pro složitý technologický celek, existují priority v obnově, přičemž je třeba, aby veřejný zájem byl upřednostněn před soukromými zájmy),
- zajistit, aby při hodnocení kritičnosti složitých technologických zařízení byly používány otázky: Jak složité technologické zařízení reaguje na určité typy pohrom?; Jak je složité technologické zařízení masivní, odolné a pružné?; Jak se chování složitého technologického zařízení může zlepšit?; Jaké jsou vhodné mechanizmy řízení bezpečnosti složitého technologického zařízení?; Jaká pravidla se mohou využít pro samoregulaci nebo pro přípustné odchylky?; Které části složitého technologického zařízení jsou kritické?
- zajistit zpracování plánu řízení rizik, aby byla zajištěna rychlá reakce a při odezvě na závažnou havárii bylo připraveno řešení možných konfliktů mezi provozními inženýry a bezpečnostními složkami zacílenými na ochranu lidí.

B3. Zásady pro řízení rizik složitých technologických zařízení z pohledu postupů pro správné umístění, kvalitní projekt, výstavbu a provoz - pro vlastníka, investora, provozovatele, odborný management, zaměstnance a kontraktory jsou:
- zajistit, aby rizika byla sledována a správně vypořádávány během celého životního cyklu složitých technologických zařízení,
- zajistit, aby v každé fázi životnosti složitých technologických zařízení se používala adekvátní opatření pro ovládnutí rizik (Rizika se ovládají na základě: Technických opatření pomocí - výběru materiálu pro stavbu a zařízení, způsobů konstrukce, 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, vložení ochran důležitých prvků; Různých typů řídicího systémů, které podle výsledků kontinuálního monitoringu upravují provoz; Organizačních opatření, která mají jak ochránit zaměstnance, pracovní a popř. i okolní prostředí od škodlivých dopadů, tak stavby a zařízení od velké destrukce, protože technologické celky nejsou levné a pro zachování schopnosti rozvoje jsou jejich výrobky žádoucí) s tím, že se bere v úvahu skutečnost, že technická opatření mají nejvyšší účinnost,
- prosadit orientaci na kritické položky, tj. sledovat a ovládat kritické aspekty technických systémů zajišťujících konzistenci operací systémů složitých technologických zařízení,
- vycházet z prověřených parametrů kvality, které se objevují již v návrhu projektu,
- respektovat kvalitní inženýrské postupy (tj.: aplikace znalosti matematiky, vědy a inženýrství; návrhy a realizace experimentů; sběr, analýza, hodnocení, zpracování a interpretace dat; návrh komponent a celého systému; podle požadavků a v rámci omezení plynoucích z disponibilních zdrojů, sil a prostředků formulovat a řešit inženýrské problémy; efektivní komunikace mezi experty z různých oborů, aby se zaručila optimální bezpečnost

a optimální náklady; pochopení dopadů inženýrských řešení v širším kontextu; aplikace nejmodernějších nástrojů a metod z inženýrské praxe – inženýrská dobrá praxe; profesionální a profesní odpovědnost; vedení interdisciplinárních týmů) a o průkazy správnosti zvolených postupů v daných podmínkách.

- využívat analýzy kořenových příčin poruch a selhání ke zlepšování opatření na zvládání rizik,
- respektovat priority, které se stanovují podle kritičnosti dopadů realizovaných rizik na procesy, poskytované služby a na veřejná aktiva, tj. priority stanovené podle úrovně rizika určují intenzitu prací s rizikem a velikost příslušné dokumentace,
- zajistit kvalitní monitoring chování složitých technologických zařízení, ve kterém jsou uvedena opatření a činnosti technické a organizační, standardizace operačních postupů nebo automatizované kontroly pro korekci nepřijatelných rizik,
- vyžadovat, aby u všech převzatých technologií byly splněny požadavky transferu pro posuzování odolnosti, zranitelnosti, provozuschopnosti, spolehlivosti a dalších vlastností složitých technologických zařízení, když se použijí techniky odvozené jinde, protože i zde může být zdroj neočekávaných škodlivých jevů, které způsobí ztráty složitým technologickým zařízením,
- opatření na snižování rizik a postupy jejich realizace zakomponovat jako nedílnou část SMS, ve kterém se kloubí optimálním způsobem důležité aspekty technické, organizační, právní, bezpečnostní, finanční, manažerské, znalostní, vzdělávací, mezinárodní apod. (SMS představuje všeobecný systém řízení složitých technologických zařízení, který zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů ve složitých technologických zařízeních a jejich okolí. Opírá se o koncepci prevence pohrom či alespoň o zmírnění jejich závažných dopadů, která zahrnuje povinnost zavést a udržovat systém řízení, ve kterém jsou zohledněny dále uvedené problémy: role a odpovědnosti osob složitých technologických zařízení podílejících se na řízení závažných ohrožení od pohrom na všech organizačních úrovních složitých technologických zařízení a opatření na zajištění výcviku, která jsou sladěna s identifikovanými potřebami výcviku; plány pro systematické identifikování závažných ohrožení od pohrom a z nich plynoucích rizik pro složitá technologická zařízení, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti); plány a postupy pro zajištění bezpečnosti všech komponent a funkcí v složitých technologických zařízeních, a to včetně údržby objektů, zařízení; plány na implementaci změn v složitých technologických zařízeních, objektech i zařízeních zaměřených na prevenci; plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na takové nouzové situace; plány pro probíhající hodnocení souladu s cíli vyjasněnými v koncepci bezpečnosti složitých technologických zařízení a SMS a mechanismy pro vyšetřování a provádění korekčních činností v případě selhání zařízení nebo komponent s cílem dosáhnout stanovené cíle; a plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků),
- zajistit, aby opatření na vypořádání rizik byla prováděna všemi zúčastněnými dle koordinace procesem PSM: řídící tým složitých technologických zařízení, pracovníci složitých technologických zařízení, veřejná správa, a veřejnost,
- zajistit, aby při návrhu a realizaci opatření a činností na odvrácení a zmírnění rizik se používal odborný přístup, tj. musí zvažovat kritické atributy kvality a kritické parametry procesů v složitých technologických zařízeních, tj. respektovat, že zajištění bezpečnosti složitých technologických zařízení vyžaduje systematický přístup, jehož model je: 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, aplikovat opatření pro ochranu; periodicky kontrolovat stav; udržovat ochranu na odpovídající úrovni; a revidovat opatření v závislosti na vývoji,
- zaměřovat se i na požadavky uživatelů a na úroveň poskytovaných služeb.

B4. Zásady pro řízení rizik složitých technologických zařízení z pohledu zajištění kontinuity provozu a podpory základních funkcí státu, tj. veřejného zájmu – pro vlastníka, provozovatele, odborný management, zaměstnance a kontraktory jsou:
- zásady uvedené v A5,
- zajistit existenci složitých technologických zařízení po celou dobu životnosti a návrat zabraného území do dalšího užívání, tj. zachovat integritu složitých technologických zařízení i koexistenci s okolím, tj. mít schopnost měnit své chování podle podmínek (tj. zajistit schopnost složitých technologických zařízení měnit své chování tak, aby chování reagovalo na chování a orientaci dalších systémů v okolí a aby je neohrožovalo a ony neohrožovaly jeho. To znamená, že musí upřednostnit řízení bezpečnosti (ve smyslu integrální) před řízením spolehlivosti, tj. uvědomit si konflikt mezi výkonností složitých technologických zařízení a výší rizika, a dle něho řídit životnost složitých technologických zařízení při provozu),
- brát v úvahu, že složitých technologických zařízení je SoS, tj. má specifické vlastnosti jako nelinearitu, různé ustálené stavy (atraktory), katastrofické chování, chaotické chování atd., které jsou příčinou průřezových rizik, které narušují bezpečí sledovaného SoS i bezpečí okolí SoS,
- sledovat u složitých technologických zařízení komponenty a funkce; bezpečnost, spolehlivost, funkčnost a interoperabilita; interakce systém-člověk, splnění či nesplnění požadavků norem a standardů,
- při posuzování závažnosti každého jevu spojeného se složitými technologickými zařízeními zajistit kvalifikované odpovědi na otázky: jaké ztráty, škody a újmy budou na chráněných aktivech?; jak často se to stane?; jak zareagují bezpečnostní systémy v území?; jaké ztráty, škody a újmy budou na chráněných veřejných aktivech, když selžou bezpečnostní systémy? Poslední otázka je zásadní, protože často je bezmezná víra v bezpečnostní systémy,
- respektovat závěry inspekcí státu, IAEA a doporučení OECD / NEA, WANO aj.
- vyžadovat rozvoj kultury bezpečnosti, ve které je kladen dostatečný důraz na prevenci chyb při provádění technických úkonů i organizačních havárií (zajistit kontinuální vzdělávání personálu, a to především kritického).
- při stanovení opatření a činností na ošetření rizika respektovat adekvátně úroveň poznání (pro práci s riziky je nutné: rozumět procesu vzniku pohrom a podmínkám, ve kterých proces probíhá; znát, kde pohroma může vzniknout a jaké má fyzikální a jiné charakteristiky; identifikovat ohrožení od pohromy dle stanovených standardů; stanovit dopady pohrom o velikosti ohrožení na chráněná aktiva; eliminovat nepřijatelné dopady pohrom tam, kde to jde za přijatelných nákladů; u zbylých dopadů vypočítat pomocí prognostických modelů pravděpodobnost jejich realizace s tím, že se vezmou v úvahu i možná selhání preventivních opatření; vypočítat možné škody na chráněná aktiva v konkrétním území podle chráněných aktiv, které jsou skutečně v území a na základě pravděpodobností určit výši rizika; identifikovat a realizovat zmírňující opatření s ohledem na lidi, majetek a životní prostředí byla ALARP (tak malá, jak je rozumně možné dosáhnout); a prokázat, že byla provedena všechna opatření k zabránění a zmírnění dopadů pohrom),
- při návrhu redundantních systémů mít na zřeteli celou řadu aspektů, a to např. skutečnost, že zvyšují složitost systému, čímž vznikají možnosti neočekávaných propojení, které jsou

příčinou nežádoucích jevů nebo celých kaskád takových jevů, neznámých, neplánovaných nebo neočekávaných sekvencí jevů, které nejsou viditelné nebo okamžitě srozumitelné, nebo i selhání v okolí složitých technologických zařízení, tj. představují zdroj nového rizika, které se realizuje neočekávaně za jistých podmínek,

- pro bezpečný provoz složitých technologických zařízení zajistit permanentní speciální péči o opatření na vypořádání rizik v kritických zařízeních a kritických komponentách, v implementaci preventivní údržby, v řešení konfliktů mezi rizikem a výkonností, implementaci korektivních opatření z důvodu bezpečnosti; zde se občas nutno řešit konflikt mezi spolehlivostí a bezpečností v integrálním pojetí,
- zajistit správnou reakci na nečekané, tj. neplánované, neznámé, neočekávané a náhlé situace, které mohou vzniknout kvůli složitým propojením i přeskokem přes rozhraní systému nebo příliš těsným propojením prvků, komponent a systémů, tj. připravit postupy na zabránění vzniku kaskádovitých selhání a akcelerace fyzikálních procesů a při jejich vzniku na jejich rychlé zastavení,
- používat indikátory, které jasně ukazují, zda dochází ke zvyšování bezpečnosti a zda trend zvyšování bezpečnosti je dostatečný. Přitom musí vycházet z dat o: souboru relevantních pohrom pro složitá technologická zařízení; provozuschopnosti složitých technologických zařízení; integritě fyzických a kybernetických bariér složitých technologických zařízení; kvalitě a dostatečnosti havarijní připravenosti,
- respektovat průběžná data o stavu okolí složitých technologických zařízení a o aktuální velikosti rizik složitých technologických zařízení a podle nich upravovat proces řízení a vypořádání rizik v čase, tj. nastavení vhodných zpětných vazeb v procesním modelu pro nakládání s riziky,
- při provozu stále vycházet z nových poznatků o pohromách a o způsobu ochrany složitých technologických zařízení před jejich dopady, a vyžadovat realizaci relevantních opatření,
- jelikož snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, kvalifikovaných lidí apod. (proto se v praxi hledá hranice, na kterou je únosné snížit riziko tak, aby vynaložené náklady byly ještě rozumné), tak lze použít ALARP či ALARA s tím, že při aplikaci bude vyžadován průkaz, že byla provedena všechna opatření k zabránění a zmírnění dopadů pohrom.
- vycházet ze scénářů průřezových rizik a mít připraveny postupy na zabránění vzniku kaskádovitých selhání a akcelerace fyzikálních procesů, a při jejich vzniku mít opatření na jejich rychlé zastavení,
- být po celou dobu životnosti efektivní, tj. mít schopnost vyrovnat se s nedostatkem zdrojů (jde o vypořádání nejen technických a bezpečnostních rizik, ale i rizik kreditních, tržních a provozních spojených se změnou legislativy či změnou daní),
- mít po celou dobu životnosti dostatečnou volnost, tj. mít schopnost dobře zvládat výzvy z okolí (vnější pohromy), tj. mít připraveny plány pro řízení rizik, ve kterých budou specifikovány opatření odezvy a odpovědnosti za provedení opatření,
- po celou dobu životnosti zajišťovat bezpečí složitých technologických zařízení, tj. vytvářet schopnost ochránit se před jevy, které jsou uvnitř i vně,
- po celou dobu životnosti zajišťovat integritu složitých technologických zařízení, tj. technickou provozuschopnost složitých technologických zařízení (Integrita bezpečnosti se vztahuje ke schopnosti systému dosáhnout požadovaných bezpečnostních funkcí. V zásadě lze odlišit dva režimy činnosti systémů souvisejících s bezpečností. Prvním je režim, kdy systém vyčkává a teprve v případě, že vznikne potřeba zásahu, realizuje bezpečnostní funkci. Druhým je režim, kdy systém trvale nebo často realizuje bezpečnostní funkci. Typickým reprezentantem systémů pracujících na vyžádání jsou ochranné a zabezpečovací systémy. Reprezentantem systémů pracujících v režimu s vysokým nebo nepřetržitým vyžádáním jsou například systémy regulace fyzikálního parametru technologického

