ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

Ústav bezpečnostních technologií a inženýrství

Posouzení bezpečnosti vybraného kritického objektu z pohledu integrální bezpečnosti a návrh na snížení kritičnosti objektu

Safety Judgement of Selected Critical Facility in Terms of Integral Safety and the Proposal on Decreasing the Criticality of the Facility

DISERTAČNÍ PRÁCE

Doktorský studijní program: Inženýrská informatika

Obor: Inženýrská informatika v dopravě a spojích

Školitel: doc. RNDr. Danuše Procházková, CSc., DrSc.

Ing. Tomáš Kertis

Praha 2021

Prohlášení

Předkládám tímto k posouzení a obhajobě disertační práci, zpracovanou na závěr doktorského studia na ČVUT v Praze Fakultě dopravní.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užívání tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne

….....

podpis

Poděkování

Za dlouholetou spolupráci, poskytnutí odborných konzultací, cenných kontaktů a literatury děkuji školitelce paní doc. RNDr. Daně Procházkové, DrSc. Velmi děkuji všem pracovníkům ČVUT FD, kteří mi pomohli při vypracování disertační práce a přispěli svými radami a materiály během doktorského studia.

Za účast na bezpečnostním výzkumu děkuji současným i minulým zaměstnancům Dopravního podniku hl. m. Prahy a všem další zúčastněným expertům.

Za podporu, zprostředkování kontaktů, poskytnutí SW a HW vybavení, dále také odborných rad z hlediska kybernetiky, dopravního řízení a zabezpečení děkuji panu Ing. Petrovi Novobílskému a společnosti Q-media, s.r.o. Děkuji manželce paní Inně Kertis za podporu a trpělivost při mém doktorském studiu. Děkuji rodičům za podporu a otci panu Ing. Jánu Kertisovi za zprostředkování kontaktů se zaměstnanci Dopravního podniku hl. m. Prahy.

V neposlední řadě děkuji bývalým zaměstnavatelům společnosti Unicontrols, a.s. a VALEO autoklimatizace, k.s. a současnému zaměstnavateli Siemens Mobility, s.r.o., kteří mně umožnili flexibilní pracovní dobu a práci z domova, což pomohlo ke zvládnutí vědecké činnosti, pracovních povinností i rodinného života zároveň.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

Posouzení bezpečnosti vybraného kritického objektu z pohledu integrální bezpečnosti a návrh na snížení kritičnosti objektu

DISERTAČNÍ PRÁCE

Ing. Tomáš Kertis

Březen 2021

Abstrakt

Disertační práce se soustřeďuje na zabezpečení kritické infrastruktury, která vytváří základnu pro kvalitní život a za kritických podmínek také pro přežití lidí. Práce navrhuje metodiku, metody a nástroje pro analýzu aktiv kritické infrastruktury, určení jejich kritičnosti, scénářů dopadů pohrom na aktiva a návrh opatření ke snížení kritičnosti aktiv. Teoretické modely aplikuje v rámci bezpečnostního výzkumu provozu pražského metra, vybraného kritického objektu, provedeného ve spolupráci ČVUT s Dopravním podnikem hlavního města Prahy. Získané výsledky ověřuje ve spolupráci s experty z praxe. Disertační práce obsahuje zpracování reálných dat. Na jejich základě určuje kritická místa, na která se musí soustředit řízení bezpečnosti provozu a navrhuje opatření pro snížení kritičnosti metra, tj. zvýšení bezpečnosti.

Klíčová slova

Kritická infrastruktura, provoz objektu kritické infrastruktury, pražské metro, systémy řízení, kritičnost, bezpečnost, zabezpečení, All-Hazard-Approach, Defence-In-Depth, řízení rizik.

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

Safety Judgement of Selected Critical Facility in Terms of Integral Safety and the Proposal on Decreasing the Criticality of the Facility

DOCTOR´ THESIS

Ing. Tomáš Kertis

March 2021

Abstract

The Doctor´ Thesis focuses on security of critical infrastructure that creates the basis for live quality and under critical conditions also for human survival. The work proposes the methodology, methods, and tools for analysis of assets of the critical infrastructure, determination of their criticality, disasters impacts scenarios on the assets and proposal of measures for decreasing the criticality of assets. Theoretical models are applied in the safety research on the Praha metro operation, the selected critical facility, that has been performed in the cooperation with the Czech Technical University and the Prague Public Transit Company. The obtained results were verified in co-operation with experts from practice.

The Doctor´ Thesis includes processing the real data from the safety research. On its basis it determines the critical spots to which the operation safety management needs to concentrate and propose measures for decreasing the criticality, i.e., safety improvement.

Key words

Critical infrastructure, operation of the critical infrastructure facility, Praha metro, management systems, criticality, safety, security, All-Hazard-Approach, Defence-In-Depth, risk management.

Obsah

Seznam příloh

Příloha A: Popis metody sběru dat o provozu metra a jeho chování při možných situacích pomocí expertů, 47 stran.

Příloha B: Číselné označení pohrom / škodlivých jevů, 2 strany.

Příloha C: Aktiva ze skupiny „Vazby a Toky“ a kybernetická aktiva, která zajišťují propojení potřebná pro kritický personál a kritická technologická (fyzická) aktiva, 5 stran.

Seznam zkratek

AI	Artificial Intelligence (Umělá inteligence)
ARS	Автоматическая регулировка скорости (Automatická regulace rychlosti – zabezpečovací zařízení)
ASDŘ	Automatický systém dispečerského řízení
ASDŘ-D	ASDŘ dopravní
ASDŘ-E	ASDŘ elektro
ASDŘ-O	ASDŘ osvětlení
ASDŘ-T	ASDŘ technický/technologický
ATC	Automatic Train Control (Automatické řízení vlaku)
ATO	Automatic Train Operation (Automatický provoz vlaku)
ATP	Automatic Train Protection (Automatická ochrana vlaku)
CC	Common Criteria (Společná kritéria)
CIA	Confidentiality, Integrity, Availability (Důvěrnost, integrita (celistvost), dostupnost)
COBIT	Control Objectives for Information and Related Technology (řízení cílů pro informační a související technologie)
CSM	Common Safety Methods (Společné bezpečnostní metody)
CST	Common Safety Targets (Společné bezpečnostní cíle)
ČR	Česká republika
E/E/PE	Electric/Electronic/Programmable Electronic systems (Elektrické, elektronické a programovatelné elektronické systémy)
EU	European Union (Evropská unie)
FTA	Fault Tree Analysis (Analýza stromem poruch)
GOA	Goal of Automation (Cíl automatizace)
IEC	International Electrotechnical Commission (Mezinárodní elektrotechnická komise)
IRIS	International Railway Industry Standard (Mezinárodní standard drážního průmyslu)
ISMS	Information Security Management System (Systém řízení zabezpečení informací)

ISO	International Organization for Standardization (Mezinárodní organizace pro normalizaci)
ITIL	Information Technology Infrastructure Library (Knihovna infrastruktury informačních technologií)
KI	Kritická infrastruktura
LZA	Liniový zabezpečovač pro trať A pražského metra
MHD	Městská hromadná doprava
MS	Microsoft (společnost)
OECD	Organisation for Economic Co-operation and Development (Organizace pro hospodářskou spolupráci a rozvoj)
OSN	Organizace spojených národů
PC	Personal Computer (Osobní počítač)
(P)CD	(Probability of) Proper Decision (Pravděpodobnost správného rozhodnutí / správné rozhodnutí)
RAMS	Reliability, Availability, Maintainability, Safety (Bezporuchovost, dostupnost, udržovatelnost, bezpečnost)
SDM	Sdělovací a zabezpečovací dispečink metra
SMS	Safety Management System (Systém řízení bezpečnosti)
SoS	System(s) of Systems (Systém(y) systémů)
SPT	Samostatný provozní technik
SW	Software
SZZ	Staniční zabezpečovací zařízení
TQM	Total Quality Management (Řízení celkové jakosti)
TSS	Total Safety Systems (Systémy celkové bezpečnosti)
TPS	Total Preventive Systems (Systémy celkové prevence)
UGTMS	Urban Guided Transport Management and Control System (Systém řízení městské kolejové dopravy)
UPS	Uninterruptible Power Supply/Source (Zdroj nepřerušovaného napájení)
VKV	Velmi krátké vlny
VZZ	Vlakové zabezpečovací zařízení

Seznam obrázků

Seznam tabulek

1 Úvod

Životy a zdraví lidí, jejich majetek a blaho, životní prostředí a také technologie a kritická infrastruktura jsou základními veřejnými aktivy lidského systému, který je modelem světa, ve kterém žijeme [1,2]. Kritická infrastruktura je důležitým aktivem, protože zajišťuje základní výrobky a služby pro lidi. Proto v případě kritických podmínek, jako například při výskytu velkých živelních, technologických a jiných pohrom, je třeba, aby prvky kritické infrastruktury bezpečně plnily své úkoly.

Předmětný úkol je dnes složitější a obtížný, protože dochází ke zvyšujícímu zavádění nových neozkoušených technologií a jejich propojování. Propojováním systémů vznikají tzv. složité (komplexní) systémy a nové funkce, které by za normálních okolností jednotlivých nepropojených systémů nevznikly, proto se jedná o takzvaný systém systémů. Za pomoci žádaných vazeb vytvořených podle norem mají předmětné komplexní systémy systémů vysokou spolehlivost za normálních provozních podmínek, tj. podmínek, které jsou zvažovány v projektu. Pomocí provozních předpisů jsou zvládnuté výchylky, které nastávají při abnormálních provozních podmínkách. Problémy nastávají při kritických podmínkách, kdy se často vyskytují nežádané a nežádoucí vazby, které vedou k selhání kritických aktiv, a tím ohrožují celý systém i jeho okolí. Proto je třeba hledat kritická aktiva systému, hodnotit jejich kritičnosti a zajišťovat jejich provozuschopnost i za nepříznivých podmínek. Hodnocení kritičnosti aktiv umožňuje identifikovat a řídit významná rizika, analyzovat zranitelnosti systému a navrhovat opatření pro zvýšení jeho bezpečnosti.

Při řízení bezpečnosti kritické infrastruktury je nezbytné počítat s aktivy a vazbami, které za určitých podmínek mohou vést k selhání systému. Tzn. je nutné je zahrnout do analýzy aktiv a jejich kritičností a definovat pravidla pro práci s nimi [3]. Současné znalosti, metody a nástroje umožňují zajištění bezpečnosti infrastruktur na jisté úrovni, ale z důvodu neustálého rozvíjení technologií, nároků na rozhraní mezi systémy i operujícími subjekty se stále ukazuje, že existují nezajištěná místa.

Oblast bezpečnosti a zabezpečení kritické infrastruktury kvůli složitosti kritické infrastruktury se vyznačuje prací s mnoha měkkými faktory, objekty a subjekty v rámci systému systémů (dále jen SoS). Z důvodu rozsahu a složitosti mnoha

vnitřních propojení ve studovaném objektu lze systém analyzovat pouze expertními a heuristickými metodami. Existuje mnoho metod a nástrojů systémové analýzy a inženýrství, ale neexistuje formalizovaný metodický postup pro stanovení kritičnosti jednotlivých prvků (aktiv) kritické infrastruktury, míry bezpečnosti a návrh opatření pro zvýšení bezpečnosti. Proto jsem se na problematiku bezpečnosti kritické infrastruktury zaměřil ve svém doktorském studiu.

Doktorské studium v oboru Inženýrská informatika v dopravě a spojích na Ústavu bezpečnostních technologií a inženýrství jsem navázal na svojí Diplomovou práci zaměřenou na plán bezpečnosti modelové stanice metra [4]. V rámci doktorského studia jsem provedl výzkum bezpečnosti provozu pražského metra s případovými studiemi ve spolupráci s Dopravním podnikem hlavního Města Prahy [5]. Cílem bylo najít a ověřit vhodný metodický postup, navrhnout metodu pro analýzu a stanovení kritičností aktiv, dále pak ověřit postupy na konkrétním případu, tj. zajištění bezpečného provozu metra jako prvku kritické infrastruktury.

Výsledky práce, a to jak definované metody či konkrétní případové studie a události, byly průběžně prezentované na řadě českých i mezinárodních konferencí a také zveřejněné v řadě odborných recenzovaných i impaktovaných publikací.

Předložená disertační představuje ve své první části rešerši zaměřenou na nejmodernější metody v oblast řízení bezpečnosti a stav inženýrské praxe a techniky. V další části zavádí metodologii pro identifikaci a analýzu aktiv objektu kritické infrastruktury, stanovení jejich kritičností a následné zpracování pro analýzu primárních rizik, hledání scénářů dopadů různých událostí a tím umožnění jejich zvládnutí, respektive jejich řízení. Kromě heuristických metod také aplikuje teorii citlivosti a teorii grafů. V posledních dvou částí pak uvádí výsledky výzkumu bezpečnosti provozu pražského metra, jejich diskusi, vyhodnocení a návrhy opatření na zvýšení bezpečnosti provozu metra.

Výsledky disertační práce lze aplikovat na další podobné složité systémy, u kterých je zapotřebí identifikovat a řídit slabá místa, při kterých je třeba zvažovat zranitelnost a důležitost jejich aktiv, kritičnost a bezpečnost. Oblasti aplikovatelnosti výsledků disertační práce jsou kritické infrastruktury, prvky kritické infrastruktury, řízení kritických aktiv a řízení bezpečnosti v území či složitých technologických celků.

1.1 Cíle a rozsah vědecké práce

Tématem práce je posouzení bezpečnosti vybraného kritického objektu z pohledu integrální bezpečnosti a návrh na snížení kritičnosti objektu, tj. zvýšení jeho bezpečnosti. Vybraným kritickým objektem je metro v Praze.

Hlavním cílem práce je zvýšení bezpečnosti metra aplikací metod pro identifikaci a práci s aktivy, jejich kritičnostmi a riziky tak, aby bylo možné zajistit celkovou (integrální) bezpečnost metra na základě zvýšení znalostí o problémech a zranitelnostech aktiv, a to v oblasti techniky, v oblasti kybernetické, kde jde o zvýšení informačního výkonu systému, a dalších oblastech řízení, které jsou důležité pro bezpečný provoz.

Dílčí cíle disertační práce jsou:

- zvýšit znalost o problémech, rizicích systémů a jejich zvládání,
- data o sledovaném problému, tj. data o provozu pražského metra,
- stanovit metodický postup, popsat metody a nástroje pro práci s aktivy,
- identifikovat a určit kritičnosti aktiv pro bezpečné řízení provozu pražského metra,
- vhodně interpretovat a vyhodnotit výsledky pro další práci s aktivy,
- transformovat výsledky do grafů s cílem najít slabá místa provozu metra z hlediska bezpečnosti,
- analyzovat a vyhodnotit vybraný scénář dopadů na pohromy,
- navrhnout opatření pro snížení kritičností aktiv metra a tím snížit jeho celkovou kritičnost a zvýšit jeho bezpečnost.

1.2 Formulace vědeckého problému

Předložená disertační práce je zaměřena na studium složitých systémů typu SoS (systém systémů) v reálném světě a na zajištění jejich bezpečnosti. Z důvodu složitosti systémů je třeba zohledňovat kritičnost aktiv v závislosti na různých zdrojích rizik v reálném světě. Zvláště při realizaci nadprojektových jevů, které jsou původci rizik, dochází ke kritickým situacím, které jsou způsobeny vznikem nežádaných propojení v složitém systému, tj. vznikají neočekávaná propojení, která vedou k selhání, a často k celým kaskádám selhání [6]. Tím vznikají dopravní

nehody, jejichž důsledkem jsou ztráty na lidských životech, škody na majetku veřejném i dopravce a na životním prostředí.

Vzájemné závislosti (angl. Interdependences), a to žádané i nežádané, mají povahu fyzickou, logickou, kybernetickou a místní [6], což znamená, že problematika je velmi široká. Při zvážení povahy SoS (tj. socio-kyber-fyzického systému), kterým je i pražské metro, lze navíc konstatovat, že se jedná o měkký systém, kde vzniká mnoho problémů především z nedostatečného řízení, tj. managementu, na různých úrovních a v různých souvislostech mezi technikou, informačním systémem a lidským faktorem.

Při zajištěných jistých podmínek technického díla, resp. řešeného systému, lze některé situace řešit exaktními metodami, avšak bezpečnost zasahuje především do oblasti mimo uvedené limity a podmínky systémů, tj. nadprojektové jevy. Za uvedených podmínek, a kvůli anizotropiím a nehomogenitám v systému i jeho okolí, vznikají v SoS propojení, která nebyla zvažována v projektu [6]. Proto u velmi komplexních systémů s velkým počtem známých i neznámých stavů, nelze za uvedených podmínek s určitostí predikovat jejich chování, tj. vznikají tzv. emergentní jevy (jevy, které vznikají spontánně a nelze je jednoduše odvodit z vlastností prvků systému a jejich vazeb).

Předložená disertační práce, vzhledem k výše uvedenému rozsahu a složitostem, proto používá metody multikriteriální a heuristické a zaměřuje se pouze na vybrané části problémů v řízení bezpečnosti řešeného systému. Pro řešení uvedeného problému používá postup uvedený níže.

1.3 Metodika zpracování disertační práce

K dosažení výsledků práce byl použit následující postup:

1. Výběr a návrh metod a nástrojů pro:
   - pro sběr dat – identifikaci aktiv, zranitelností (výběr),
   - pro práci s daty – stanovení kritičností a jejich interpretace (výběr),
   - pro transformaci matic citlivostí (zranitelností) do grafu (návrh),
   - tvorbu scénářů dopadů (návrh).
2. Identifikace aktiv objektu kritické infrastruktury (provozu pražského metra).

3. Určení zranitelností a kritičností aktiv.
4. Zjištění reálného stavu zabezpečení systému vůči specifickým a kritickým pohromám.
5. Interpretace výsledků pomocí matic citlivostí.
6. Transformace matic do grafu.
7. Modelování scénářů dopadů na vybranou kritickou pohromu.

1.4 Očekávaný přínos disertační práce

Disertační práce přispívá aplikací pokrokových metod, nástrojů a recentních znalostí ke zvýšení integrální bezpečnosti systému, jak požaduje koncept OSN [9]. Výsledky práce, tj. návrh opatření na celkové zvýšení bezpečnosti provozu pražského metra byly předány Dopravnímu podniku hl. Města Prahy pro implementaci v praxi [7].

Práce uvádí řadu otevřených neošetřených zranitelností, čímž otevírá možnost novým výzkumným projektům. Navržené metody a nástroje disertační práce lze dále rozvíjet a podpořit vhodnými softwarovými nástroji, čímž je otevřena možnost dalším projektům v rámci vývoje a inovací.

Přínosem práce je souhrn poznatků, stanovení a ověření metody, která umožňuje dosažení vyšších cílů než jen bezpečnost procesů nebo jednotlivých technických zařízení, tj. dosažení integrální bezpečnosti. To je v souladu nejen s cíli odborného poznání, ale především s požadavky OSN i EU na bezpečný a udržitelný svět [2,8,9].

2 Rešeršní část – souhrn poznatků o sledovaném problému

Disertační práce vyhodnocuje zranitelnosti a kritičnosti vztažené k aktivům bezpečného provozu metra (tj. drážního systému), které je součástí dopravní kritické infrastruktury, přičemž zvažuje relevantní pohromy, které mohou danou infrastruktury postihnout. Následující odstavce poskytují rešerši základních poznatků a znalosti relevantní k uvedené problematice.