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

- po celou dobu životnosti zajišťovat adaptabilitu složitých technologických zařízení na vnější změny bez porušení integrity,
- po celou dobu životnosti zajišťovat schopnost složitých technologických zařízení překonat nejen abnormální a kritické podmínky, ale i málo pravděpodobné kruté nouzové situace, tj. kromě standardních opatření odezvy mít i nadstandardní opatření a rezervy pro minimalizaci lidských ztrát, prevenci ztrát při odezvě a obnově, překonání obtíží a pro obnovu složitých technologických zařízení (tím se zamezí jak ztrátě konkurenceschopnosti vlastníků složitých technologických zařízení, tak ztrátě ekonomického potenciálu území a nadměrným výdajům veřejné správy na podporu nezaměstnaných),
- po celou dobu životnosti zajišťovat neustálé zvyšovat kulturu bezpečnosti, tj.: omezovat nebezpečné nebo neproduktivní pracovní praktiky, které se zjistí studiem nehod; využívat pozitivní zpětnou vazbu z auditů řízení, auditů bezpečnosti, auditů nebezpečných dějů, auditů chemických reakcí, zpráv o nehodách a skoro nehodách a monitoringu dodržování všech bezpečnostních opatření pro prevenci a zmírnění nehod; na základě kritické analýzy havárií dělat 3 úrovně doporučení pro zabránění haváriím, a to: bezprostřední technická doporučení, doporučení pro zabránění vzniku bezprostředního nebezpečí, a doporučení pro řízení zaměřená na primární příčiny nehod; zajistit plány odezvy na možné havárie a zajistit schopnost provést obnovu technologického celku s tím, že se vezme v úvahu, že při obnově rozhoduje: kvalita znalostí o konkrétních rizicích v daném konkrétním místě, kvalita řízení konkrétních rizik v daném konkrétním místě, a kvalita vypořádání konkrétních rizik v daném konkrétním místě pomocí kvalifikovaných inženýrských disciplín; jelikož vždy existuje několik závažných pohrom, kterým je třeba věnovat pozornost z pohledu rizika (ze zkušenosti obvykle 7 – 8) a opatření vůči některým pohromám jsou konfliktní, je třeba kombinace opatření a činností, které zvyšují četnost výskytu pohromy nebo eskalují dopady pohromy. Následně je třeba pro potřeby praxe provést optimalizaci založenou na řízení konfliktů.
- po celou dobu životnosti zajišťovat schopnost plnit v dostatečné kvalitě úkoly, i když dojde k omezení zdrojů, sil a prostředků (Prevence ztrát při obnově znamená: vytvořit koncepci prevence ztrát při obnově; identifikovat a vyhodnotit všechny možné pohromy a jejich možné dopady na technologický celek; určit priority obnovy; vytvořit skupiny programů, které minimalizují možné ztráty. Při plánování obnovy složitých technologických zařízení po havárii je nutno zvážit, že: náklady na obnovu závisí i na době trvání obnovy; a při dlouhotrvající obnově jsou velké dopady na společnost. Proto je třeba vybudovat systém, ve kterém obnova navazuje na odezvu. Do identifikace vnitřních zdrojů a schopností složitých technologických zařízení provést kvalifikovanou odezvu a obnovu patří problémy spojené s personálem, zařízením, objekty, organizační schopností (výcvik, evakuační plány apod.), záložními systémy (pro komunikaci, výrobu, nouzové zdroje energii, vodu atd.). Při přípravě kvalifikované odezvy a obnovy složitých technologických zařízení je třeba zvažovat: fyzickou polohu složitých technologických zařízení a místní poměry, tj. rozmístění veřejných aktiv a zdrojů domino efektů; klimatické podmínky místa, kde se

technologický celek nachází; a blízkost a dostupnost bezpečných míst a míst, ze kterých se odezva na pohromu a obnova řídí).

6.3. Shrnutí

Ze systémového hlediska je pro zajištění bezpečnosti technického díla třeba sledovat:

1. Informační činnost pro podporu rozhodování, protože stav bezpečí je výsledkem racionálního rozhodování, dobrých informací a správně provedených účinných činností. Je však třeba počítat s dopady na rozhodování o bezpečí jako jsou různá omezení (institucionální, právní, organizační), vlivy médií a veřejného mínění a dimenze politické (zájmové skupiny, ideologie) a technologické. Je třeba zavést povinnost investora a později provozovatele technického díla předkládat a po celou dobu životnosti obhajovat věcnými argumenty, že technické dílo je bezpečné.
2. Zařízení podporující bezpečnost, což jsou zařízení, technologie a organizační složky.
3. Lidi jako subjekty bezpečnosti (experti a manažeři bezpečnosti), lidé jako objekty bezpečnosti (ochrana a prevence).
4. Procedury spojující lidi a strukturu technického díla.

Ze systémového pohledu jsou chráněnými aktivy technického díla také vazby a toky mezi chráněnými aktivy.

V rámci řízení rizik technického díla je třeba kvalitně provést pět klíčových aktivit, a to:

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

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

- vyhnutí se riziku, tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika, když to jde,
- odstranění zdrojů rizik, tj. zabránění vzniku pohrom, když to jde,
- snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom, když to jde,
- snížení závažnosti dopadů rizika, tj. příprava zmírňujících opatření jako jsou varovací systémy, systémy odezvy a obnovy,
- sdílení rizika, tj. rozdělení rizika mezi zúčastněné a pojišťovny,
- retence rizika.

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

- část rizika se sníží, tj. preventivními opatřeními se odvrátí realizace rizika,

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

K tomu se rovněž připojuje rozdělení zvládání rizik mezi všechny zúčastněné. Rozdělení ve správném řízení se provádí tak, že se vychází z toho, že za zvládání rizik odpovídají všichni zúčastnění (od politiků přes pracovníky správy, vedení technických děl až po techniky a občany) a že zvládání konkrétního rizika se přiděluje tomu subjektu, který je na to nejlépe připraven. Při výběru opatření na zvládání rizik je třeba zajistit, aby náklady na zvládnutí rizik nepřevýšily možné škody vyvolané realizací rizika.

Zásady pro řízení rizik složitých technických děl na úseku propojení veřejné správy a managementu technických děl jsou stanoveny pro úrovně řízení státu: politickou (parlament, vláda, veřejná správa) - 4; strategickou (veřejná správa, vlastník, investor, provozovatel) - 8; taktickou (veřejná správa, vlastník, investor, provozovatel) - 4; operativní / funkční (provozovatel) - 5; a technickou (provozovatel) - 19.

Zásady pro řízení rizik složitých technických děl ve věcné oblasti na úsecích jsou pro úseky: koncepce technického díla a způsob řízení technického díla - 21; požadavky na data, metody a techniky, které zajišťují kvalitní rozhodování a řízení technického díla - 9; postupy pro správné umístění, kvalitní projekt, výstavbu a provoz technického díla - 13; a zajištění kontinuity provozu technického díla a podpory základních funkcí státu, tj. veřejného zájmu - 23.

Výše uvedené zásady byly prezentovány na seminářích a konferencích inženýrů, kteří navrhují, konstruují, provozují či kontrolují technická díla, např. semináře na ČVUT či konference TLAK2017 [9]; na mezinárodním poli pak přednáška na konferenci ESREL2017, která je otištěná v [392]. Implementace zásad do praxe byla vždy na všech akcích podpořena.

7. ZÁVĚR

Dodnes je skutečností, že při navrhování a provozování technologických systémů a při vytváření jejich bezpečnosti experti z různých oborů pracují odděleně, což nezaručuje ani optimální bezpečnost, ani optimální náklady. Často se stává, že jednotlivé podsystémy jsou bezpečné, protože pro ně existují standardy a normy (např. jednotlivé technické části určitého provozu), ale bezpečnost celku, který vznikl jejich propojením s kybernetickými a jinými infrastrukturami již sledovaná není, protože se hodnocení a prokázání bezpečnosti nepožaduje relevantní legislativou a navíc k danému účelu není dosud k dispozici relevantní odborný postup.

Jelikož v posledních letech došlo k velkým selháním energetických infrastruktur, jejichž dopady tíživě dolehly na lidi ve vyspělých zemích, EU soustředila své úsilí v oblasti výzkumu na pochopení vnitřních závislostí mezi podsystémy s cílem stanovit zásady pro zajištění bezpečnosti systému složeného z historicky vytvořených systémů, jejichž bezpečnost byla zajištěna tradičními přístupy; výsledky předmětného výzkumu jsou citovány a zváženy v předchozích kapitolách.

Bezpečnost technických děl je spojená s vyjednáváním s riziky. Integrální bezpečnost je spojená s vyjednáváním s integrálním rizikem, tj. nejenom s dílčími riziky (zaměřenými na jednotlivá chráněná aktiva), ale i s riziky, které souvisí s vazbami a toky mezi chráněnými aktivy. Snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, apod. Proto se v praxi hledá hranice, na kterou je únosné riziko snížit tak, aby vynaložené náklady byly ještě rozumné (viz principy ALARP, ALARA aj.). Předmětná míra snížení rizika je většinou předmětem vrcholového řízení a politického rozhodování, při kterém se využívají současné vědecké a technické poznatky a zohledňují se ekonomické, sociální a další podmínky. Proto je nutné znát zdroje rizik, dopady spojené s realizací rizik a také disponibilní zdroje, síly a prostředky pro jejich zvládnutí, aby škody, ztráty a újmy na chráněných aktivech byly únosné.

Rozvoj technologií objektů a infrastruktur směřuje stále více ke kombinaci jednotlivých zařízení a k tvorbě komplexních systémů s cílem dosáhnout zvýšení výroby a vysoké ziskovosti. Takto vytvářené systémy nejsou výsledkem expertů z jedné disciplíny (oboru), nýbrž jsou výsledkem interdisciplinárních týmů. Zvláště pro síťové technologie platí, že jednotlivý expert není schopen kompletně posoudit a ovládat velké technické systémy. Z hlediska potřeby zajistit udržitelný rozvoj lidské společnosti je předpokladem pro konstrukci předmětných komplexů ovládání jejich bezpečnosti. Je logické, že v komplexních systémech bezpečnostní funkce musí být zvažovány v souvislostech s ostatními funkcemi systému a jeho podsystémů. Tj. nestačí řešit jednotlivosti (tj. problémy bezpečnosti uvnitř jednotlivých podsystémů), ale je třeba řešit zároveň bezpečnost celku i bezpečnost jednotlivostí (tj. dílčích podsystémů). Přitom je třeba počítat s dále uvedenými ohroženími: vnější ohrožení (ohrožení od jevů v okolí systému); vnitřní ohrožení (ohrožení od vnitřních zařízení jednotlivých podsystémů); funkční ohrožení (ohrožení spojená se selháním funkcí celého systému nebo zařízení či komponent systému, tj. selháním podsystémů); ohrožení spojená s montáží; a lidská ohrožení (ohrožení spojená s lidskými činnostmi).

Je skutečností, že bezpečnost jednotlivých technologických sektorů závisí na bezpečnostních tradicích, které se vyvíjely určitou dobu v daném sektoru. Proto v celku složeném z několika sektorů jsou provedená bezpečnostní opatření různorodá a odpovídají znalostem a zkušenostem doby, ve které byly vytvořeny. Dodnes je skutečností, že při sestavování technologických systémů a při vytváření jejich bezpečnosti experti z různých oborů pracují odděleně, což nezaručuje ani optimální bezpečnost, ani optimální náklady.

Protože zdrojů, sil a prostředků na bezpečnost technických děl, tj. na řízení rizik s nimi spojených, není nikdy dostatek, je třeba z důvodů hospodárnosti postupovat následovně:

- rizika určovat jen pomocí dat a metod, které zajistí kvalitní podklady pro rozhodování o vypořádání rizik na příslušné úrovni řízení,
- na strategické úrovni řízení a inženýrského vypořádání rizik je nutné řešit rizika složitých technologických zařízení tak, že je chápeme jako SoS a naším cílem je zajištění dlouhodobé existence a rozvoje složitých technologických zařízení i jejich okolí,
- na taktické a funkční úrovni řízení a inženýrského vypořádání rizik je nutné řešit rizika složitých technologických zařízení způsobem zaměřeným na bezpečný systém,
- na technické a funkční úrovni řízení a inženýrského vypořádání rizik lze řešit rizika složitých technologických zařízení 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).