2.1 Definice použitých pojmů

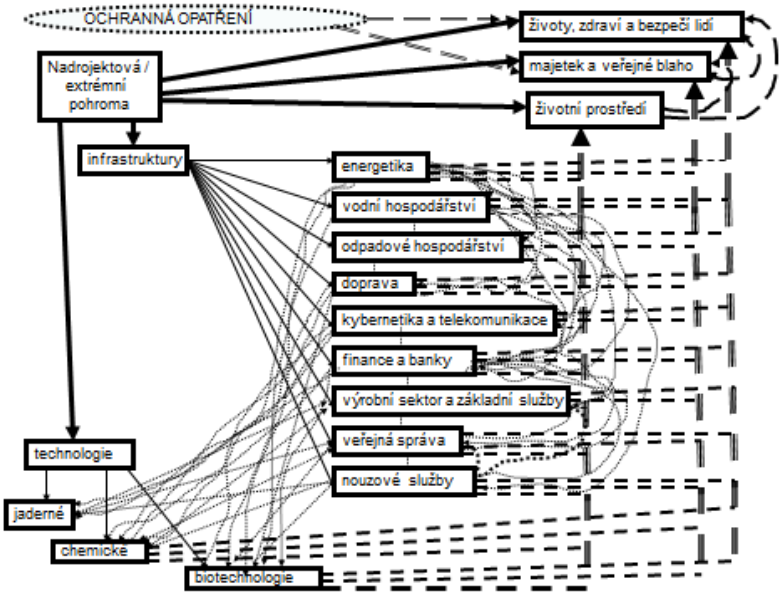
Na základě analýzy zdrojů [1-6,8-76] je dále uveden souhrn znalostí a odkazy vztahující se k použitým termínům a k jejich definicím, použitým v předložené disertační práci.

2.1.1 Aktiva

Aktivem se rozumí fyzická, logická či kybernetická položka, která určuje strukturu a chování sledovaného systému [6]. Výsledky prací [1,4] poskytují seznamy identifikovaných aktiv modelové stanice metra a systému řízení pražského metra (tj. lidi, majetek včetně technologií, energetické informační a materiálové toky), a to především na základě analýz dokumentace metra [1,4,10,11]. Vzhledem k tomu, že se jedná o otevřený systém systémů, je nutné zvažovat mimo technické části, zvažované v [1,4] také další aspekty, tj. například organizační, finanční, funkční, logické vazby, a další. Pro účely dalších analýz a uvažujeme následující skupiny aktiv: konstrukce, technika, personál, místa, funkce, vazby a toky, organizace a ekonomika.

2.1.2 Pohromy

Příčinou rizik jsou pohromy (všeho druhu), tzv. All-Hazard-Approach [12]) a v případě rizik u technologických systémů se jedná také o poruchové stavy v důsledku náhodných či systematických chyb systému [4,13]. Z výše uvedeného je patrné, že vznik jedné extrémní pohromy může vyvolat řetězec dalších pohrom, tj. sekundární dopady, i celou kaskádu dopadů. Sekundární, terciální a další dopady jsou označovány jako nepřímé dopady. Nepřímé dopady extrémních pohrom jsou znázorněny na obrázku 1. Obrázek 1 ukazuje propojení dopadů extrémní pohromy s různými chráněnými aktivy, které vyvolají další dopady na jiná aktiva, tj. nepřímé dopady, které mají tvar kaskád (tj. kaskádový efekt).



Obrázek 1. Účinky extrémních pohrom na veřejná aktiva [14].

Podle velikosti škod a ztrát na veřejných aktivech a pravděpodobnosti výskytu, tj. na základě analýzy a vyhodnocení rizik pomocí metody matice rizik dle [13], lze pohromy v řízení bezpečnosti kategorizovat do tří kategorií:

1. ***Pohromy kritické:*** mohou vyvolat na sledovaném území nebo jeho části kritickou situaci, při které, podle současné české legislativy, může být vyhlášena krizová situace, a tudíž bude třeba dělat obnovu majetku po krizové situaci. Z pohledu řízení bezpečnosti je třeba dělat preventivní a zmírňující opatření v územním plánování, projektování, výstavbě a provozu občanských a technologických objektů i infrastruktury.
2. ***Pohromy specifické:*** mohou vyvolat nouzové situace, a proto s nimi musí počítat odezva a připravenost (opatření na zmírnění). Z pohledu řízení bezpečnosti je třeba dělat preventivní opatření v územním plánování, projektování, výstavbě a provozu občanských a technologických objektů i infrastruktury a zmírňující opatření v rámci připravenosti na odezvy.
3. ***Pohromy relevantní:*** všechny ostatní pohromy, které mohou entitu postihnout a nejsou kritickými ani specifickými. Měly by být zvládnuty běžnými standardními prostředky, tj. prevencí prováděnou v praxi. Z pohledu řízení bezpečnosti dosavadní opatření prováděná v územním plánování,

projektování, výstavbě a provozu občanských a technologických objektů i infrastruktury jsou dostatečná, a tudíž je nutná jen pravidelná kontrola jejich účinnosti.

Pro účely předložené disertační práce byly použité následující pohromy, identifikované v práci [4] analýzou archivních dokumentů hl. m. Prahy [15]:

Výsledky procesů probíhající vně i uvnitř Země: povodeň, vichřice, zemětřesení, ztekucení podloží, výstup plynu na zemský povrch.

Výsledky procesů v lidském těle, v chování lidí a procesů v lidské společnosti: epidemie, pandemie, porucha stability lidské společnosti, útok, teroristický útok, útok za použití chemických, jaderných, radiologických a biologických (CBRNE) zbraní, ozbrojený konflikt, válka.

Výsledky procesů a činností instalovaných lidmi: průmyslová havárie, havárie při přepravě či skladování nebezpečných látek, havárie při dopravě, pohroma v oblasti kritické infrastruktury, pohroma v ekonomice, pohroma v územní infrastruktuře, pohroma v kybernetické infrastruktuře, pohroma v infrastruktuře služeb, zásobování a spojení, selhání technologií, ztráty obslužnosti.

Interakce planety Země a životního prostředí na činnosti lidí: porušení stability podloží vlivem vibrací, kontaminace ovzduší, kontaminace vody, rychlé variace klimatu, migrace velkých skupin lidí.

Vnitřní závislosti v lidském systému přirození nebo lidmi vytvoření: organizační havárie, porucha toků surovin a výrobků, porucha v toku energií, porucha v toku informací.

Tabulka 1 obsahuje rozdělení pohrom, které jsou relevantní pro hl. m. Prahu, do kategorií, podrobnosti jsou uvedené v práci [4]. Tj. zvažuje přístup All-Hazard-Approach [12,13] a data [15]; detaily jsou v pracích [12,13,16].

Tabulka 1 Rozložení pohrom – relevantní, specifické, kritické.

	Relevantní	Specifické	Kritické
Výsledky procesů probíhající vně i uvnitř Země			
Povodeň	ano	ano	ano
Vichřice	ano	ano	
Zemětřesení	ano		

Ztekucení podloží	ano	ano	ano
Výstup plynu na zemský povrch	ano		
Výsledky procesů v lidském těle, v chování lidí a procesů v lidské společnosti			
Epidemie	ano	ano	ano
Pandemie	ano	ano	ano
Porucha stability lidské společnosti	ano	ano	
Kriminalita	ano	ano	
Útok	ano	ano	
Teroristický útok	ano	ano	ano
Útok za použití chemických, jaderných, radiologických a biologických (CNRB) zbraní	ano	ano	ano
Ozbrojený konflikt	ano	ano	ano
Válka	ano	ano	ano
Výsledky procesů a činností instalovaných lidmi			
Průmyslová havárie	ano		
Havárie při přepravě či skladování nebezpečných látek	ano		
Havárie při dopravě	ano	ano	ano
Pohroma v oblasti kritické infrastruktury	ano	ano	
Pohroma v ekonomice	ano		
Pohroma v územní infrastruktuře	ano		
Pohroma v kybernetické infrastruktuře	ano	ano	
Pohroma v infrastruktuře služeb, zásobování a spojení	ano		
Selhání technologií	ano	ano	ano
Ztráty obslužnosti	ano		
Interakce planety Země a životního prostředí na činnosti lidí			
Porušení stability podloží vlivem vibrací	ano	ano	ano
Kontaminaci ovzduší	ano	ano	
Kontaminace vody	ano	ano	
Rychlé variace klimatu	ano		
Migrace velkých skupin lidí	ano		
Vnitřní závislosti v lidském systému přirozené nebo lidmi vytvořené			
Organizační havárie	ano	ano	ano
Selhání toků surovin a výrobků	ano		
Selhání toků energií	ano	ano	ano

Selhání toků informací	ano	ano	ano

2.1.3 Riziko a kritičnost

Pojem riziko má v mnoha oblastech rozdílné a nejednotné pojetí, některé definice rizika staví na pravděpodobnosti, jiné pak na očekávané hodnotě nebo nejistoty a neurčitosti [17]. Z hlediska projektového řízení a systému řízení bylo riziko obecně definováno jako „účinek nejistoty“ [18]. Účinek nejistoty, pokud dojde k její realizaci, může nabývat negativních, ale i pozitivních vlastností (tj. příležitosti) [18].

Riziko v inženýrských oborech, jako je řízení rizik systému, řízení spolehlivosti a řízení bezpečnostních rizik, ***vyjadřuje pravděpodobnou velikost nepřijatelných (tj. nežádaných) dopadů (ztrát, škod a újmy) pohromy o velikosti ohrožení (tj. potenciál pohromy normativně určený) na chráněné zájmy (aktiva) za stanovený časový interval v určitém místě*** [17].

Zdrojem uvedených rizik jsou pohromy uvedené předchozím odstavci. Jedná se o rizika pro člověka, jeho majetek, životní prostředí, kritickou infrastrukturu a v neposlední řadě i pro stát. Rizika lze členit podle toho, jaká jsou pro zvážení rizika zvolená chráněná aktiva a zda je sledováno jedno chráněné aktivum (tj. dílčí riziko) či soubor chráněných aktiv (integrované riziko) nebo soubor chráněných aktiv a vazby a toky mezi nimi (komplexní riziko / integrální riziko).