Analýza současné situace ukazuje, že umíme systematicky zvládnout řadu nežádoucích procesů, tj. poruch a selhání, které dokážeme předem odhalit. Někdy se však vyskytne vzájemné propletení řady zdánlivě nesouvisejících faktorů a v důsledku nelinearit v systému vznikají velmi atypické havárie (černé labutě, dračí králové atd.). Proto nyní připouštíme, že složité kritické objekty jsou z různých důvodů čas od času v nestabilním stavu a vznikají organizační havárie, kaskády selhání bez zjevné příčiny, neobvyklé jevy apod., tj. připouštíme nejistoty náhodné i epistemické (znalostní) v jejich chování.

Role řídících týmů provozujících složitá technologická zařízení je: 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; a provádět neustálé vylepšování bezpečnosti.

Z důvodu zajištění bezpečnosti kritických technických objektů a ochrany lidí musíme připravovat řešení odezvy pro možné případy, kdy se realizují rizika z příčin, které nelze odhalit pravděpodobnostními přístupy, a budovat pro ně náhradní zdroje vody a energie, specifické systémy odezvy a specifický výcvik inženýrů a záchranářů.

Pro dosažení rozumné úrovně bezpečnosti technologických celků je nutné do praxe zavést povinnost, aby deterministické, pravděpodobnostní a heuristické analýzy bezpečnosti byly prováděny pro všechna důležitá technická díla s větším rizikem; heuristické posouzení umožní identifikovat případy selhání, které nejsou identifikovatelné statistickými metodami, jde o postižení neurčitosti v chování technických děl za podmínek jiných než projektových, které jsou za jistých podmínek možné. Proto je nutný další rozvoj metod rizikového inženýrství pro analýzu poruch, které jsou nasměrované na určení rizik.

Správné řízení věcí veřejných, které z důvodů svého určení upravuje i bezpečnost technologických systémů, musí zajistit, aby bezpečnostní certifikáty byly vyžadovány u všech technologií se zvýšeným rizikem. To vyžaduje, aby se v praxi muselo provádět spolehlivé zvládání rizika pomocí preventivních opatření, která jsou ekonomicky rozumná. Z toho vyplývá, že technická legislativa musí být primárně orientovaná na soulad s cíli bezpečnosti, které znamenají jen přípustná / dovolená rizika. Pouze jako sekundární cíl legislativa může požadovat konkrétní technické kroky pro dosažení cílů bezpečnosti.

Legislativa musí rovněž zajistit, aby riziko spojené s technologickými celky bylo přijatelné především pro ty, kteří mohou být rizikem ovlivněni, tj. především zaměstnanci

technologických celků, občané žijící v okolí technologických celků a uživatelé produktů technologických celků.

Pro kritéria přijatelnosti rizika musí být sestaven mezinárodně přijatelný scénář, protože jen tak lze odstranit rozdíly způsobené rozdílností kultur a politických tradic. Podstata technologie a její globální rozšíření stěží dovoluje národně specifické řešení. Je zřejmé, že musíme zvažovat národní charakteristiky, být si vědomi hledisek dalších států a kulturního prostoru. Je třeba zvážit etické i ekonomické zájmy. Proto je důležitá mezinárodní spolupráce.

Je třeba mít na paměti, že každý systém obsahuje řadu inherentních zdrojů rizika. K selhání systému dojde, když v systému dojde k nežádoucímu procesu, který je nežádoucí proces iniciován buď nějakým očekávaným rizikem, anebo je spuštěn náhodnou kombinací několika málo pravděpodobných jevů. V podkladech pro řízení bezpečnosti se dosud druhá možnost často zanedbává. Dokladem jsou obvykle legislativní požadavky na bezpečnostní zprávy, které se ve vyspělých zemích musí zpracovávat pro technologické objekty a v řadě případů i pro důležité občanské objekty.

Pro všechny výše uvedené a další potřeby je třeba pro rozhodování mít namodelované možné situace ve variantním provedení; a to nejen pro situace při normálních podmínkách, ale i pro situace při kritických a extrémních podmínkách. Z hlediska bezpečí a rozvoje je třeba udělat takové znalostní, personální, materiální a technické zázemí, aby technické dílo při:

- kritických podmínkách neohrozilo ani sebe, ani své okolí, a bylo ho možno obnovit,
- extrémních podmínkách si zachovalo schopnost obnovy.

Protože úlohy spojené s dlouhodobými selháními důležitých technických děl a hlavně celých infrastruktur jsou rozmanité a značně různorodé, je třeba podle povahy úlohy sebrat data, vybrat vhodné metody jejich zpracování (metoda závisí na formátu, vlastnostech a vypovídací schopnosti dat) a udělat spolehlivé metody. Globálně bohužel nelze stanovit jeden postup, který vyřeší vše. Na základě shromážděných poznatků a zkušeností je třeba:

1. Zavést řízení území, které je zacílené na bezpečí a udržitelný rozvoj lidí s ohledem na dlouhodobá selhání velkých technických děl, hlavně infrastruktur na úrovni lokální, regionální, státní i evropské. Jde o: řízení rizik procesů spojených se zajištěním koexistence technického díla a okolí; řízení rizik procesů spojených s umístěním, výstavbou, konstrukcí a zahájením provozu technického díla; řízení rizik procesů spojených s provozem technického díla během životnosti; a řízení rizik procesů spojených s ukončením životnosti technického díla a předáním území do dalšího užívání.
2. Brát v úvahu, že sledovaný problém je mnoha oborový, interdisciplinární a vyžaduje znalosti, data, kvalitní strategické, taktické i operativní řízení založené na principech znalostního managementu. Proto v první fázi je třeba problém strukturovat tak, že jednotlivé odborné skupiny budou řešit to, co umí a budou vedeny týmem, který zajistí interoperabilitu jejich výstupů v území. To platí i o modelech, které musí vycházet ze stavu konkrétních znalostí o dílčích problémech a postupně být propojovány tak, aby byla zajištěna jejich kompatibilita a interoperabilita. Teprve posouzení kvality znalostí a kvality souboru disponibilních dat umožní pro jednotlivé problémy, uvedené výše, vybrat vhodné nástroje, které zajistí schopnost soustavy pracovat jak autonomně, tak ve větším celku s ohledem na požadovanou interoperabilitu.
3. Protože odpovědnost za přežití obyvatelstva je na veřejné správě, je třeba vytvořit nástroje pro podporu rozhodování veřejné správy v předmětné záležitosti. Protože bez relevantních dat žádnou ochranu obyvatelstva vůči žádné pohromě, a to včetně dlouhodobého výpadku elektroenergetické soustavy, nezajistíme, je třeba v první fázi zajistit kvalifikovaná data o dopadech dlouhodobých selhání elektroenergetické soustavy v konkrétních lokalitách, regionech a státu. Protože v ČR žádnou takovou databázi nemáme, tak v první fázi stačí nástroj What, If; vrstva GIS a několik časových úseků – 1 hodina, 3 hodiny, 1 den, 3 dny, 14 dní, 1 měsíc, 3 měsíce, 180 dní. Vytvoření cílené databáze vyžaduje určitou odbornost a

metodickou zručnost a je časově náročné. Výsledek však umožní kvalifikované řešení úkolů ochrany obyvatelstva ve variantách s ohledem na rozmanitou kombinaci náhodných jevů možných v konkrétním území. Vzhledem k tomu, že pohromy v nejširším pojetí, které je ve studii zvažováno, mají různou fyzikální podstatu, tak konkrétní dopady na elektroenergetickou soustavu se různí podle kombinace vlastností pohromy a místních zranitelností chráněných zájmů, proto databáze musí být sestavena odděleně pro jednotlivé možné pohromy. Podobné závěry platí i pro kybernetickou infrastrukturu.

4. Po sestavení databáze možných dopadů na důležitá technická díla v časoprostoru lze dělat modely nad územím, modely dopadů v časoprostoru a k nim pomocí základních kritérií pro přežití lidí určit potřeby ochrany obyvatelstva. Na jejich základě modelovat strom závislosti veřejných služeb ve variantách a podle těchto dat rozpracovávat například model zásobování, model chování obyvatelstva apod. (přitom aplikovat např. metody teorie grafů, metodu kritické cesty, síťové metody v deterministickém, stochastickém, fuzzy i expertním pojetí).
5. Do praxe zavést legislativu, která zajistí, že riziko spojené se selháním kritických infrastruktur, a to zvláště elektroenergetické, kybernetické, vodohospodářské a dopravní je přijatelné především pro ty, kteří mohou být rizikem ovlivněni, tj. především zaměstnanci a občané žijící v území, které je obsluhováno danou infrastrukturou. Pro kritéria přijatelnosti rizika musí být sestaven mezinárodně přijatelný scénář, protože jen tak lze odstranit rozdíly způsobené rozdílností kultur a politických tradic. Podstata technologie a její globální rozšíření stěží dovoluje národně specifické řešení. Je zřejmé, že musíme zvažovat národní charakteristiky, být si vědomi hledisek dalších států a kulturního prostoru, zvážit etické i ekonomické zájmy, a proto je důležitá mezinárodní spolupráce.
6. Protože odborný svět již více než 10 let řeší problémy systému systémů, je třeba zajistit kvalifikované vzdělávání a kvalifikovaný výzkum v předmětné oblasti i v ČR a upustit od toho, co je jednoduché a nevyžaduje úsilí a znalosti, protože podcenění složitosti a závažnosti problému by se mohlo nevyplatit a mohlo by v budoucnu přinést nemalé celospolečenské náklady.

V předmětném výzkumu je třeba pokračovat, protože ve výzkumu popsaném výše jsou z důvodu omezeného času, finančních prostředků a kapacit středem zájmu jen některé problémy.

Konkrétní uvedené výsledky v kapitole 5 ukazují, že bezpečnost složitých technologických objektů a zařízení nelze zajistit sebedokonalejšími dílčími opatřeními. Pro její zajištění je třeba zvažovat vlastnosti objektů, kterými jsou interoperabilita, kritičnost a integrita. Kvůli dynamickému vývoji světa a nedostatečným lidským znalostem a schopnostem, je třeba počítat s tím, že mohou nastat kritické situace. Proto je třeba se připravit na jejich zvládnutí s cílem, aby ztráty, škody a újmy na veřejných a dalších aktivech byly přijatelné. Předmětné nástroje poskytuje rizikové inženýrství, a proto je nutné je zavádět do praxe, a je třeba začít v oblasti vzdělávání.

Předložená kniha je tudíž ucelenou studií, která v určitém rozsahu na současné úrovni poznání řeší mezioborový vědecko-výzkumný problém s nejvyšší odbornou a společenskou prioritou „bezpečí a rozvoj lidí“. Obsah knihy přináší vizi komplexnosti, ve které řešení praktického problému je na hranici teorie chaosu, kde se uplatňují nelineární vazby mezi prvky různých objektů a sítí. Ukazuje zbytečnost izolovaného studia částí celku (uzavřený systém v neměnném prostředí), když cílem je zajistit bezpečná technická díla (tj. bezpečné celky). V souladu s tvrzení Bruce Schneiera [393] ukazuje, že zajišťování bezpečnosti je proces, ve kterém se aplikují opatření pro bezpečí lidí v proměnných podmínkách. Vysoká míra neurčitosti (znalostní nejistoty) neumožňuje uspokojující predikci chování složitého systému systémů v podmínkách, ve kterých vzniká mnoho pohrom vnitřních a vnějších a působí lidský faktor.

LITERATURA

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

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

[3] TAYLOR, F. *The Principles of Scientific Management*. ISBN 0-415-27983-6. Routledge 1911.

[4] FAYOL, H. *General and Industrial Management: Henri Fayol's Classic Revised by Irwin Gray.* Belmont: David S. Lake Publishers 1987.

[5] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. ISBN: 978-80-01-04841-2. Praha: ČVUT, Praha, 2011, 405p.

[6] PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládání*. ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234p.

[7] PROCHÁZKOVÁ, D. *Study of Disasters and Disaster Management*. ISBN: 978-80-01-05246-4. Praha: ČVUT 2013, 202p.

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

[9] PROCHÁZKOVÁ, D. Zásady řízení rizik složitých technologických zařízení. *TLAK 2017*. ISBN:978-80-871140-45-1. Líbeznice: Medim, spol. s.r.o. 2017, pp. 83-106.

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

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

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

[13] PROCHÁZKOVÁ, D. *Optimum Concept of Management and Trade-off with Risks.* In: Safety and Reliability: Methodology and Application. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, pp 1463-1471.

[14] HAIMES, Y. Y. *Risk Modeling, Assessment, and Management*. ISBN: 978-0-470-28237-3. John Wiley & Sons 2009. 1040p.

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

[16] PROCHÁZKOVÁ, D. Plány řízení rizik. In: *Požární ochrana 2014*. ISBN:978-80-7385-148-4. Ostrava: SPBI 2014, pp 282-291.

[17] PROCHÁZKOVÁ, D. Nástroj pro sestavení podkladů pro řízení bezpečnosti. In: *Bezpečnost 1 ochrana zdraví při práci 2011*. ISBN 978-80-248-2424-6. Ostrava: VŠB-TU 2011, pp. 57-169.

[18] PROCHÁZKOVÁ, D. Critical Infrastructure Safety Management. In: *Reliability, Risk and Safety. Theory and Applications*. ISBN 978-0-203-85975-9. Leiden: Balkema 2009, pp. 1875-1882.

[19] EU. *FOCUS project*. EU, 2012, http://www.focusproject.eu/documents/14976/-5d7 63378-1198-4dc9-86ff-c46959712 f8a

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

[21] EU. *The Safe Community Concept*. EU, 2004 Brussels, PASR project.