Dále se rizika dělí podle toho, jaké pohromy, resp. zdroje pohrom, se berou v úvahu (pouze některé pohromy, část jejich scénářů nebo veškeré relevantní pohromy apod.).

V běžné praxi, a především u dopravních systémů, se počítá většinou s riziky dílčími a integrovanými, která bývají vyjádřená součinem pravděpodobnosti výskytu pohromy (resp. incidentu nebo selhání) či četnosti výskytu a velikosti jejich dopadů (ztrát, škod, újmy) na sledovanou entitu či vybraný soubor entit. Veličin pro výpočet rizika může být dle sledované oblasti mnoho, ale většinou se jedná o součin výše dvou uvedených. V podrobnějších studiích se zvažuje míra zranitelnosti a někdy též míra ovladatelnosti škodlivé události; například v oblasti automobilového průmyslu [19].

V chápání rizika (R) tedy pozorujeme mnoho rozdílů a společné je jen to, že riziko vychází z obav z nejisté budoucnosti [5,17]:

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.

Pro zajištění bezpečného území, popřípadě větších technologických celků nebo zařízení, je nutné počítat s komplexním rizikem, tj. rizikem integrálním založeném na systémovém pojetí reality [2]. 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 (anglicky interdependences) [4,17].

Integrální riziko označené jako ***R*** je pro všechny pohromy v území dané vztahem [17]:

$$\boldsymbol{R} = \sum_{k=1}^{m} \boldsymbol{R_k} \qquad (1)$$

$\boldsymbol{R_k}$ vyjadřuje riziko pro k-tou pohromu:

$$\boldsymbol{R_k} = \sum_{i=1}^{n} \boldsymbol{P_k} \cdot \boldsymbol{D_{i,k,}} \qquad (2)$$

$\boldsymbol{P_k}$ označuje pravděpodobnost výskytu k-té pohromy a $\boldsymbol{D_{i,k}}$ dopad k-té pohromy na i-tý chráněný zájem. Podobné vztahy jsou aplikované i pro integrované riziko, ovšem s tím rozdílem, že dopady $\boldsymbol{D_{i,k}}$ pro riziko integrální zahrnují mimo přímé dopady $\boldsymbol{DD_{i,k}}$ i dopady nepřímé (sekundární, terciální a více) $\boldsymbol{DI_{i,k}}$, jejichž vztahy jsou dle zdroje [19] následující:

$$\mathbf{DD_{i,k}} = \int_S \mathbf{Z_{i,k}} \cdot \mathbf{V_i dS}\,;\ \mathbf{DI_{i,k}} = \int_S \mathbf{I_{i,k}} \cdot \mathbf{V_i dS} \qquad (3)$$

V_i je hodnota chráněného zájmu, **S** je sledované území či objekt, $Z_{i,k}$ je zranitelnost i-tého chráněného zájmu při k-té pohromě, $I_{i,k}$ je funkce vzájemných vazeb (interdependences). Vzájemné vazby závisí na konkrétní struktuře chráněných zájmů v území a konkrétních propojení chráněných zájmů a na pohromě, tj. dle [17]:

$$\boldsymbol{I_{i,k} = f\left(VD_k, VP_{i,k}\right)} \quad (4)$$

VD_k je charakteristika míry k-té pohromy, která ovlivňuje dopady na chráněná aktiva. $VP_{i,k}$ charakteristika míry vzájemné propojitelnosti chráněných zájmů v daném území. Stanovení $VP_{i,k}$ je předmětem podrobného výzkumu na základě Booleovské logiky nebo při složitějších vazeb na základě metod operační analýzy [17,19,20].

Pro technické systémy [21] platí vztah:

$$\boldsymbol{R(H) = \left[\sum_{i=1}^{n} A_i(H) Z_i(H) + \sum_{i=1}^{n} \int_0^T \int_S F(H, A_i, P_i, O, t) dS dt\right] \cdot \tau^{-1}} \quad (5)$$

ve kterém **H** je ohrožení spojené s danou pohromou v místě objektu; A_i jsou hodnoty sledovaných aktiv pro i = 1,2,…, n; Z_i jsou zranitelnosti aktiv pro i = 1,2,…, n; **F** je ztrátová funkce; P_i jsou pravděpodobnosti výskytu poškození aktiv pro i = 1,2,…, n – jde o podmíněné pravděpodobnosti; **O** zranitelnost ochranných opatření; **S** velikost sledovaného objektu; **t** je čas měřený od vzniku škodlivého jevu; **T** je čas, po který vznikají ztráty; a τ je perioda opakování pohromy. Jelikož není obvykle známa ztrátová funkce, tak se vytváří scénáře selhání a k ocenění rizika se používají multikriteriální metody; obvykle systémy pro podporu rozhodování [22].

Z výše uvedených znalostí a vzhledem ke komplexnosti (složitosti) systémů je zřejmé, že ***integrální bezpečnost lze zvyšovat*** pouze při zvažování a řízení integrálních rizik, které nezvažují pouze součet dílčích rizik, ale počítají i s vazbami a toky mezi aktivy [13].

Pro účely řízení bezpečnosti se ***kritičností aktiva*** (K) rozumí funkce důležitosti a zranitelnosti sledovaného aktiva nebo i celé entity vyjádřená součinem [13,17]:

K = důležitost · zranitelnost (6)

Kritičnost s ohledem na jistou pohromu lze vyjádřit vztahem

C = S · O · B (7)

ve kterém ***S*** je závažnost největšího dopadu pohromy (škodlivého jevu), ***O*** pravděpodobnost výskytu pohromy a ***B*** podmíněná pravděpodobnost, že se vyskytne nejzávažnější dopad [13,23].

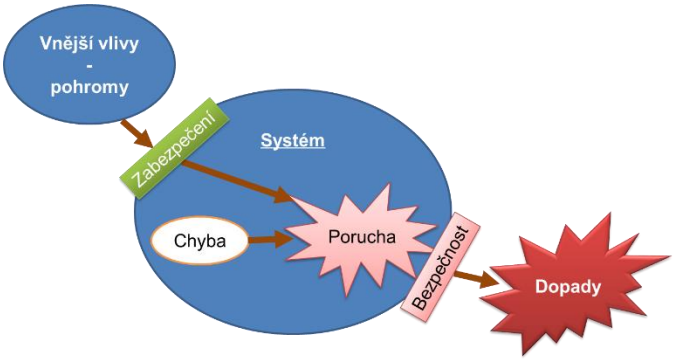
Riziko, jak již bylo zmíněno v úvodu tohoto odstavce, se odkazuje na účinek nejistoty, tj. jak často (resp. pravděpodobně) dojde k jak rozsáhlým ztrátám. Snižováním rizika snižujeme četnost výskytu nepříznivé události (pokud je to v naší moci) nebo její dopady. Riziko tímto souvisí s bezpečností, ale není jím bezpečnost definována. Kritičnost se vztahuje na mezní (prahovou) hodnotu mezi dvěma stavy, v oblasti bezpečnosti jde o nežádoucí (nebezpečí) a žádoucí (bezpečí). Snižováním kritičnosti, tj. prahové hodnoty mezi nebezpečí a bezpečí, zvyšujeme stavový prostor systému v bezpečné oblasti, tj. zvyšujeme bezpečnost. Proto je kritičnost komplementární veličinou k bezpečnosti, i když je kritičnost důsledkem rizikových faktorů a může mít s rizikem stejné vstupní parametry (např. zranitelnost) [27].

2.1.4 Bezpečnost

V současné praxi se pojmu bezpečnost přikládá několik různých významů. V dopravních systémech je pojem bezpečnost spojován s: ochranou lidí bez zvážení vazeb se systémem; odolností systému proti narušení nějakou nepříznivou událostí (pohromou); nebo proti vnitřním chybám. Ve spojení s ochrannými, resp. zabezpečovacími systémy je bezpečnost chápána jako tzv. funkční bezpečnost, tj. realizace bezpečné funkce nebo procesu v případě předvídaných situací [24]. Ve skutečnosti mají zmíněné významy stejný cíl, chránit zdraví a životy lidí, a zajistit rozvoj lidské společnosti, tj. všechny významy jsou součástí integrální bezpečnosti, která všechny slučuje dohromady.

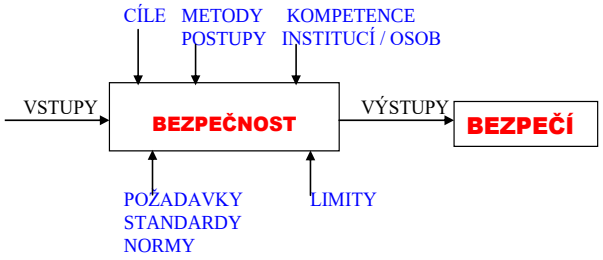
Systémová bezpečnost v kontextu integrální bezpečnosti znamená, že je systém chráněn proti interním i externím pohromám, včetně lidského faktoru, tj. systém má dostatečnou odolnost a přizpůsobivost vůči očekávaným podmínkám. Bezpečný systém navíc nesmí neohrozit své okolí ani v jeho kritických podmínkách [20,25,26,27], Obrázek 2 dle [20].

Případné dopady poruch systémů znázorněné na obrázku 2 se projeví u dalších systémů jako pohroma v jejich okolí, v tomto případě vzniká zřetězení pohrom, tj. kaskádový efekt.



Obrázek 2. Vztah mezi bezpečností a zabezpečením systému [20].

Pojem bezpečnost (Safety) dle současných znalostí znamená soubor prostředků a opatření, kterými lidstvo zajišťuje svoje bezpečí (angl. Security) a udržitelný rozvoj (angl. Sustainable Development). Na obrázku 3 je znázorněn koncept zacílený na bezpečí, tj. na vyšší cíl; nejde jen o snížení rizika, ale o zvýšení bezpečí lidí a dalších veřejných aktiv, na kterých jsou lidé závislí [27].



Obrázek 3. Vztah mezi bezpečím a bezpečností, jako nástrojem k zajištění bezpečí [27].

Z výše uvedeného vyplývá, že bezpečnost a riziko sice spolu souvisí, ale nejsou komplementárními veličinami, protože bezpečnost lze zvýšit i organizačními opatřeními, kterými velikost rizika neovlivníme. K bezpečnosti je komplementární veličinou kritičnost. ***Snižováním kritičnosti zvyšujeme bezpečnost sledovaného objektu***.

2.1.5 Bezpečí lidí a integrální bezpečnost

Bezpečí lidí (anglicky Human Security), jehož zajištění je cílem řízení bezpečnosti, je téma známé od počátku lidstva, nicméně je tento pojem v oblasti bezpečnostních věd definován teprve nedávno. Organizace spojených národů definovala Bezpečí lidí jako koncept, který znamená:

„… ochraňovat nezbytný základ všech lidských životů takovým způsobem, který lidi obohatí o jejich svobodu a seberealizaci. Bezpečí lidí znamená chránit základy svobod – svobod, které jsou podstatou života. To znamená chránit lidi před kritickými (závažnými) a všudypřítomnými (rozsáhlými) hrozbami a situacemi, To znamená používat procesy, které staví na lidských silných stránkách a touhách. To znamená vytvářet politické, sociální, environmentální, ekonomické, vojenské a kulturní systémy, které společně pro lidi poskytují základní stavební kameny pro jejich přežití, obživu a důstojnost… „ [8].

Jedná se tedy především o změnu přístupu od pouhé ochrany státu před hrozbami nepřátelských ozbrojených sil k přístupu, který klade důraz na životy lidí a jejich ochranu před dalšími známými hrozbami. Základní oblasti konceptu „Bezpečí lidí a jejich hrozby“ jsou dle OSN následující [8]:

- zabezpečení ekonomiky (přetrvávající bída, nezaměstnanost),
- zabezpečení potravin (hlad, hladomor),
- zabezpečení zdraví (smrtelné infekční choroby, nebezpečné jídlo, podvýživa, pochybení v základní zdravotní péči),
- zabezpečení životního prostředí (environmentální degradace, úbytek zdrojů, živelní pohromy, znečištění),
- osobní zabezpečení (fyzické násilí, kriminalita, terorismus, domácí násilí, týrání dětí),
- politické zabezpečení (inter-etnikum, náboženství a další napětí založené na identitě),
- zabezpečení politiky (politická represe, zneužívání lidských práv).

Z hlediska ekonomického zabezpečení klade koncept Bezpečí lidí důraz na obnovu (rehabilitaci) dopravy a dopravních cest. Doprava podmiňuje úspěšné plnění cílů jednotlivých oblastí zabezpečení, tj. konceptu Bezpečí lidí, zároveň může naopak předmět jednotlivých cílů vlastními chybami a slabinami poškodit. Z toho vyplývá, že doprava a dopravní systém vytváří nové hrozby, kterými jsou například znečištění, přímý vliv na životy a zdraví lidí a majetek [19].

Státy zajišťují bezpečí lidí a jednotlivé cíle zabezpečení pomocí tzv. hlavních funkcí státu. Jedním z prostředků je infrastruktura [2]. Zaměřením předložené práce je infrastruktura dopravní a související kritická infrastruktura (například kritická informační infrastruktura).

Nástrojem k zajištění bezpečí lidí je ***integrální bezpečnost***, která je zajišťována různými druhy bezpečnostních metod a technologií. Zastřešuje další inženýrské oblasti, jako jsou například řízení spolehlivosti, funkční bezpečnost, zabezpečení kyber-fyzických systémů, technické i fyzické zabezpečení, ostraha, bezpečnost práce, zajištění bezpečného místa, bezpečnost lidí aj. Integrální bezpečnost se zabývá bezpečností více aktiv ve sledované oblasti, které navzájem interagují, jsou vzájemně provázané a mají různé typy vazeb s nadřazenými a okolními systémy. Koncept integrální bezpečnosti zároveň zvažuje výskyt všech možných zdrojů ohrožení, která mohou sledovanou entitu postihnout [2]. Řízení integrální bezpečnosti pracuje s řízením integrálních rizik [19].

Reálný svět, který vnímáme, není ideální, a proto kvůli nedokonalostem a rozdílnostem v něm vznikají konflikty. Konflikty vznikají také v jednotlivých oblastech zabezpečení, bezpečnosti i mezioborových kontextech. Důsledkem je, že zvyšováním zabezpečeni jednoho prvku sledovaného systému můžeme nepřímou úměrou zhoršovat bezpečnost prvku druhého, tím ovlivňujeme integrální bezpečnost i celkové bezpečí lidí.

Z výše uvedeného je patrné, že pro to, aby byla zajištěná integrální bezpečnost, nestačí zvyšovat bezpečnost nebo zabezpečení jednotlivých prvků systému, které svými vzájemnými vazbami tvoří komplexní systém, ale musíme zajistit efektivnější systém řízení, který je schopen se se složitostí reálného světa co nejlépe vypořádat [19].

Zvyšování integrální bezpečnosti je založené na procesním a projektovém řízení, jejichž cílem je neustálé zlepšování kvality a zachování jisté míry bezpečnosti systémů při dynamicky se měnících podmínkách reálného světa (okolní fyzikální podmínky, vazby s jinými systémy, změna kultury a chování jednotlivců či skupin lidí apod.). V podmínkách Evropské unie se používá projektové řízení typu tzv. řízení celkové jakosti (angl. Total Quality Management, dále jen TQM) [28]. Pro jeho úspěšnost byly vytvořeny ISO normy třídy 9000, 14000 apod.

Přístup TQM spočívá na požadavku, že na procesu zlepšování kvality entity se podílí všichni zaměstnanci, od řadových zaměstnanců až po nejvyšší řídící pracovníky entity. Proces zlepšování jakosti (tj. v jeho nejvyšší úrovni jde de facto o zvyšování integrální bezpečnosti) vychází z impulsů, které vychází z potřeb zákazníka, respektive občana [29,30]. TQM vychází z předpokladu, že trvalá kvalita (jakost) výrobků a služeb se nedá zajistit příkazy, kontrolou, dílčími programy, organizačními nebo ekonomickými opatřeními, ale cíleným hledáním, měřením a hodnocením příčin toho, proč se produktivita a kvalita nezvyšuje; de facto jde o jistou kulturu bezpečnosti (jinými slovy způsobu aplikace opatření a činností lidí). Pozornost se zaměřuje na procesy probíhající v entitě. Při implementaci TQM se přihlíží na specifika entity, protože z důvodu účinnosti všechna opatření musí odpovídat struktuře entity, tj. musí být místně specifická [19,30].

Navíc od standardizovaných systémů řízení (ISO normy), které jsou na principech TQM založeny, TQM zahrnuje i principy a postoje k řízení měkkých socio-technických systémů, s jednoduchými idealizovanými cíli tak, aby byli pochopené veškerým dotčeným personálem, respektive obyvateli v uvažovaném místě.
Z hlediska bezpečnosti TQM buduje tzv. systémy celkové bezpečnosti (z angličtiny Total Safety Systems, zkráceně TSS). TSS zavádí koncept nulových rizik (angl. Zero Risks), který je základem pro následování strategie nulových defektů (angl. Zero Defects) a dělání věcí tzv. hned napoprvé (angl. Right First Time).

Začleněním specifické prevence do bezpečnosti u socio-technických elementů organizačních systémů zahrnuje porovnávání příspěvků tzv. systému celkové prevence (angl. Total Prevention Systems – TPS), které zahrnují principy nulové poruchy (angl. Zero Breakdown), a systému rozvoje lidí (angl. Human Development System), který je určen ke vzdělávání a tréningu pracovníků k uvedenému principu

„hned napoprvé“ [28]. Uvedené systémy celkové prevence zahrnují například implementaci známé údržby celkového provozu (angl. Total Operation Maintenance) [28] apod.

Celkově (integrálně) bezpečný systém zahrnuje tři základní elementy:

- bezpečnost místa (dispozice, řízení environmentálních aspektů, nouzové postupy, protipožární opatření, zajištění první pomoci, osvětlení, sociální zázemí a jiné),
- bezpečnost procesů (fyzická ostraha, prvky nouzového zastavení, principy „selži bezpečně“, ochrana perimetru),
- bezpečnost lidských zdrojů (bezpečnostní školení, osobní ochranné pomůcky, dohled, zdravotní prohlídky).

EU vydala kontrolní seznam, ve velké míře využívaný především pro inspekce, zahrnující tři výše uvedené oblasti [2]. Systém TQM společně s TSS v mnoha oblastech výrazně přesahuje legislativní požadavky platné v ČR. Pro účely zvyšování bezpečnosti je základním předpokladem představených systémů snižování rizika, pomocí proaktivních programů s neustálým měřením a eliminací již tzv. skoro-nehod (angl. Near-misses). Skoro-nehody jsou události, které na základě současného poznání by obvykle vedly k nehodě nebo havárii, ale v daném případě k žádnému problému nedošlo, např. z důvodu duchapřítomnosti obsluhy [19,21,28]. Současné trendy v oblasti bezpečnostních věd a inženýrství rizika jsou založené na principech inženýrského řízení rizik, a to s uvážením složitosti systémů, která vyplývá z podstaty, vlastností a neurčitostí socio-technických, kyber-fyzických systémů, označovaných jako systémy systémů (z angličtiny zkráceně SoS) [2,19,26,30,31].