[22] NOWAKOWSKI T. et al. (eds). *Safety and Reliability: Methodology and Application.* ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, 2453p.

[23] SEVCIK, A., GUDMESTADO. T. Solutions and Safety Barriers: The Holistic Approach to Risk-Reducing Measures. In: *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, pp. 1438-1444.

[24] VATN, J. Structuring Contributors to Successful Operation. In: *Safety and Reliability: Methodology and Application*. ISBN 978-1-138-02681-0. London: Taylor & Francis Group 2014, pp. 1445-1453.

[25] IAEA. *Assessment of Defence in Depth for Nuclear Power Plants*. Safety report series No. 46. ISBN: 92–0–114004–5. Vienna: IAEA 2005, 119p.

[26] BRIEF, A. P., UMPHRESS, E. E., DIETZ, J., BURROWS, J. W., BUTZ, R. M., SCHOLTEN, L Community Matters: Realistic Group Conflict Theory and the Impact of Diversity. *Academy of Management Journal,* 48 (2005), 5, pp. 830-844.

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

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

[29] OECD. *Guiding Principles on Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2003, 192p.

[30] ICAO. *Safety Management Manual.* Order No. 98592006, 290p.

[31] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Data a metodika jejich zpracování pro potřeby inženýrských disciplín*. ISBN: 978-80-01-05792-6. Praha: ČVUT 2015, 186p.

[32] BORGES, HICKEY, C. Balancing Safety and Performance through QRA and RAM Analyses. In: *Safety and Reliability: Methodology and Applications*. ISBN: 978-1-138-02681-0. London: Taylor & Francis Group 2015, pp. 445-452.

[33] MAYERS, R. A. Encyclopedia of Complexity and Systems Science. ISBN:978-0-387-75888-6. Berlin: Springer 2009.

[34] REASON, J. *Human error*. Cambridge: Cambridge University Press, 1990.

[35] SAGAN, S. *The limits of safety.* Princeton: Princeton University 1993.

[36] TURNER, B. *Man-made disasters.* New York: Wykeham Science Press 1978.

[37] PERROW, CH. *Normal Accidents: Living with High-Risk Technologies.* Princeton: Princeton University Press 1999.

[38] PROCHÁZKOVÁ, D. Outline on Risk, Risk Management and Trade-off with Risks. In: *Risk of Processes and Their Management.* ISBN: 978-80-01-06144-2. Praha: ČVUT 2017, pp. 6-26.

[39] MOOS, P. MALINOVSKÝ, V. *Informační systémy a technologie.* Edice monografií NNW. ISBN: 80-903298-5-3. Praha: 2006.

[40] ISA. *ANSI/ISA–62443-1-1 (99.01.01)-2007.* Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models. EU: ISA 2007.

[41] NOVOBÍLSKÝ, P., KERTIS, T., PROCHÁZKOVÁ, D., PROCHÁZKA, J. Cyber security of metropolitan railway communication infrastructure. In: *Risks of Business and Territorial Processes*. ISBN: 978-80-7561-021-8. Ústí nad Labem: UJEP 2016, pp.78-91.

[42] SVOBODA, V. SVÍTEK, M. *Telematika nad dopravními sítěmi*. Praha: ČVUT 2013.

[43] MOOS, P. ZELINKA, T. MALINOVSKÝ, V. *Telekomunikační služby*. Praha: ČVUT 2007.

[44] PROCHÁZKOVÁ, D. *Challenges Connected with Critical Infrastructure Safety*. Saarbruecken: Lambert Academic Publishing 2014, 218p.

[45] KERTIS, T. Porovnání přístupů pro řízení bezpečnosti v dopravě. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 34-59.

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

[47] LEITL, R. *Spolehlivost elektrotechnických systémů*. Praha: SNTL1990.

[48] QUANTERION SOLUTIONS. https://www.quanterion.com/KnowledgeBase/ReliabilityToolkit.shtml.

[49] BARUH, H. *Applied Dynamics*. New York: CRC Press 2014.

[50] MAIXNER, L. *Navrhování automatických výrobních systémů*. Praha: NTL 1980.

[51] KLAS, A. Krok za krokem k výnosné automatizaci montážních linek. *MM průmyslové spektrum*, 2004, p. 28.

[52] ZLOCHOVÁ, M. Optimalizace výrobních buněk. *Úspěch - Produktivita a inovace v souvislostech*, 2012 (2012), 1.

[53] 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.

[54] ENDSLEY, M. R. Design and evaluation for situational awareness enhancement. In: *Proceedings of the Human Factors Society 32nd Annual Meeting*. Santa Monica, CA: Human Factors Society 1988, pp. 97-101.

[55] LAWSON, E. & J. *První letecká válka.* ISBN 80-7217-035-X. Brno: Jota 1997.

[56] POVOLNÁ, L., POVOLNÝ, J. Obsolescence Risk Mitigation Approaches. In: *Selected Risks of Business Processes.* ISBN: 978-80-01-05831-2. Praha: ČVUT 2015, pp. 62-71.

[57] www.konstrukter.cz/2015/10/29

[58] MASLOW, A. H. *Motivation and Personality*. Haper, New York 1954, 236p.

[59] US: *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*. 122p.

[60] US. *Guide for Critical Infrastructure Protection*. 2005.

[61] SANDIA NATIONAL LABORATORIES. *Vital Area Identification*. Albuquerque 2005.

[62] FEMA *Promoting Critical Infrastructure Protection by Emergency Managers and First Responders.* Nationwide. 2005. www.usfa.fema.gov

[63] EMA. *Critical Infrastructure Emergency Risk Management and Assurance*. Handbook Emergency Management Australia, 2003, www.ema.gov.au

[64] SAIC. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. National Cooperative Highway Research Program Project 20-07/Task 151B, Science Applications International Corporation–Transportation Policy and Analysis Center, Vienna 2002.

[65] GEBHARTOVÁ, J., CALETKOVÁ, J., BENEŠ, I. Zvyšování odolnosti prvků kritické infrastruktury v oblasti zásobování vodou. ISSN:1802-2626. *Periodica Academica,* 9 (2014), 1.

[66] MERTLOVÁ, O., DONT, M. Risk Assessment of Project of Implementation of Video Tolling for the Fee Collection System within the Roads Network of the Czech Republic as Part of Regulatory Impact Assessment In: *Risk of Processes and Their Management.* ISBN: 978-80-01-06144-2. Praha: ČVUT 2017, pp. 93-109.

[67] SCHÜLLEROVÁ, B., ADAMEC, V., SKŘEHOT, P., MELICHAROVÁ, M., VÉMOLA, A. Assessment of Capabilities of Conventional Tools for Analysing and Assessing of Risk in Context with Dynamic Risks. In: *Risk of Processes and Their Management.* ISBN: 978-80-01-06144-2. Praha: ČVUT 2017, pp. 231-247.

[68] BRYSON, J. M. *Strategic Planning for Public and Non-profit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement*. John Wiley & Sons 2011.

[69] EPPLER, M. J., PLATTS, K. W. The systematic use of visualization in the strategic-planning process. *Long Range Planning.* 42 (2009), pp. 42-74.

[70] www.iaea.org

[71] JUDGE, W. Q., DOUGLAS, T. J. Performance implications of incorporating natural environmental issues into the strategic planning process: An empirical assessment. Journal of Management Studies. ISSN:1097-0266. 35 (1998), 2, pp.241–262.

[72] MOORE, M. H. *Creating Public Value: Strategic Management in Government.* Cambridge: Harvard University Press 1995.

[73] MOTEFF, J., COPELAND, C., FISCHER, J. What Makes an Infrastrucuture Critical? *Report for Congress 2003,* CRS Web, Order Code RL31556.

[74] EU. *Council Directive 82/501/EEC of 24 June 1982 on the Major-Accident Hazards of Certain Industrial Activities*. Brussels: EU 1982.

[75] IAEA. The Interface between Safety and Security at Nuclear Power Plants. INSAG-24. ISBN 978–92–0–107910–7. Vienna: IAEA 2010, 25p.

[76] IAEA. *Earthquakes and Associated Topics in Relation to Nuclear Power Plant Siting. Safety Guide 50-SG-S1*. Vienna: IAEA 1978.

[77] IAEA. *Earthquakes and Associated Topics in Relation to Nuclear Power Plant Siting. Safety Guide 50-SG-S1 - Revised*. Vienna: IAEA 1991, 59p.

[78] IAEA. *Seismic Hazards in Site Evaluation for Nuclear Installations. Specific Safety Guide No. SSG-9*. ISBN 978–92–0–102910–2. Vienna: IAEA 2010, 62p.

[79] IAEA. *Action Plan on Nuclear Safety*. Vienna: IAEA 2012.

[80] PROCHÁZKOVÁ, D. Historické údaje o pohromách jsou důležité pro stavbu technologických komplexů. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 329-339.

[81] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Problems Connected with Determination of Size of Maximum Expected Disaster in Selected Site. *In: Risk, Reliability and Safety: Innovating Theory and Practices*. ISBN: 978-1-138-02997-2. London: CRC Pres / Balkema 2016, pp. 1443-1450.

[82] PANZA, G., F., VACCARI, F., COSTA, G., SUHADOLC, P., FACH, D. Seismic Input Modelling for Zoning and Microzoning. *Earthquake Spectra* 12 (1996), pp. 529-566.

[83] PROCHÁZKOVÁ, D. The Comparison of the Results of the Different Procedure of the Calculating of the Magnitude - Frequency Relation. *Veröff. des ZIPE,* 18 (1972), pp. 68-70.

[84] PROCHÁZKOVÁ, D. Kritická ínfrastruktura a zásady pro její bezpečnost. In: *Manažérstvo životného prostredia 2008*. ISBN 978-80-89281-34-3. Žilina: Strix et VeV 2010, pp.301-366.

[85] TALEB, N. N. *The Black Swan: The Impact of the Highly Improbable.* ISBN: 978-1-4000-6351-2. London: PENGUIN, 2007, 366p.

[86] EU. *Zelená kniha o Evropském programu pro ochranu kritické infrastruktury*. COM (2005) 576. Green paper on a European Programme for critical infrastructure protection, Brussels, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC05 76&

[87] EU. European Programme for Critical Infrastructure Protection (EPCIP). Council Directive 2008/114/EC, on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection.

[88] EU. Rozhodnutí Rady o výstražné informační síti kritické infrastruktury (CIWIN). KOM (2008) 676.

[89] US. *White House (1998) The Clinton's Administration's Policy on critical infrastructure protection: presidential decision directive 63/PDD-63*, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

[90] ROSSIGNOL, M. Critical infrastructure and emergency preparedness. *Report PRB 01-7E,* Canada, 001. http://publications.gc.ca/Collection-R/LoPBdP/EB/ prb017-e.htm.

[91] BRUNNER, E. M., SUTER, M. *International CIIP handbook 2008/2009*. Zurich: ETH, Center for Security Studies, ETH 2008. http://www.css.ethz.ch/content/dam /ethz/special interest /gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf.

[92] CIPedia©, 2016. www.cipedia.eu.

[93] EU. *Council Directive 2008*/114/ECof8December2008 ontheidentification anddesigna tionofEuropeancriticalinfrastructuresandtheassessment oftheneedtoimprovetheir protec tion(TextwithEEArelevance), http://eur-lex.europa. eu/legal-content/EN/TXT/PDF/?uri =CELEX:32008L0114&from=EN.

[94] BOLOGNA, S., SETOLA, R. The need to improve local self-awareness in CIP/CIIP. *First IEEE international workshop on critical infrastructure protection (IWCIP'05).* IEEE 2005.

[95] LUIIJF, H., NIEUWENHUIJS, A. H., KLAVER, M., VAN EETEN, M., CRUZ, E. Empirical findings on European critical infrastructure dependencies. *Int. J. Syst. Syst. Eng.*, 2 (2010), 1, pp. 3-18.

[96] VAN EETEN M., NIEUWENHUIJS, A., LUIIJF, E., KLAVER, M., CRUZ, E. The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. *Public Adm.*, 89 (2011), 2, pp. 381–400.

[97] US GENERAL ACCOUNTING OFfiCE. Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants. *Report GAO-03-251,* Washington DC, Feb 2003. http://www.gao.gov/new.items/d03251.pdf.

[98] OCIPEP. The September 11, 2001 Terrorist Attacks - *Critical Infrastructure Protection Lessons Learned, IA02-001,* 27 Sept 2002, Ottawa. http://www.au.af.mil/au/awc/awc gate/9-11/ia02-001_canada.pdf.

[99] NIEUWENHUIJS, A. H., LUIIJF, H. A. M., KLAVER, M. H. A. Modeling Critical Infrastructure Dependencies. In: Mauricio P, Shenoi S (eds) IFIP international federation for information processing. *Critical Infrastructure Protection II,* 290 (2008), Springer, Boston, pp. 205–214.

[100] SETOLA, R., LUIIJF, E., BOLOGNA, S. R&D Activities in Europe on Critical Information Infrastructure Protection (CIIP). *Int J. Syst. Syst. Eng.*, (2008), ½, pp. 257–270.

[101] OUYANG, M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. *Reliab. Eng. Syst. Saf.,* (2014), 121, pp. 43–60.