2.1.6 Kritická infrastruktura a její bezpečnost

Kritická infrastruktura je z hlediska Směrnice rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu [32] 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 [33] 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. V České republice je kritická infrastruktura složena z infrastruktur rozdělených do následujících devíti oblastí [33]:

1. Dodávky energie (elektrické, plyn, teplo, olej a ropné produkty).
2. Voda (zajištění pitné a užitkové vody, zabezpečení a správa povrchových i podzemních vodních zdrojů, systém odpadních vod).
3. Zásobování potravinami a zemědělství (výroba potravin, péče o potraviny, zemědělská produkce).
4. Zdravotní péče (přednemocniční neodkladná péče, nemocniční péče, ochrana veřejného zdraví, výroba, skladování a distribuce farmaceutických produktů a zdravotních zařízení).
5. Doprava (silniční, železniční, letecká a vodní).
6. Kybernetické, komunikační a informační systémy (pevné a mobilní telekomunikační síťové služby, rádiová komunikace a navigace, televizní a satelitní komunikace, pošta a zásilkové služby, internet a datové služby).
7. Bankovnictví a finanční sektor (správa veřejných financí, bankovnictví, pojištění, kapitálový trh).
8. Záchranný systém (Hasičský záchranný sbor ČR, jednotky požární ochrany, Policie ČR, Armáda ČR, monitoring radiace, předpovědi, varovací systém apod.).
9. Veřejná správa (státní správa a samospráva, sociální zabezpečení a zaměstnanost, statní sociální podpora a sociální pomoc, výkon soudního a vězeňského systému).

Oblast kritické infrastruktury upravuje krizový zákon [34]. Objektem neboli prvkem kritické infrastruktury se rozumí stavba, zařízení, prostředek nebo veřejná infrastruktura, určená podle průřezových a odvětvových kritérií, tj. dle [35]. Z hlediska drážního systému jsou objektem kritické infrastruktury 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 [33].

Ochrana zdraví a majetku lidí je předním zájmem základní funkce státu zakotvené v Ústavě České republiky (zákon č. 1/1993 Sb.). Možné výskyty pohrom mohou ovlivnit nejen správnou funkci prvku kritické infrastruktury, ale taktéž mohou ohrozit zdraví a majetek lidí i životní prostředí. Proto se podle kategorie pohromy, uvedené v předchozím odstavci, provádí příslušná opatření [4,13,33].

2.1.7 Moderní přístupy: All-Hazard-Approach a Defence in Depth

Přístup ***All-Hazard-Approach*** [12] znamená zvažovat při řízení bezpečnosti všechny možné druhy pohrom, tj. jevů, které mohou způsobit škody, ztráty a újmy sledovaným aktivům, tj. lidem i příslušným entitám v daném území [2].

Defence-In-Depth (ochrana do hloubky) je komplexní filozofie zajištění bezpečnosti, která se začala v technologii aplikovat v 80. letech minulého století [27]. V obecné rovině lze tento přístup chápat jako ochranu systému za pomocí opatření ve více vrstvách systému.

Na základě [36] Defence-In-Depth představuje komplexní přístup, který zajišťuje, že lidé i životní prostředí budou ochráněny i při kritických podmínkách v objektu. Zahrnuje všechny činnosti zacílené na bezpečnost objektu i území, ve kterém se objekt nachází, a to počínaje umísťováním, přes navrhování a projektování, výstavbu, konstrukci, uvedení do provozu, provoz a odstavení objektu z provozu. Pro zajištění bezpečného systému systémů se používají systémy bariér a režimová opatření.

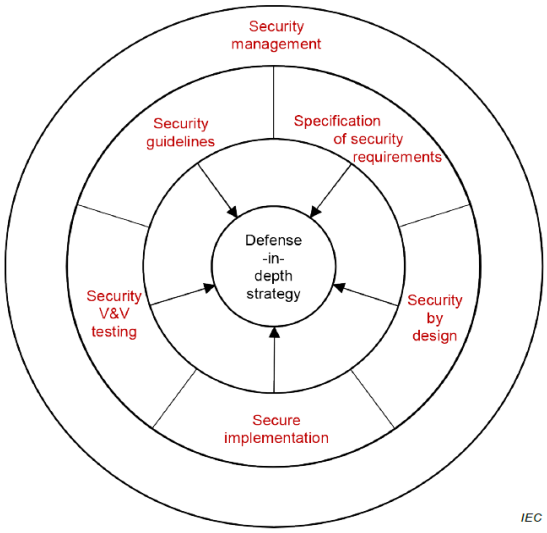
Přístup Defence-In-Depth je známý také v kybernetice a zabezpečení řídicích systémů např. dle [37], obrázek 4.

Obrázek 4 znázorňuje přístup Defence-In-Depth jako strategii pro řízení zabezpečení zahrnující následující oblasti:

- směrnice pro zabezpečení,
- specifikace požadavků na zabezpečení,
- zabezpečení pomocí návrhu (designu),
- zabezpečená implementace,

- verifikace a validace zabezpečení,
- strategie Defence-In-Depth.

Zobecněný vrstvový model pro řízení bezpečnosti podle přístupu Defence-In-Depth, použitý v disertační práci, je popsán dále v odstavci 2.3.4.



Obrázek 4. Strategie Defence-In-Depth dle [37].

2.1.8 Systémy systémů (SoS), projektové a nadprojektové jevy

Systém systémů (SoS) je v oblasti systémového inženýrství [38] definován jako množina nezávislých systémů, integrovaných do většího systému, který poskytuje unikátní vlastnosti. Nezávislé tzv. složkové (angl. constituent) systémy spolupracují na produkci globálního chování, které nemohou sami produkovat. V souladu se zdrojem [39] se klasické pojetí systému a SoS liší především v následujících elementech:

- ***autonomie –*** autonomie je vykonávána složkovými systémy, aby splnila účel globálního systému, tj. SoS,
- ***příslušnost –*** jednotlivé složkové systémy volí příslušnost dle poměru nákladů a přínosů, kvůli naplnění svého vlastního účelu a ve víře v supra-účel SoS; u klasického pojetí systému je příslušnost daná dle jejich povahy a nemůže ji svévolně změnit (např. jako člen jedné rodiny),

- ***konektivita –*** nesčetné možné propojení systémů a jejich částí pro zlepšení schopností SoS,
- ***diverzita*** – vyšší diverzita (rozmanitost) v schopnostech SoS dosažená pomocí autonomie různých složkových systémů, zaujaté příslušnosti a otevřené konektivity,
- ***emergence*** – v pojetí SoS má zvýšena záměrná nepředvídatelnost systému a vytvoření podmínek pro možnost emergence (tj. vzniku) zásadní význam ve smyslu negativním (vznik nepředvídatelných negativních událostí, pohrom) i pozitivním (včasná detekce a eliminace nepříznivého chování systémů).

Element emergence má zásadní vliv pro volbu metod pro práci se systémy, převaha metod exaktních pro klasické systémy, a převaha metod heuristických pro SoS, tj. včetně použití umělé inteligence (angl. Artificial Intelligence – AI), apod.

Pro účely disertační práce chápeme SoS jako množinu otevřených vzájemně propojených systémů [33], dále složených z podsystémů a objektů (komponent) různých vlastností i jejich umístění. Vazby mezi subsystémy a objekty zajišťují potřebné funkce a chování celého SoS [40]. Vzájemné vazby a závislosti, tj. interdependence, jsou dle jejich povahy fyzické, kybernetické, místní a logické [6]. Dále lze interdependence SoS rozdělit na:

- ***žádané:*** zlepšují vlastnosti systémů, zařízení a infrastruktur,
- ***nežádané:***
  a) za normálních a abnormálních podmínek: jsou ošetřené projektem dle požadavků legislativy [41],
  b) za podmínek kritických (***nadprojektových***):
     - vedou ke ztrátám systému,
     - způsobují, že systémy řádně neplní svoje funkce,
     - způsobují, že systémy ohrožují sebe a své okolí.

Při zajištěných jistých podmínek řešeného systému, lze některé situace řešit exaktními metodami. Uvedené podmínky pro zajištění bezpečnosti jsou stanovené v projektu dle jeho životnosti a kritičnosti, v tomto případě hovoříme o ***projektových kritériích.*** V případě, že nastanou nepříznivé jevy, resp. nehody, po kterých nedojde k překročení projektových kritérií, resp. podmínek, jde o tzv. ***projektové***

jevy (nehody). Bezpečnost zasahuje především do oblasti mimo uvedené limity a podmínky systémů, tj. ***nadprojektové jevy***, resp. nehody.

Pojmy projektové (angl. Design Basis Accident) a nadprojektové (angl. Beyond Design Basis Accident) nehody jsou například formálně definované Mezinárodní agenturou pro atomovou energii (IAEA) [42], ovšem jsou běžně používané i v dalších oblastech řízení bezpečnosti technických děl [41].

2.2 Bezpečnost technických děl

Současné poznání ukazuje, že při řešení problémů současného světa je nutno zvažovat systémovou podstatu, jednotlivé entity a skutečnost, že u velkých technických děl jde o složité systémy, jejichž struktura je popsána modelem SoS [19]. Aktiva každé entity jsou: všechny základní veřejné zájmy, (tj. životy, zdraví a bezpečí lidí, majetek, veřejné blaho, životní prostředí, kritické infrastruktury a technologie [2], zájmy spojené s plněním úkolů, ke kterým byla entita zřízena); prosperita (zisk); a soulad entity se státem v místě působení. Poslední vyjmenovaná tři aktiva jsou typická pro soukromé entity, jako např. pro systém provozující železniční dopravu. Pro úplnost je třeba uvést, že aktiva lidského systému jsou strukturní elementy a že vazby a toky energií, hmot, informací a povelů mezi nimi jsou vytvářeny fyzikálními, biologickými, chemickými, společenskými, sociálními či psychickými zákonitostmi, které jsou spojené s hmotnou a energetickou podstatou světa, legislativou, financemi, etickými a morálními pravidly, tj. představují toky v architektuře sledovaného systému [43].

2.2.1 Vztah systému s jeho okolím

V realitě každý systém existuje v rámci nějakého kontextu nebo okolí a ze vztahu mezi systémem a okolím vyplývá, že vlastnosti okolí se odráží ve vlastnostech systému. Proto např. se Bossel [44] zabýval uvedenou skutečností a ukázal základní vlastnosti systému, které souvisí s chováním okolí systému. Tabulka 2 shrnuje současné poznání v předmětné oblasti.

Tabulka 2 Souvislosti mezi chováním systému a stavem okolí; dle [44].

Stav okolí	***Vlastnosti systému reagující na stav okolí***
Normální stav (rovnováha)	Existence
Nedostatek zdrojů	Efektivnost – systém musí být dlouhodobě efektivní, ne nutně účinný, v zajišťování nedostatkových zdrojů z prostředí, na něž působí
Rozmanitost procesů	Volnost akcí – systém musí být schopen různými způsoby zvládat veškeré výzvy a podněty z okolí
Proměnlivost	Bezpečí – systém musí být schopen se ochránit před škodlivými vlivy z okolí
Změny	Přizpůsobivost – systém musí být schopen adaptace na změny
Jiné systémy v okolí	Koexistence – systém musí být schopen změnit své chování tak, aby reagoval na chování ostatních systémů v okolí; tj. nesmí je ohrožovat a ony nesmí ohrožovat jeho

2.2.2 Bezpečnost a rizika technických děl

Bezpečnost v současném pojetí založeném na dokumentu OSN z r. 1994 [9] je soubor opatření a činností, které provádí člověk, aby zajistil své bezpečí a udržitelný rozvoj. V uvedeném pojetí bezpečnost zahrnuje jak funkčnost, tak spolehlivost.

Analýza a syntéza poznatků a zkušeností uvedených v odborných publikacích, shrnutá v knize [6] ukazuje, že bezpečnost drážního systému (v integrálním smyslu) lze naplnit jen tehdy, když se při jejím řízení: zvažují všechna výše uvedená aktiva; používá současné poznání v kontextu teorie systému; a drážní systém provádí své činnosti tak, aby nezpůsobovaly jevy, které by vedly k desintegraci až rozpadu drážního systému, anebo až celého lidského systému, tj. i jejího okolí. Jinými slovy cíl je možné dosáhnout jen tehdy, když technické dílo:

- zná a zvažuje všechna možná rizika v detailech i souvislostech (tzv. All Hazard Approach v představě zpracované pro Evropu v rámci projektu FOCUS [45],
- má správně nastavené řízení rizik.

Řízení rizik složitých systémů není jednoduché, protože jejich chování a stav jsou ovlivněny procesy a jevy, které probíhají uvnitř i vně systému, a navíc jejich dopady se modifikují spletitou sítí vazeb a toků, které jsou uvnitř podsystémů, napříč

podsystémů, napříč celého systému i v okolí. Řízení rizik proto musí být komplexní a jeho priority musí být zaměřeny na bezpečí a udržitelný rozvoj entity [6].

2.2.3 Charakteristika systémů

Ze současného poznání systémů a způsobů jejich ovládání (dle zdrojů [6,17,27] a v pracích v nich citovaných), z vlastního výzkumu v oblasti fyzikálních a geovědních disciplín a ze zkušeností získaných při řešení závažných úkolů spojených s umísťováním, projektováním a provozem důležitých objektů vyplývá, že celistvou charakteristiku každého systému dostaneme, když vytvoříme:

1. Morfologický popis systému, tj. popis souboru prvků systému a vnitřních vazeb mezi prvky.
2. Popis souboru spřažení (angl. Couplings) prvků systému, po kterých probíhají toky energií, hmot, informací, peněz a pokynů (jako lidských instrukcí pro realizaci opatření a činností) mezi prvky buď vždy, nebo jen za určitých okolností. Důležité je, že tato spřažení na jedné straně zajišťují jisté žádoucí procesy v systému, tj. jisté chování a podmínky v systému, a na straně druhé jsou příčinou nežádoucích jevů, mezi které patří např. kaskádovité šíření poruch v systému, vytváření slabých míst systému apod.
3. Popis souboru odezev na dynamické procesy probíhající v systému a v jeho okolí, tj. možné typy chování systému způsobem určitý proces v systému nebo jeho okolí – určitá odezva systému.
4. Popis souboru ovládacích mechanismů, kterými za očekávaných podmínek dosáhneme žádoucí chování systému a při neočekávaných podmínkách (abnormálních a zvláště kritických) zajistíme, aby selhání systému nevedlo k degradaci až rozpadu systému, tj. v případě lidského systému zajistíme za kritických podmínek přežití lidí a kontinuitu důležitých činností v území.

Důkladnou znalostí a pochopení položek, na které jsme výše soustředili pozornost, vytváříme schopnost člověka v oblasti zdokonalování ovládacích mechanismů předmětného systému. Vnitřní vazby v systému řízení technického díla jsou založeny v jeho projektu a v provozních předpisech. Spřažení, soubory odezev na dynamické procesy v technickém díle a jeho okolí i soubory ovládacích

mechanismů, kterými člověk usměrňuje v rámci svých možností chování technického díla, jsou pak určené jak přírodními, tak ekonomickými, technickými, finančními, společenskými a sociálními zákonitostmi, z nichž jen některé jsou kodifikovány platnou legislativou.

Pro podporu žádoucích spřažení, odezev a ovládacích mechanismů byly na základě znalostí a zkušeností vytvořeny jisté specifické nástroje pro podporu řízení [6,22], z nichž nejdůležitější jsou:

- zlatá pravidla bezpečnosti (angl. Golden Rules for Safety),
- kultura bezpečnosti (angl. Safety Culture),
- program na zvyšování bezpečnosti (angl. Safety Performance Indicator Programme),
- indikátory / ukazatelé bezpečnosti (angl. Safety Performance Indicators).

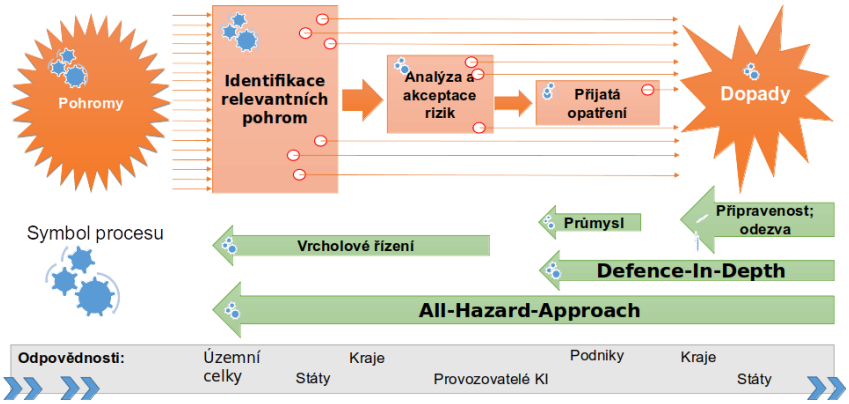
Uvedené nástroje jsou souhrnně popsány v práci [6]. Z pohledu současného poznání do nástrojů patří i systematická aplikace řízení znalostí (angl. Knowledge Management) a přátelského řízení (angl. Friendly Management) lidských zdrojů [6]. V oblasti technologické má dominantní roli vlastník / majitel licence, protože on má znalosti a možnosti pro účinné a kvalitní řízení technologických pohrom, ale celkově má významnější roli veřejná správa, která musí vlastníky donutit k tomu, aby ve veřejném zájmu zajišťovali možnou úroveň bezpečnosti aplikací výše uvedených principů [6,27,46].

2.3 Systémy řízení bezpečnosti (SMS)

Systémy řízení bezpečnosti (dále jen SMS) lze rozdělit do tří dimenzí: vertikální rozdělení dle řešení problému (obrázek 5) [2], horizontální rozdělení dle oblastí působnosti (pro účely předložené práce to je drážní doprava) [20] a třetím je rozdělení dle stupně kritičnosti dané události (řízení za stavu normálních podmínek, v odchylkách od normálního stavu, v abnormálních a kritických podmínkách).

Obrázek 5. Systémy řízení dle úrovně řešení problému [2].

Obrázek 6 znázorňuje proces řízení bezpečnosti dle na různých úrovních jako návazné podprocesy, cílem je zmírnit rizika pohrom a jejich dopady metodami pro řízení rizik a bezpečnosti, které sami o sobě nepokryjí veškeré události a nezajistí totální bezpečnost (znázornění oranžově), proto se zavádí proaktivní přístupy a implementují se opatření (znázorněné zeleně), odpovědnost za danou implementaci je uvedená v šedé části.



Obrázek 6. Proces řízení bezpečnosti dle [20].

Následující odstavce popisují z hlediska integrální bezpečnosti ty nejdůležitější úrovně řízení bezpečnosti, dle zdroje [19,47].

2.3.1 Vrcholové řízení bezpečnosti

Vrcholové řízení bezpečnosti je základním kamenem řízení na úrovni politické a spočívá na identifikaci a analýze rizik mezi různými oborovými odvětvími. Analýza a řízení rizik počínaje v nejvyšší vrstvě na úrovni celého státu umožňuje identifikovat prioritní rizika a chráněná aktiva státu včetně stanovení kritičnosti objektů kritické infrastruktury [6]. Výstup řízení bezpečnosti vyšší vrstvy musí sloužit jako vstup pro

řízení bezpečnosti na nižších úrovních, tj. konkrétního území, kritické infrastruktury a vybrané kritické objekty [26] (tj. strategická a taktická úroveň).

Vrcholové řízení bezpečnosti zahrnuje následující postupy blíže popsané v [6]:

1. Určit seznam relevantních živelných a jiných pohrom.
2. Provést analýzu poznatků a zkušeností, spojených s každou relevantní živelnou či jinou pohromou.
3. Provést hodnocení dopadů každé sledované živelné či jiné.
4. Provést ocenění sledované živelné či jiné pohromy.
5. Regulovat činnosti v dané oblasti pro zmírnění dopadů pohrom.
6. Soustavně ověřovat přijatou metodiku vrcholového řízení bezpečnosti.