[102] THEOCHARIDOU, M., MELKUNAITE, L., ERIKSSON, K., WINBERG, D., HONfi, D., LANGE, D., GUAY, F. *IMPROVER Deliverable D1.2* First Draft of a Lexicon of Definitions Related to Critical Infrastructure Resilience, 30, EU 2015.

[103] UNISDR. Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction. Geneva: UNISDR 2009. http://www.unisdr.org/ we/inform /publications/7817.

[104] MOTEFF, J. D. Critical Infrastructures: Background, Policy, and Implementation., *Congressional Research Service, 7-5700, RL30153, 2015*. https://www.fas.org/sgp/ crs/home sec/RL30153.pdf.

[105] US. White House. Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience. Washington, 12, 2013. https://www.dhs.gov/sites/default/files/publication s/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf.

[106] US. Department of Homeland Security, NIPP. Partnering for Critical Infrastructure Security and Resilience, 2013. https://www.dhs.gov/sites/default/files/publications/ National-Infrastructure-Protection-Plan-2013-508.pdf.

[107] US. http://www.sandia.gov/nisac/.

[108] EC. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final. *Official Journal C 126 of 7. 6. 2007*. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri =CELEX :52006DC0786&from=EN.

[109] EU. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/ critical_infrastructure_ warning _information_network/index_en.htm.

[110] KLAVER, M., LUIIJF, E., NIEUWENHUIJS, A. Good Practices Manual for CIP Policies for Policy Makers In Europe, TNO 2016.

[111] EC. Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure., Brussels, 28. 8. 2013, SWD (2013) 318 final. http://ec.europa.eu/transparency/regdoc/ rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF.

[112] EU. *Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union* ["NIS Directive"], Brussels, July 2016. http://eur-lex. Europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[113] LUIIJF, E., VAN SCHIE, T., VAN RUIJVEN, T., HUISTRA, A. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers. TNO 2016. https://www.tno.nl/gpciip.

[114] EC. *Examples of CIPS Projects*. http://ec.europa.eu/dgs/home-affairs/financing/fundin gs/projects/per-program/cips/index_en.htm#/c

[115] EU. *Critical Infrastructure Preparedness and Resilience Research Network* (CIPRNet) website, 2016. www.ciprnet.eu.

[116] AUSTRALIAN GOVERNMENT. Critical Infrastructure Resilience Strategy. ISBN: 978-1-921725-25-8. 2010. http://www.emergency.qld.gov.au/publications/pdf/Critical_ Infrastructure_Resilience_Strategy.pdf.

[117] PURSIAINEN, C., GATTINESI, P. Towards Testing Critical Infrastructure Resilience, EUR— *Scientific and Technical Research reports*, European Commission, Joint Research Center 2014.

[118] ALSUBAIE, A., ALUTAIBI, K., MARTI, J. Resilience Assessment of Interdependent Critical Infrastructure. In: Rome E, Theocharidou M, Wolthusen S (eds) *Critical Information Infrastructures Security*, 10th international conference, CRITIS 2015, Berlin, Germany, 5–7 Oct 2015, Revised Selected Papers 2016, pp. 43–55.

[119] BRUNEAU, M., CHANG, S. E., EGUCHI, R. T., LEE, G. C., O'ROURKE, T. D., REINHORN, A. M., SHINOZUKA, M., TIERNEY, A. M., WALLACE, A. M., VON WINTERFELDT, D. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthq. Spectra,* 19 (2003), 4, pp. 733–752. http://doi.org /10.1193/1.1623497.

[120] FRANCIS, R., BEKERA, B. A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems. *Reliab. Eng. Syst. Saf.*, 121 (2014), pp. 90–103. http://dx.doi. org/10.1016/j.ress.2013.07.004.367.

[121] OUYANG, M., DUEÑAS – OSORIO, L., MIN, X. A Three–Stage Resilience Analysis Framework for Urban Infrastructure Systems. *Struct. Saf.*, 36-37 (2012), 23–31. http:// dx.doi.org/10.1016/j.strusafe.2011.12.004.

[122] MELKUNAITE, L. (ed). *IMPROVER deliverable D1.1 international survey*, 2016. http: //media.improverproject.eu/2016/06/IMPROVER-D1.1-InternationalSurvey DRAFT pdf.

[123] SETOLA, R. ET AL. (eds.). *Managing the Complexity of Critical Infrastructures, Studies in Systems.* Decision and Control 90, ISBN 978-3-319-51043-9 (eBook). http://cipedia.eu

[124] EU. Ciprnet.eu

[125] EU. http://www.cascade-project.eu/

[126] EU. http://esdac.jrc.ec.europa.eu/projects/cascade

[127] PROCHÁZKA, J., VAŠATOVÁ, L. Risks of Drinking Water Failures. In: *Risks of Business and Territorial Processes.* Ústí nad Labem: UJEP 2016, pp. 92-104.

[128] MEICHERS, R. E. *Structural Reliability Analysis and Prediction*. Chichester: Horwood/Wiley 14987.

[129] PROCHÁZKOVÁ, D., ŘÍHA, J. *Krizové řízení*. ISBN 80-86640-30-2. Praha: MV-GŘ HZS ČR 2004, 225p.

[130] PROCHÁZKOVÁ, D. Některé problémy kritické informační infrastruktury. In: *Fire Safety*. ISBN 80-86634-66-3. Ostrava: SPBI 2005, 5p.

[131] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Kybernetická infrastruktura – identifikace kritických míst a dopady jejího selhání. *CYTER2012,* ISBN 978-80-01-05072-9. Praha: ČVUT 2012.

[132] SRP, J., PROCHÁZKOVÁ, D. Systémová analýza kybernetických sítí. In: *Bezpečnostní management a společnost.* ISBN 978-80-7231-871-1. Brno: Univerzita obrany 2012, pp. 506-513.

[133] PROCHAZKOVA, D., SRP, J., PROCHAZKA, J. Analysis of Cyber Networks in a System Concept. In: *Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics. Recent Advances in Systems, Control, Signal Processing and Informatics*. ISBN: 978-1-61804-204-0, Rhodes Island 2013, pp. 102-109.

[134] OERTEL, B. ET AL. *Security Aspects and Prospective Applications of RFID Systems*. German Federal Office for Information Security (BSI) 2005. http://www.rfidconsultation.eu/docs/ficheiros/RIKCHA_englisch_Layout.pdf

[135] CREMONINI, L. ET AL. *Cyber Trust & Crime Prevention: Foresight Overview*. RAND Europe 2003, http://www.foresight.gov.uk/PreviousProjects/CyberTrustandCrime Prevention/ReportsandPublications/ForesightOverview/cybertrustforesightoverview.pdf

[136] WALMSLEY, R., ANDERSON, T., BRENDISH, C., MCDERMID, J., ROLFE, M., SULTANA, J., SWAN, M., TOMS, M.. *NATS System Failure 12 December 2014*. http://www.caa.co.uk/docs/2942/Independent%20Enquiry%20Final%20Report%202.0.pdf

[137] LEE, R. M., ASSANTE, M. J., CONWAY, T. *Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack*. https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf

[138] MILLER, B., ROWE, D. C. A Survey of SCADA and Critical Infrastructure Incidents. *Proceedings of the 1st Annual conference on Research in information technology.* New York ACM 2012, pp. 51 – 56.

[139] LEE, R. M., ASSANTE, M. J., CONWAY, T. *German Steel Mill Cyber Attack2014.* https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[140] ABRAMS, M., WEISS, J. *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia. 2008*. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

[141] ABRAMS, M., WEISS, J. *Control System Cyber Security Case Study, 2007*. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf?q=year-10-information-processing-flash-introduction

[142] EM-DAT. *The OFDA/CRED International Disaster Database* – www.emdat.net. Brussels: Université catholicque de Lou-vain. www.emdat.be

[143] http://crypto-world.info/news/index.php?prispevek=19129&sekce=s

[144] http://vtm.zive.cz/chytre-site-a-nebezpeci-kyberterorismu

[145] http://crypto-world.info/news/index.php?prispevek=20710&sekce=s

[146] BISOGNI, F., CAVALLINI, S., FRANCHINA, L., SAJA, G. The European Perspective of Telecommunications as a Critical Infrastructure. In: *Critical Infrastructure Protection VI*. ISBN: 978-3-642-35763-3, e-ISBN: 978-3-642-35764-0. Heidelberg: Springer IFIP 2012.

[147] KOPŘIVA, J. Kybernetické hrozby pro regionální bezpečnost a obranná opatření proti nim. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 76-82.

[148] NÝVLT, V., KRUŽNÍK, J. *Anonymous napadli servery OSA*, web české vlády i Evropského parlamentu. 2012. http://technet. idnes.cz/anonymous-napadli-servery-osa-web-ceske-vlady-i-evropskeho-parlamentu-1mp-/sw_internet.aspx?c=A120126_134112_ sw_internet_nyv

[149] US. *NIST SP 800-53.* Security and Privacy Controls for Federal Information Systems and Organizations.

[150] NICHOLSON, A., WEBBER, S., DYER, S., PATEL, T., JANICKE, H. SCADA security in the light of Cyber-Warfare. *Compute rs & security*, 31 (2012), pp. 418-456.

[151] VINAY, M. I., LAUGHTER, S. A., WILLIAMS, R. D. Security Issues in SCADA Networks. *Compute rs & security*, 25 (2006), pp. 498-506.

[152] KERTIS, T. PROCHAZKOVA, D. Cyber Security of Underground Railway System Operation. In: *Smart Cities Symposium in Prague*. Praha: ČVUT 2017; in print.

[153] PROCHÁZKOVÁ, D. Super Processes for Management of Risks in Territory and in Technological Entities Directed to Human Security and Development. In: *Risk of Processes and Their Management.* ISBN: 978-80-01-06144-2. Praha: ČVUT 2017, pp. 248-281.

[154] DPP. Ochranný systém metra. In: *Technická dokumentace ochranných systémů.* Praha: DPP archiv.

[155] KERTIS, T., PROCHÁZKOVÁ, D. Risk Management Directed to Safety of Metro Control Systems. In: *Risk of Processes and Their Management.* ISBN: 978-80-01-06144-2. Praha: ČVUT 2017, pp. 43-62.

[156] www.google.cz

[157] LINDA, M., KŰNZEL, G., HROMASOVÁ, M., PROKOPEC, J. The Reliability Evaluation of Assembly Lines Using Models. In: *Risk of Processes and Their Management*. Praha: ČVUT, 2017, pp. 200-216.

[158] http://www.ceps.cz

[159] https://publi.cz/books/260/01.html.

[160] ESRA. *Reliability, Risk and Safety: Theory and Applications.* ISBN 978-0-415-55509-8. Leiden: CRC Press / Balkema 2009, 2367 p.

[161] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Příčiny selhání elektroenergetické infrastruktury a identifikace oblastí, které vyžadují prevenci a připravenost. In: *Rizika podnikových procesů 2015*. ISBN: 978-80-7414-967-2. Ústí nad Labem: UJEP 2015, pp. 115-123.

[162] PROCHÁZKOVÁ, D., Poučení z dlouhodobého výpadku elektrického proudu ve východní části USA a Kanady v 2003. In: *Environmentální aspekty podnikání*. ISSN 1211-8052. Praha: CEMC 2004.

[163] BO, Z., SHAOJIE, O., JIANHUA, Z., HUI, S., GENG, W., MING, Z. An analysis of Previous Blackouts in the World: Lessons for China´ Power Industry. *Renewable and Sustainable Energy Reviews*. 42 (2015), pp. 1151-1163. http://linkinghub.elsevier.com /retrieve/pii/S1364032114008946

[164] ADIBI, M. M., MARTINS, N. Impact of Power System Blackouts. In: *Panel Session at the IEEE PES GM 2015 "Cascading Failures: Advanced Methodologies, Restoration and Industry Perspectives".* Denver, July 2015.

[165] NERC. http://www.nerc.com/~filez/blackout.html

[166] KJØLLE, G. H., UTNE, I. B., GJERDE, O. Risk Analysis of Critical Infrastructures Emphasizing Elektricity Supply and Interdependencies. *Reliability Engineering and System Safety,* 105 (2012), pp. 80–89

[167] DOORMAN G., UHLEN K., KJOLLE CH., HUSE E. Vulnerability Analysis of the Nordic Power systém. *IEE Transactions on Power Systems*, 21 (2006), 1, pp. 402-410.

[168] NORDSECUREEI. Risk and Vulnerability Assessments for Contingency Planning and Training in the Nordic Elektricity System. *Final Report Statens Energimyndighet.* Eskilstuna: EU EPCIP 2009.

[169] EMA. *Australian Emergency Manual Disaster Recovery*. Emergency Management Australia. Sydney 1996, 166p.

[170] US. Worksheets for Electric Utility Vulnerability and Risk Assessment. www.esisac. com.

[171] EMA. Critical Infrastructure Emergency Risk Management and Assurance. *Handbook Emergency Management Australia*, 2003, www.ema.gov.au

[172] CISP. *Workshop on Critical Infrastructure Protection and Civil Emergency Planning-Dependable Structures, Cybersecurity, Commnon Standard*. Zurich: Centre for International Security Policy 2005, www.eda.admin.ch

[173] US DOE. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. U.S.A. - Canada Power System Outage Task Force. Governments, April 2004, 228p.

[174] LEONARD, W. Blackout 2003. In: *Training of Czech Firefighters.* Podklady k přednáškám (eds D. Brennan, D. Procházková, D. Vávrů). EMO, Winnipeg 2004, 37p.

[175] ASCE. *Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters", Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards", Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters*". Washington: ASCE 2001.

[176] PROCHÁZKOVÁ, D. Dopady selhání energetické infrastruktury. In: *Energetické koncepce Středočeského kraje / Jihočeského kraje*. Zprávy pro Krajské úřady. CITYPLAN spol. s r.o., Praha 2004, 48p.

[177] http://www.ceskatelevize.cz/ct24/ekonomika/1046346-blackout-v-cesku-stoprocentne-nebudeme-pripraveni-nikdy

[178] https://www.ceproas.cz

[179] www.mero.cz

[180] www.sshr.cz

[181] SŽDC. *Technické kvalitní podmínky staveb státních drah. Kapitola 13*. Praha: SŽDC 2008, 16p.

[182] VLČEK, J. Produktovody ČEPRO a.s. v podmínkách EU. In: *Energetika a stavebnictví.* Praha: For Arch 2003, 20p.

[183] PROCHÁZKA, J., RETAMOZOVÁ, P. Havárie ropovodů. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 164-173.

[184] www.novinky.cz/zahranicni/evropa/151932-v-madarsku-praskl-ropovod-druzba.html

[185] PROCHÁZKOVÁ, D., PROCHÁZKA, J., PATÁKOVÁ, H., PROCHÁZKA, Z., STRYMPLOVÁ, V. *Kritické vyhodnocení přepravy nebezpečných látek po pozemních komunikacích v ČR.* ISBN 978-80-01-05599-1. Praha: ČVUT 2014, 150p.

[186] ČR. www.svitavsky.denik.cz/zpravy_region/do-svitavy-unikly-ropne-latky20111106.html

[187] RETAMOZOVÁ, P. *Ocenění rizik vybraného ropovodu*. Diplomová práce. Praha: ČVUT 2016, 103p.

[188] ČESKÁ TELEVIZE. *Havárie na ropovodu Družba zastavila dodávky na Slovensko*. 2008. http://www.ceskatelevize.cz/ct24/svet/1437924-havarie-na-ropovodu-druzba-zastavi la-dodavky-na-slovensko

[189] VOTRUBA, l., HEŘMAN, J. A KOLEKTIV. *Spolehlivost vodohospodářských děl.* ISBN: 80-209-0251-1. Praha: Česká matice technická 1993, 496p.

[190] PATÁKOVÁ, H., PROCHÁZKA, J. Analysis of Data on Traffic Incidents with Presence of Hazardous Substances. In: *Proceedings of the 11th European Transport Congress*, ISBN: 978-80-01-05321-8. Praha: ČVUT 2013.

[191] PATÁKOVÁ, H. *Kritická místa při přepravě nebezpečných látek po dálnici D1.* Diplomová práce ČVUT v Praze. Praha: ČVUT 2014, 124p.

[192] VAŠATOVÁ, L. *Rizika spojená se selháním dodávek pitné vody.* Diplomová práce ČVUT v Praze. Praha: ČVUT 2016, 74p.

[193] PROCHÁZKA, J., VAŠATOVÁ, L. Risks of Drinking Water Failures. In: *Risk of Processes and Their Management.* ISBN: 978-80-01-06144-2. Praha: ČVUT 2017, pp. 27-42.

[194] PROCHÁZKOVÁ, D. *Krizové řízení pro technické obory*. ISBN 978-80-01-05292-1. Praha: ČVUT 2013, 303p.

[195] VÚV. *Technická dokumentace vodovodů a kanalizace.* Praha: VUV 2016.

[196] KÚ STŘEDOČESKÉHO KRAJE. Databáze vodovodní sítě ve Středních Čechách a přidružených problémů. Praha: Krajský úřad.

[197] http://wol.jw.org./cs/wol/d/r29/lp-b//102002049#h=6

[198] http://www.prehrady.wbs.cz/

[199] http://www.lomyatezba.cz/component/k2/item/647-prehrady-sveta

[200] http://www.prehrady.cz

[201] https://cs.wikipedia.org/wiki/Seznam_p%C5%99ehradn%C3%ADch_n%C3%A1dr%C5%BE%C3%AD_v_% C4%8Cesku

[202] BROŽA, V. *Přehrady Čech, Moravy a Slezska*. ISBN 80-86660-11-7. Liberec: Knihy 2005, 251p.

[203] http://www.ceskatelevize.cz/ct24/archiv/1369806-pres-400-mrtvych-si- vyzadala-protrzena-hraz-prehrady-malpasset

[204] http://www.geocities.com/Athens/Acropolis/2907/vajont.html

[205] MD. *TP 229. Bezpečnost v tunelech pozemních komunikací.* Praha: ELTODO EG a.s. 2010, http:www.pjpk.cz/TP%20229.pdf

[206] MD. www.mdcr.cz

[207] REMEŠ, P. *Bezpečnostní plán dálnice D1 - úsek Praha – Mirošovice.* Diplomová práce. Praha: ČVUT 2015, 95 p.

[208] REMEŠ, P., PROCHÁZKOVÁ, D. Sestavení kontrolního seznamu pro identifikaci kritických míst na dálnici. In: *Rizika podnikových procesů 2015*. ISBN: 978-80-7414-967-2. Ústí nad Labem: UJEP 2015, pp. 151-160

[209] http://dge.stanford.edu/SCOPE/SCOPE_40/SCOPE_40_2.6_McQuaid_157-188.pdf

[210] http://blog.chron.com/bayoucityhistory/2011/05/35-years-later-houstons-deadly-ammonia-truck-disaster/

[21] http://www.pozary.cz/clanek/746-svetove-katastrofy-costa-blanca-1978/

[212] http://en.wikipedia.org/wiki/Los_Alfaques_disaster

[213] http://en.wikipedia.org/wiki/List_of_disasters_in_Thailand

[214] http://www.zachranny-kruh.cz/chemicka_havarie_ochromila_spojeni_mezi_kraji.html

[215] ČR. Bezpečnostní list dle zákona 356/2003 Sb. Technický benzín*, Číslo ES: 295-438-4, 2006, 1-5.*

[216] PROCHÁZKOVÁ, D. Zemětřesení v Kalifornii. *Vesmír.* 1990, 3.

[217] JAMRTAL. *Historie projektu. 2012*. http://www.jamrtal.com/nuselsky-most/#!.

[218] DAHINTER, K. *Nuselský most - 40 let od uvedení do provozu.* 2014. http://www.earch.cz/cs/architektura/nuselsky-most-40-let-od-uvedeni-do-provozu

[219] SEMECKÝ, A. *Projektová dokumentace.* Technická správa komunikací hl. m. Prahy, 2014-10-20

[220] PROCHÁZKOVÁ, D. *Seismické inženýrství na prahu třetího tisíciletí*. ISBN 978-80-7385-022-7. Ostrava: SPBI 2007, 325p

[221] PROCHÁZKOVÁ, D., ŠIMŮNEK, P. *Fundamental Data for Determining Seismic Hazard for Localities in Central Europe*. ISBN 80-238-2661-1. Praha: Ústav mezinárodních vztahů 1998, 132 p

[222] PROCHÁZKOVÁ, D., DEMJANČUKOVÁ, K.:*Earthquakes, Hazards and Principles for Trade-off with Risks*. ISBN 978-80-261-0170-3. Plzeň: University of West Bohemia, 2012, 215p.

[223] ČR. ČSN EN. *Eurokód 8: navrhování konstrukcí odolných proti zemětřesení.* Část 1: Obecná pravidla, seismická zatížení a pravidla pro pozemní stavby. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[224] DAVID., J. Rizika spojená s Nuselským mostem a jejich vypořádání. Diplomová práce. Praha: ČVUT 2015, 77p.

[225] DAVID, J., PROCHÁZKOVÁ, D. Dopady silného zemětřesení na Nuselský most a jeho okolí. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 21-33.

[226] www.ceskedrahy.cz

[227] PROCHÁZKA, J., KERTIS, T., PROCHÁZKOVÁ, D. Zdroje rizik pro dopravu na železnici v ČR. In: *Sborník Příspěvků JUFOS 2017*. ISBN: 978-80-214-5486-6. Brno: VUT 2017, pp. 283-291

[228] http://dge.stanford.edu/SCOPE/SCOPE_40/SCOPE_40_2.12_Vilian_251-290.pdf

[229] http://en.wikipedia.org/wiki/Kingman_Explosion

[230] http://kingmanhistoricdistrict.com/points-of-interest/firefighters-memorial-park/the-disaster-story.htm

[231] http://www.aristatek.com/newsletter/0704April/TechSpeak.pdf

[232] http://www.atsdr.cdc.gov/toxprofiles/tp172-c3.pdf

[233] http://en.wikipedia.org/wiki/Graniteville,_South_Carolina,_train_crash

[234] http://theses.cz/id/831kmp/Diplomov_prce.pdf

[235] http://en.wikipedia.org/wiki/List_of_rail_accidents_(2000%E2%80%932009)

[236] http://news.bbc.co.uk/2/hi/europe/6907177.stm

[237] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Osobní šetření v objektech kolem nádraží Děčín východ.* Srpen 2013. Praha: ČVUT.

[238] ROSOVÁ, L. *Řízení rizik železničních nadražích.* Diplomová práce. Praha: ČVUT v Praze Fakulta dopravní 2014, 96p.

[239] EU. *Directive 2002/49/EC of the European Parliament and of the Council of 25 June 2002 relating to the assessment and management of environmental noise* - Declaration by the Commission in the Conciliation Committee on the Directive relating to the assessment and management of environmental noise. Brussels: EC, 2002.

[240] EU. *Regulation 402/2013 on the CSM for Risk Assessment and Rrepealing.* Regulation 352/2009. EC, 2013.

[241] ČR. *Vyhláška číslo 376/2006 Sb. o systému bezpečnosti provozování dráhy a železniční dopravy a postupech při vzniku mimořádných událostí na dráhách*. https://www.zakonyprolidi.cz/cs/2006-376

[242] ČR. *ČSN EN ISO 9001:2009 (01 0321). Systémy managementu kvality – Požadavky.* Praha: ÚNMZ 2009.

[243] UNIFE. *IRIS Rev. 02.1. International Railway Industry Standard.* Belgie: UNIFE, 2012. http://www.iris-rail.org/

[244] ČR. *ČSN EN 50126-1 (333502). Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS): Část 1: Základní požadavky a generický proces.* Praha: ČNI, 2001.

[245] ČR. *ČSN EN 50129 (34 2680). Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy.* Praha: ÚNMZ, 2012.

[246] EN 50 128 ČR. *ČSN EN 50128 (342680). Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídicí a ochranné systémy*. Praha: ČNI, 2002.

[247] ČR. *ČSN EN 61508-1 ed. 2 (180301). Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky.* Praha: ÚNMZ, 2005.

[248] KERTIS, T. Introduction of Modern Approaches of Ensuring Safety into Business Processes in Railway Industry. In: *Vybraná rizika podnikových procesů 2015*. ISBN 978-80-01-05831-2. Praha: ČVUT v Praze, pp. 26-38.

[249] ČD. Hodnocení rizik – stupnice. Archiv. www.ceskedrahy.cz

[250] KERTIS, T., PROCHÁZKOVÁ, D. Posouzení úrovně shody legislativy s normativem pro zajištění bezpečnosti drážních systémů z pohledu integrální bezpečnosti. In: *ExFoS 2017 – Expert Forensic Science 2017*. ISBN: 978-80-214-5459-0. Brno: VUT 2017, pp. 355-365.

[251] KERTIS, T., PROCHÁZKOVÁ, D. Reduce of Criticality of Critical Infrastructure Facilities in the Railway Domain. In: *Smart Cities Symposium Prague (SCSP) 2015.* ISBN:978-1-4673-6727-1/15/531.00©2015 European Union, 8 p.

[252] DPP. *Technická a provozní dokumentace metra*. Archiv Dopravního podniku Praha.

[253] NOVOBILSKÝ P. Kybernetická bezpečnost drážní komunikační infrastruktury. In: *Rizika podnikových procesů 2015*. ISBN: 978-80-7414-967-2. Ústí nad Labem: UJEP 2015, pp. 54-61.

[254] ČR. *ČSN EN 13816 - Doprava - Logistika a služby - Veřejná přeprava osob - Definice jakosti služby, cíle.* Praha: ÚNMZ, 2003.

[255] KERTIS, T. *Bezpečnostní plán vybrané stanice pražského metra*. Diplomová práce. Praha: ČVUT 2015, 108p.

[256] KERTIS, T., PROCHÁZKOVÁ, D. Plán řízení rizik spojených s provozem metra. In: *ExFoS - Expert Forensic Science XXV. mezinárodní vědecká konference soudního inženýrství*. Brno: VUT 2016, pp. 399-416.

[257] KERTIS, T., PROCHÁZKOVÁ, D. Posouzení kritičnosti plánu řízení rizik pro metro. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 60-75.

[258] ARTEMIS. Joint undertaking. integrated design and evaluation methodology. In: *SESAMO: Security and Safety Modelling*. http://sesamo-project.eu/sites/default/files/ downloads/publications/integrated-design-and-evaluation-communication-material.pdf

[259] ČR. ČSN ISO/IEC 27000 (36 9790). Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Přehled a slovník. Praha: ÚNMZ 2010.

[260] EU. *ANSI/ISA–62443-1-1 (99.01.01)-2007. Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models*. EU ISA, 2007.

[261] ČR. ČSN ISO/IEC 15408-1 (36 9789). *Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT: Část 1: Úvod a všeobecný model*. Praha: ČNI, 2001.

[262] ČR. ČSN EN 62290-1:2006 (33 3530). Drážní zařízení - Systémy řízení městské dopravy vyhrazenou vodicí dráhou: Část 1: Systémové principy a základní pojmy. Praha: ČNI, 2007.

[263] IEC. IEC 61508: *Functional safety of electrical/electronic/programmable electronic safety-related system*. Geneva: International Electrotechnical Commission 2011.

[264] CENELEC. EN 50159: Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems. Brussels: EC for Electrotech. Standardization 2010.

[265] KERTIS, T., PROCHAZKOVA, D. Risk Management Plan for Metro Station Safe Operation. In: *Risk, Reliability and Safety: Innovating Theory and Practices*. ISBN: 978-1-315-37498-7. London: Taylor & Francis Group 2016, pp. 1306-1314.

[266] ISO. EN ISO 9000:2005 *Quality management systems. Fundamentals and vocabulary.* Geneva: IOS 2005

[267] CENELEC. EN 50126-1: *The specification and demonstration of reliability, availability, maintainability and safety*. Brussels: EC for standardization 1999.

[268] ŽÁK, J. *Studie blackoutu s ohledem na jadernou elektrárnu Dukovany*. Diplomová práce. Brno: VUT 2013.

[269] DPP, a.s. *DP Kontakt: Časopis zaměstnanců veřejné dopravy.* Praha: DPP, 1999-2016. ISSN 1212-6349.

[270] KRÁKORA, J. *Ocenění rizik při výpadku elektrické energie v metru.* Diplomová práce. Praha: ČVUT 2015, 85p.

[271] KRÁKORA, J., PROCHÁZKOVÁ, D. Dopady výpadku elektrické energie na metro. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 84-91.

[272] DOPRAVNÍ PODNIK hl. m. Prahy. *Archiv.* D 2/1. Postupy evakuace cestujících z traťového tunelu. Technická dokumentace.

[273] PRUŠA. J. *Svět letecké dopravy*. ISBN 978-80-239-9206-9. Praha: Galileo CEE Service ČR 2007. 315 p.

[274] ÚŘAD PRO CIVILNÍ LETECTVÍ. www.caa.cz

[275] ÚŘAD PRO CIVILNÍ LETECTVÍ. *Předpis L13.* http://lis.rlp.cz/predpisy/predpisy/ dokumenty /L/L-13/index.htm

[276] ČR. Historie letecké dopravy. *Vítejte na zemi* http://vitejtenazemi.cz/cenia/index.php?p =historie_letecke_dopravy&site=doprava

[277] www.iata.org**),**

[278] www.airdisaster.com

[279] www.technet.cz

[280] NATIONAL TRANSPORTATION SAFETY BOARD. *Controlled Flight Into Terrain, Learjet 35A, N30DK*. http://www.ntsb.gov/investigations/AccidentReports/Pages/AAB0605.aspx

[281] PRAŽAN, M. *Identifikace závažných rizik v letovém provozu a návrh jejich vypořádání*. Diplomová práce. Praha: ČVUT 2016, 79p.

[282] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Causes of Accidents in Civilian Aircraft Operation and Tools for Management of Selected Risks. In: ESREL 2017, in print.

[283] NTSB. *Loss of thrust in both engines, US Airways Flight 1549 Airbus Industrie A320-214, N106US.* 2010. http://www.ntsb. gov/investigations/Accident Reports/Pages/AAR1 003.aspx

[284] NTSB. *Controlled flight into terrain, Korean air flight 801, Boeing 747-300, HL7468.* 2000. http://www.ntsb.gov/investigations/AccidentReports/Pages/AAR0001.aspx

[285] MIKA, L. 2016. Aircraft operating safety in the world in 2015. ISSN 0024-1156, *Letectví + kosmonautika,* 92 (2016), 2, pp. 50-52.

[286] SAS. *A332, En-Route, Atlantic Ocean*, 2009. http://www. skybrary.aero/index. php/ A332,en-route,Atlantic Ocean, 2009

[287]SAS.*MD83 En Route South East of Gossi, Mali 2014.* http://www.skybrary.aero/index. php/MD83_En_Route_South_East_of_Gossi,_Mali_2014

[288] SAS. *B733, en-route, Grammatiko Greece.* http://www.skybrary.aero/index.php/ B733,enroute,_Grammatiko_Greece 2005

[289] ŘLP, 2016. *Letecká informační příručka.* Jeneč: ŘLPZU 2016.

[290] NTSB. *In-Flight separation of vertical stabilizer American Airlines Flight 587, Airbus Industrie A300-605R, N14053.*2004. http://www.ntsb.gov/investigations/AccidentReports/Pages/AAR0404.aspx

[291] DSB. *Investigation crash MH17, 17 July 2014 Donetsk.* http://www.onderzoeksraad.nl/en/onderzoek/2049/investigation-crash-mh17-17-july-2014

[292] ŘLP. *Vyhlašování stupňů pohotovosti na LKPR a pravidla spolupráce TWR a HZS LP.* Jeneč, 2014.

[293] ŘLP. *Plan for non-standard situation solution.* Jeneč: ŘLP ČR 2015.

[294] SAS. *T154 / B752, en-route, Uberlingen Germany.* 2002. http://www.skybrary. aero/index.php/T154_/_B752,_enroute,_Uberlingen_Germany,_2002

[295] SAS, *B744, Taipei Taiwan.* 2000. http://www.skybrary.aero/index.php/B744, _Taipei_Taiwan,_2000

[296] SAS. *MD87 / C525, Milan Linate*, 2001. http://www.skybrary.aero/index.php /MD87 /C525,Milan_

[297] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Akceschopný krizový plán pro velká rizika. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 321-332.

[298] ŘLP. *Provozní řád IATCC Praha.* Jeneč: ŘLP 2012.

[299] ŠIMÍK. J. *Vliv lidského činitele na bezpečnost malých letadel.* Diplomová práce. Praha: ČVUT 2016. 98p.

[300] THOM. T. *Human Factors and Pilot Performance: Safety. First Air and Survival*. ISBN: 978-184-3360-704. Beds. England: Air Pilot Publishing 2006.

[301] ŠULC. J. *Letecká psychologie*. ISBN 80-7204-482-6. Praha: Naše Vojsko 1980.

[302] CR. *Mapy CZ.* https://mapy.cz/

[303] Směrnice 2012/18/EU (SEVESO III)

[304] PROCHÁZKOVÁ, D., BUMBA, J., SLUKA, V., ŠESTÁK, B. *Nebezpečné chemické látky a chemické přípravky a průmyslové nehody*. ISBN 978-80-7251-275-1. Praha: PA ČR, 2008, 420p.

[305] PROCHÁZKOVÁ, D. Příčiny technologických havárií. In: *Sustainability-Environment-Safety 2015*. ISBN:978-80-89753-01-7. Žilina: STRIX, n.f. 2016, pp. 55-64; ww.sszp.eu

[306] PROCHÁZKOVÁ, D., PROCHÁZKA, J., PROCHÁZKA, Z. Výsledky hodnocení technologických havárií s přítomností nebezpečných látek. *Ochrana obyvatelstva - Nebezpečné látky 2015.* ISBN: 978-80-7385-158-3, ISSN 1803-7372. Ostrava: SPBi 2015, pp 144-151.

[307] XENIDIS, Y., GIANNARIS, K. Modeling and Assessment of Performance Shaping Factors in Construction. In: *Safety and Reliability: Methodology and Applications.* ISBN: 978-1-138-02681-0. London: Taylor & Francis Group 2015, pp 1019-1026.

[308] ISSA. *ISSA Prevention Series*. ISSN 1015-8022, ISBN 92-843-1177-2, Heidelberg: ISSA, 75p.

[309] PROCHÁZKA, Z., PROCHÁZKOVÁ, D. Výsledky studia chemických havárií zaměřené na dioxin. In: *Ochrana obyvatelstva 2014.* ISBN: 978-80-7385-142-2, ISSN: 1803-7372, Ostrava: SPBI 2014, pp. 177-181.

[310] PROCHÁZKOVÁ, D. Příčiny nehod a havárií a způsoby řízení bezpečnosti technologických systémů s ohledem na dopady havárií. In: *Manažérstvo životného prostredia 2013.* ISBN 978-80-89281-90-9. Žilina: STRIX 2014, pp. 151-157.

[311] PROCHÁZKOVÁ, D. *Řízení technologických pohrom a detekce prioritních problémů pro budoucí výzkum.* In: *Manažérstvo životného prostredia 2013***.** Žilina, ISBN 978-80-89281-90-9. Žilina: Strix 2014, pp. 249-255

[312] PROCHÁZKOVÁ, D. Poznatky pro bezpečnost průmyslu. In: *Bezpečnost a ochrana zdraví při práci 2014*. ISBN 978-80-7385-145-3. Ostrava: SPBI 2014, pp. 101-107

[313] PROCHÁZKA, Z., PROCHÁZKOVÁ, D. Výsledky analýzy havárií s kyselinou dusičnou v České republice. In: *Požární ochrana 2014*. ISBN:978-80-7385-148-4. Ostrava: SPBI 2014, pp. 277-281.

[314] PROCHÁZKA, Z., KOSHKINA, E., PROCHÁZKOVÁ, D. Rizika spojená s provozem technologických provozů. In: *Rizika podnikových procesů 2015.* ISBN: 978-80-7414-967-2. Ústí nad Labem: Universita Jana Evangelisty Purkyně 2015, pp. 97-114.

[315] Procházková, D. Řízení rizik velkých technických děl. In: *Motivation, Education, Trust, Environment, Safety 2016*. ISBN 978-80-89753-13-0. Žilina: STRIX, n.f. 2016, pp. 48-58.

[316] AIChE. *Guidelines for Consequence Analysis of Chemical Releases.* New York: CCPS/AIChE 1999.

[317] AIChE. *Guidelines for Chemical Process Quantitative Risk Analysis (2. edition).* New York: CCPS/AIChE 2000.

[318] AIChE. *Guidelines for Investigating Chemical Process Incidents*. New York: CCPS-AIChE 1992.

[319] CPD. *Guidelines for Quantitative Risk Assessment (Purple Book 1999).* The Hague: CPR 18E. Committee for the Prevention of Disasters 1999.

[320] AIChE. *Guidelines for Use of Vapor Cloud Dispersion Models (2. edition*). New York: CCPS/AIChE 1996.

[321] CHEREMISINOFF, N. P. *Handbook of Hazardous Chemical Properties*. Boston: Butterworth 2000. 454p. ISBN:0-7506-7209-9

[322] KIRCHSTEIGER, Ch. (ed.). *Risk Assessment and Management in the Context of the SEVESO II Directive*. Amsterdam: Elsevier, 1998.

[323] KLETZ, T. A. *What Went Wrong? Case Histories of Process Plant Disasters.* 2nd ed., Houston: Gulf Publishing Company, 1988.

[324] LEES, F. P. *Loss Prevention in the Process Industry, Volumes 1, 2, 3*, (2. edition). Oxford: Butterworth-Heinemann 2001.

[325] MARŠÁK, J. et al. *Bezpečnost při manipulaci s chemickými látkami a jedy*. Praha: Práce 1980.

[326] CPR. *Methods for Calculation of Physical Effects, (the „Yellow Book*"). The Hague: CPR 14 E 1997.

[327] CPR. *Methods for the Determination of Posible Damage (the „Green Book").* Voorburg: CPR 16E 1989.

[328] PITBLADO, R., TURNEY, R. *Risk Assessment in the Process Industry. 2. edition.* Rugby: IChemE 2001.

[329] RASMUSSEN, K. *The Experience with the Major Accident Reporting System from 1984 to 1993*. EUR 16341, 1996.

[330] http://en.wikipedia.org/wiki/Ammonium_nitrate_disasters

[331] http://www.aria.developpement-durable.gouv.fr/ressources/14373_gb.pdf

[332] http://blisty.cz/art/37810.html

[333] http://arnika.org/historie-otrav-rtuti

[334] http://en.wikipedia.org/wiki/Piper_Alpha

[335] EU: Project EDEN. www.eden-security-fp7.eu

[336] http://en.wikipedia.org/wiki/Phillips_Disaster_of_1989

[337] http://en.wikipedia.org/wiki/Formosa_Plastics_Corp

[338] http://www.csb.gov/formosa-plastics-vinyl-chloride-explosion/

[339] http://www.sj-r.com/article/20091222/News/312229900

[340] http://de.wikipedia.org/wiki/Liste_der_gr%C3%B6%C3%9Ften_k%C3%BCnstli chen,_nichtnu klearen_Explosionen

[341] http://www.novinky.cz/krimi/350719-vybuchy-znicily-municni-sklad-na-zlinsku-hasici-muse li -pryc.html

[342] http://www.novinky.cz/krimi/351162-pyrotechnici-se-ve-vrbeticich-dostali-k-epicentru-po-pohresovanych-zadne-stopy.html

[343] http://www.novinky.cz/krimi/351162-ve-vrbetickem-skladu-vybuchuje-munice-pyrotechnikum-primo-pod-rukama.html

[344] http://litvinov.sator.eu/kategorie/zanikle-obce/zaluzi/vybuch-v-chemicce-v-zaluzi-1971974

[345] http://pardubicky.denik.cz/zpravy_region/vybuch-chemicky-v-semtine-je-nejtragictejsi-od-rok.html

[346] http://www.czech-press.cz/index.php?option=com_content&view=article&id= 7376:maly-esky-cernobyl-sp-634390438&catid=1516:1994-01&Itemid=148

[347] http://www.novysmer.cz/index.php?option=com_content&view= article&id=1228: diox in&catid=37:zahranicnipolitika&Itemid=48

[348] http://cs.wikipedia.org/wiki/Spolana_Neratovice

[349] COLLINS, J., STRAUSS, M. E., LEVINSKAS, G. J., CONNER, P. R. The Mortality Experience of Workers Exposed to 2,3,7,8-Tetrachlorodibenzo-P-Dioxin in a Trichlorophenol Process Accident. *Epidemiology.* 4 (1993), 1, pp. 7-13. http://www. ncbi.nlm. nih.gov/pubmed/8420584

[350] http://www.aerzteblatt.de/archiv/88106/BASF-Mehr-Erkrankungen-nach-Dioxin-Unfall-1953.

[351] STOKES, R. G. Von der I.G. Farbenindustrie AG bis zur Neugründung der BASF, in: Werner Abelshauser (Hrsg.), Die BASF. Eine Unternehmens-geschichte. München 2002, p. 348. http://archiv.rhein-zeitung.de/on /98/08/10/topnews/basfhin.html

[352] http://books.google.cz/books?id =V524J4zh06MC&pg=PA106& rediresc=y#v =one page &q&f=false

[353] http://en.wikipedia.org/wiki/Coalite

[354] http://archive.unu.edu/unupress/unupbooks/uu21le/uu21le09.htm

[355] http://en.wikipedia.org/wiki/Love_Canal

[356] http://en.wikipedia.org/wiki/Times_Beach,_Missouri

[357] Belgian PCB and Dioxin Incident of January–June 1999: Exposure Data and Potential Impact on Health, Environ Health Perspect 109:265–273 (2001). http://en.wikipedia.org/wiki/Dioxin_Affair

[358] http://www.independent.co.uk/news/world/europe/italys-toxic-waste -crisis-the-mafia-ndash-and-the-scandal-of-europes-mozzarella-799289.html

[359] http://www.foodrisc.org/the-case-of-dioxin-in-irish-pork-and-beef-_51.html

[360] http://cs.wikipedia.org/wiki/Dioxinov%C3%BD_skand%C3%A1l _v_N% C4%9 Bmecku

[361] http://www.cizp.cz/Havarie-na-vodach

[362] https:iaea.org

[363] GALLAGHER, T., SCOTT, M., 2007 The Complementary Role of Dominant Designs and Industry Standards. IEEE Transactions on Engineering Management. 52(2007), 2, pp 371-379.

[364] PROCHÁZKOVÁ, D. Analýza havárie jaderné elektrárny Fukushima a první poučení. In: *Požární ochrana 2011*. ISBN: 978-80-7385-102-6. Ostrava: SPBI 2011, pp. 288-291.

[365] GUSTIN, J. F. *Disaster & Recovery Planning: a Guide for Facility Managers*. ISBN 0-88173-323-7 (FP), 0-13-009289-4 (PH). Lilburn: The FairMont Press, Inc. 2002, 304p.

[366] PROCHÁZKOVÁ, D. *Metodika pro odhad nákladů na obnovu majetku v územích postižených živelní nebo jinou pohromou*. SPBI SPEKTRUM XI Ostrava 2007, ISBN 978-80-86634-98-2, 251p.

[367] EU. *Návrh nařízení Evropského parlamentu a Rady o hlavních směrech transevropské energetické infrastruktury a o zrušení rozhodnutí č. 1364/2006/ES*. COM/2011/0658.

[368] KRÁL, J. *Ocenění rizik při testu tlumení nárazu podvozku letounu v okamžiku přistání.* Diplomová práce. Praha: ČVUT 2015, 157 p.

[369] SLAVĚTINSKÝ, D. *O letadlech. Koncepce přistávacího zařízení*. http://www. slavetind.cz/stavba/koncepce/Koncepce_prist_zar.aspx\

[370] TŮMA, J. *Letadla*. Opora pro učební a studijní obory na SOU. Praha: SNTL 1981.

[371] PETRÁSEK, M. *Základy konstrukce letadel*. Brno: VUT 1999.

[372] AERO VODOCHODY AEROSPACE. *Interní materiály* – technická dokumentace, technické postupy, bezpečnostní dokumentace.

[373] MAREK, J. a kol. *Management rizik v konstrukci výrobních strojů*. ISSN 1212-2572. Praha: Průmyslové spektrum, speciální vydání., 2009.

[374] CHRISTOPHER, M. *Logistics and Supply Chain Management*. London: Pearson Education Limited 2005, p. 17

[375] CHOPRA, S., MENDL, P. Supply Chain Management. *Prentice Hall, Essex 2001, 3 p.*

[376] PROCHÁZKOVÁ, D. Model pro řízení bezpečnosti dodavatelských řetězců. *Požární ochrana 2013*. ISBN: 978-80-7385-127-9, ISSN: 1803-1803. Ostrava: SPBI 2013, pp. 209-213.

[377] HARRISON, A., VAN HOEK R. *Logistic Management and Strategy. Competing through the supply chain.* Prentice Hall, Essex 2008, 7 p.

[378] PERNICA, P. *Logistics for 21 Century. Supply Chain Management*. Radix 2005, 1660 p.

[379] GROS, I. *Logistika*. Praha: VŠCHT 1996.

[380] PATÁKOVÁ, H., PROCHÁZKOVÁ, D. Dodavatelské řetězce jako další téma krizového řízení. In: *Rizika podnikových procesů 2015*. ISBN: 978-80-7414-967-2. Ústí nad Labem: UJEP 2015, pp. 62-69.

[381] STEIN, W., HAMMERLI, B., POHL, H., POSCH, R. (eds). Critical Infrastructure Protection – Status and Perspectives. *Workshop on CIP*, Frankfurt am Main, www.informatik2003.de

[382] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Critical Infrastructure Safety Management. In: *Deteritoration, Dependability, Diagnostics*. ISBN 978-80-7231-939-8. Brno: UNOB, 2013, pp. 137-146

[383] PROCHÁZKOVÁ, D. Safety of Critical Facilities. No 5391015. In: *New Developments in Environmental Science and Geoscience*. ISSN:2227-4359, ISBN:978-1-61804-283-5. Vienna: INASE 2015, pp. 27-33, INASE E-library www.inase.org

[384] ENV. *Basis of Designs and Actions on Structures*. Brussels: CEN 1993.

[385] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Results of Inspections of Risk Management Quality in Facilities of Critical Infrastructure. *International Journal of Mechanical Engineering.* ISSN:2367-8968. www.iaras.org/iaras/journals/ijme

[386] LUIJIF, E. Empirical Findings. CI Disruptions, Dependencies and Common Cause Events. CIPRNet Project 2017. Brussels: EU 2017.

[387] UK. *Turkey power outage shuts down public transportation and half of provinces*. London: The guardian, 2014, http://www.theguardian.com/world/2015/mar/31/turkey-power-outage-shuts-down-transportation-provinces

[388] PROCHÁZKOVÁ, D. Zásady obnovy infrastruktur z pohledu ochrany obyvatelstva. In: *Ochrana obyvatelstva – DEKONTAM 2013.* ISBN 978-80-7385-122-4, ISSN 1803-7372, Ostrava: SPBI 2013, pp. 133-136

[389] ČR. Směrnice rady 2008/114/ES ze dne 8. prosince 2008, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Brusel: *Úřední věstník Evropské unie*, 2008. http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF

[390] PROCHÁZKOVÁ, D., KOPECKÝ, Z. Problems of Bank Sector (In Czech). In: Požární ochrana 2012. ISBN: 978-80-7385-115-6. Ostrava: SPBI 2012, pp. 250252.

[391] MATOUŠKOVÁ, I. Rozhodování v situacích ohrožení. In: *Riešenie krízových situácií v špecifickom prostredí*. ISBN 978-80-8070-846-7. Žilina: FŠI 2008, pp. 533-540

[392] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Concept of Safety of Complex Technological Facilities and Tools for Facility Safety Management. In*: Safety and Reliability – Theory and Applications.* ISBN: 978-1-315-21046-9. Leiden: CRC Přes/Balkema, pp. 3559-3567. www.crc.press.com, www.taylorandfrancis.com

[393] SCHNEIER, B. *Schneier on Security.* Newe York: John Wiley & Sonns 2008.

SUMMARY

Present book „Principles of supervision of risks of complex technological facilities “is compact study that in certain extent on present level of knowledge solves the transdisciplinary scientific research problem with the highest professional and social priority „human security and development “. The book content carries the vision of comprehensiveness, in which the practical problem solution is on the boundary of theory of chaos, in which there are exerted the non-linear linkages among the elements of different objects and networks. It shows the non-usefulness of detail study of part of complex system (system of systems) if the need is the safe system in dynamic world.

From the system viewpoint there is necessary for ensuring the complex technological facility to pursue: level of information activity for support of decision-making in matters dealing with the complex technological facility; fittings, arrangements and mechanisms supporting the complex technological facility safety; humans in complex technological facility as subjects and objects of facility safety; and procedures interconnecting the humans and the technological facility components (from the system viewpoint the protected assets of technological facilities are also the linkages and flows among all their items).

In the framework of supervision of risks of complex technological facility, it needs to be realise the next five key activities in complex technological **safety supervision**:

1. Definition of target and centre of interest of: the goal is to identify the context, to determine the priority goals and to determine the domain and centre of task. The options in this activity are based on the evaluation of interests and entities. By this way, we determine the important risks.
2. Description: the goal is to obtain the objective understanding of the size and probability of risk impacts (in qualitative or better in quantitative expression). It goes on the high technical or scientific activity.
3. Decision: the goal is the evaluation of quality of prediction if possible by descriptive way, comparison of positive and negative consequences. The decision, how to mitigate and to control the risk, and to implement measures is the key step of decision under the risk management frame.
4. Communication: the goal is the discussion with the key process partners and other participated persons. It would be included the communication with public, the consultations, the conflicts removing and the constitution of partnerships.
5. Monitoring and lessons: the goal is the activity that describes monitoring and consequences of decision and activities that cause the change of conditions and detection of new evidences. The activity needs to be oriented to outputs.

The control of unacceptable risk is performed by application of one from next options:

- to avoid the risk, ii means to stop the activities leading to risk origin, if possible,
- to remove the risk sources, if possible,
- to reduce the occurrence probability of risk, if possible,
- to reduce the severity of risk impacts by mitigating measures,
- sharing the risk among the participants,
- retention of risk.

The trade-off with risks of complex technological facility goes out from present chances of human society and it is divided in categories:

- part of risks is reduced by preventive measures,
- for part of risks the mitigate measures are prepared,
- part of risks is insured,

- for part of risks the response measures are prepared including the necessary material, technical and human reserves,
- for part of risk that is uncontrollable or too costly or low frequent the contingency plan is prepared.

The performance of countermeasures is separated among the all participating humans and resorts. The responsibility is on all management levels in human society (from politicians, state, regional and local administrative, facility top management, facility management, workers and citizens)

At choice of measures for work with risks on all levels it is necessary to ensure, that costs for trade-off with risks risk will be substantially lower than possible losses caused by risk realization.

Principles of supervision of risks of complex technological facilities on the level of interface of public administration and technological facilities management are determined for management levels of state hierarchy: political (Parliament, Government, public administration) – 4; strategic (public administration, owner of technological facility, investor of technological facility, operator of technological facility) - 8; tactic (public administration, owner of technological facility, investor of technological facility, operator of technological facility) – 4; operation / functional (operator of technological facility) – 5; and technical (operator of technological facility) – 19.

Principles of supervision of risks of complex technological facilities on the level of pragmatic trade-off with risks are determined for: technological facility concept and technological facility operation supervision - 21; demands on data, methods and techniques that ensure the quality decision-making and management of technological facility – 9; procedures for correct sitting, quality design, building, construction and operation of technological facility – 13; and procedures for ensuring the technological facility operation during the life cycle and support of basic functions of the State, i.e. the public interest – 23.

These principles have been presented on national and international professional seminars and conferences in which there were participated the engineers, who design, construct, operate or perform the surveillance on the technological facilities. The specialists support the implementation of these principles in real practice.

REJSTŘÍK KLÍČOVÝCH SLOV

V seznamu nejsou uvedena základní klíčová slova, na které je práce zaměřena, tj. bezpečí, bezpečnost, kritičnost, nebezpečí, ohrožení, riziko, řízení bezpečnosti, řízení rizik, složitý technologický objekt, technické dílo a zranitelnost, protože se vyskytují příliš často.

Titul:	**Zásady řízení rizik složitých technologických zařízení**
Autor:	Doc. RNDr. Dana Procházková, CSc., DrSc.
Recenzenti:	Prof. Ing. Josef Říha, CSc., DrSc. Doc. Ing. Václav Beran, CSc., DrSc.
Vydavatel:	ČVUT v Praze
Počet kopií:	200
Počet stránek:	364
Rok vydání:	2017

ISBN: 978-80-01-06182-4