Aplikace zásad řízení na drážní systémy je provedena v práci [20].

2.3.2 Řízení bezpečnosti pro konkrétní území

Vrcholové řízení bezpečnosti státu poskytuje vstupy pro řízení bezpečnosti konkrétních území. Aby řízení bezpečnosti bylo efektivní, musí pracovat s integrálním rizikem a aplikovat přístupy All-Hazard-Approach, tj. přístup zvažování všech relevantních pohrom pro danou oblast [26]. Určí se dopady jednotlivých pohrom na aktiva entity, například pomocí metody What/IF. Dále se určí četnosti a provede se klasifikace pohrom [13]. Získáme rozdělení pohrom na relevantní pro konkrétní území, z relevantních pohrom určujeme pohromy specifické a kritické [4,13,19].

Pro veškeré relevantní pohromy se v rámci prevence v projektu a zhotovení aplikují společná opatření, jejichž zásady jsou v legislativě [41].

Pro specifické a kritické pohromy se aplikují kromě prevence i specifická opatření, jejichž aplikace povede ke zmírnění dopadů při odezvě [22], tj. pro provoz se zpracovávají nouzové plány a u kritických pohrom pak i plány kontinuity (pro podniky) a plány krizové (pro území).

Aby bylo možné zmírňovat dopady pohrom, je zapotřebí znát jejich rozsah, velikost a podrobnější popis. Proto se vytváří scénáře dopadů, kterými jsou například: scénáře záplavového území, scénář rozletu úlomků, scénáře šíření požáru, mapa seismických zón, mapa srážek a podobně. Odezva na specifické pohromy se

provádí s využitím standardních finančních i lidských zdrojů, sil a prostředků dle povodňových plánů, havarijních plánů, plánů kontinuity a podobně [2,4,19].
Pro případ výskytu kritické pohromy je nutné vytvořit adekvátní schopnost zvládnout dopady [6]. Jedním z bodů připravenosti je mimo jiné zpracování scénářů odezvy (zásahů), s ohledem na vlastnosti pohromy na daném území. U scénářů odezvy na kritické pohromy nejsou standardní zdroje, síly a prostředky dostatečné, proto se počítá s nadstandardními zdroji, připravují se typové plány, vytváří se finanční zálohy a krizové plány [2,4,19,41].

2.3.3 SMS technických děl zacílený na bezpečnost a zabezpečení

V úvahách, koncepcích, a praxi [6,27] se rozlišuje SMS, který zajišťuje bezpečné technické dílo, jeho bezpečné okolí a bezpečnostní systém (ve smyslu zabezpečení, tj. angl. Security System), tj. systém zajišťující zabezpečené technické dílo. První jmenovaný zahrnuje v sobě druhý, protože obsahuje nejen prvky systému, ale i pravidla pro hierarchicky uspořádané soubory opatření a činností, kterými se zajišťuje jistá úroveň bezpečnosti sledovaného technického díla a jeho okolí a která jsou navázaná na momentální situace, krátkodobé i strategické cíle řízení bezpečnosti. Cíle prvního systému jsou stále proaktivně zvyšovat úroveň bezpečnosti v čase a technickém díle, které má jasný prostorový obsah a ke kterému patří i lidská společnost) tím, že se provádí soustavný monitoring a prognózy, předem se připravují plány akcí na možné situace a ve správném okamžiku se aplikují opatření a činnosti, které rychle stabilizují technické dílo při výskytu pohromy a vedou k růstu bezpečnosti v území a čase. Cílem komplexního SMS území je integrální neboli ucelená či sjednocená bezpečnost s ohledem na chráněná aktiva a udržitelný rozvoj technického díla a jeho okolí.
Komplexní SMS technického díla má nadřazená pravidla, kterými řídí bezpečnost dílčích systémů řízení bezpečnosti v technickém díle, protože bezpečnost technického díla je chápaná jako vlastnost na úrovni celku, přičemž obecně platí, že soubor bezpečných systémů není bezpečný systém [6].
Systém řízení bezpečnosti technického díla (tj. v našem případě systém drážní dopravy) musí dle práce [6] založené na směrnici OECD [46] a konceptu

bezpečnosti OSN 1994 [9], který sleduje jak vlastní chráněná aktiva, tak veřejná chráněná aktiva, zahrnovat šest hlavních procesů (blíže popsaných v [6]) pro:

- tvorbu koncepcí a řízení jejich implementací,
- administrativní postupy,
- technické záležitostí,
- vnější spolupráce,
- nouzovou připravenost a odezvy,
- dokumentace a šetření havárií a skoronehod.

SMS zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v komunitě a jejím okolí. Opírá se o koncepci prevence pohrom či alespoň jejich závažných dopadů, která zahrnuje povinnost zavést a udržovat systém řízení., ve kterém jsou zohledněny dále uvedené aspekty (popsané v [6]):

1. Role a odpovědnosti osob.
2. Plány pro systematické identifikování závažných ohrožení.
3. Plány a postupy pro řízení bezpečnosti všech komponent a funkcí technického díla.
4. Plány na implementaci změn v technickém díle (území, objektech i zařízeních).
5. Plány na identifikaci předvídatelných nouzových situací.
6. Plán pro pravidelné hodnocení souladu s cíli.
7. Plán pro pravidelné hodnocení mechanismů pro vyšetřování a provádění korekčních činností v případě selhání dílčích opatření a činností s cílem dosáhnout stanovené cíle bezpečnosti.
8. Plán na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS.
9. Plán na periodické systematické hodnocení kritérií pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků.

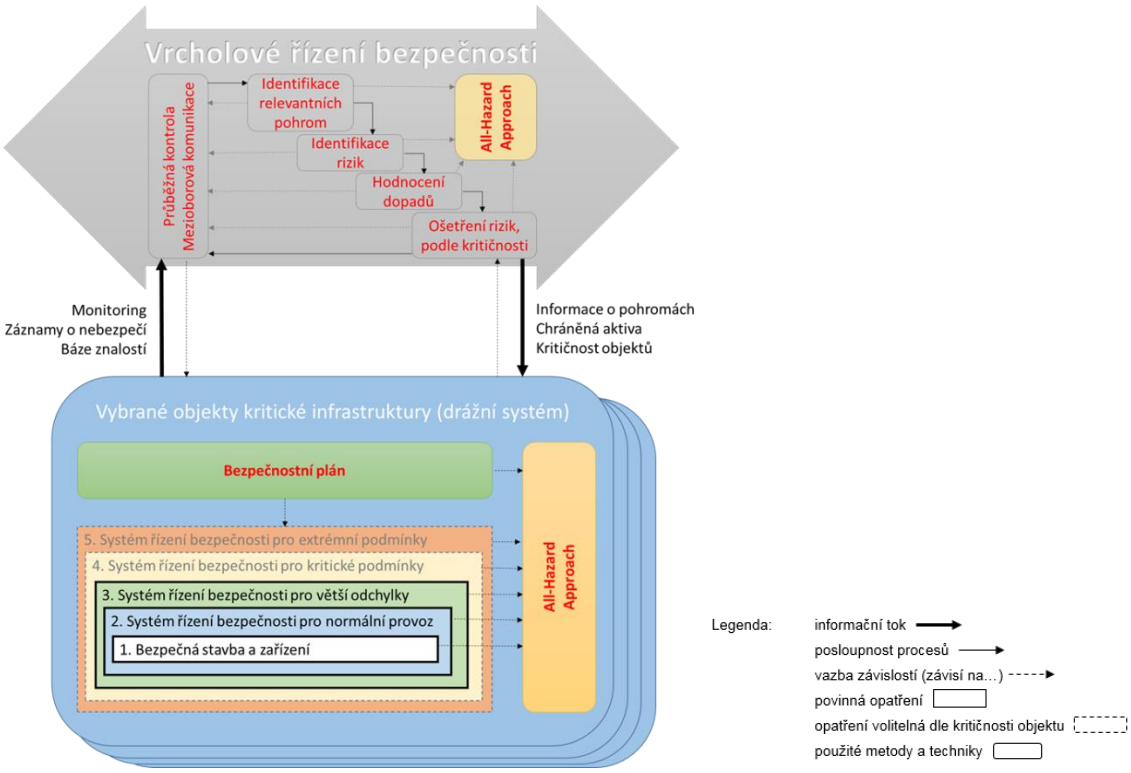
Komplexní SMS technického díla stanovuje obecné principy pro plánování zajištění bezpečnosti technického díla v proměnném světě. Jeho základní principy jsou

určené pro všechny zúčastněné, tj. jak řídící pracovníky a zaměstnance technického díla, tak veřejnou správu, která dává povolení ke zřízení a v zájmu bezpečí lidí i státu musí provádět dohled nad provozem technického díla [6].

2.3.4 SMS pro systémy systémů (SoS)

V moderním pojetí řízení bezpečnosti se pro složité technologické objekty, tedy SoS, používá dvou principů, a to All-Hazards-Approach [26] a zobecněná „ochrana do hloubky“ (Defence-In-Depth) [16,22,25]. Obecný koncept obrany do hloubky pro technologické systémy (objekty, infrastruktury) byl definován v práci [25]. Jedním z výsledků výše uvedené práce je definice pětistupňového modelu řízení bezpečnosti technologického objektu. Obrázek 7 znázorňuje implementaci uvedeného modelu konkrétně pro drážní systém v kontextu s vyššími úrovněmi řízení dle [48].

Při rozlišení míry bezpečnosti objektů a infrastruktur se dle zdroje [25] používá bezpečnostní charakteristika, dle které má objekt jednostupňovou nebo až pětistupňovou ochranu do hloubky, obrázek 7. Jednotlivé systémy řízení bezpečnosti zajišťují aplikaci technických, provozních a organizačních opatření a činnosti, které jsou navrženy tak, aby buď zabránily iniciaci řetězce škodlivých jevů, anebo ho zastavily.



Obrázek 7. Pětistupňový model řízení bezpečnosti SoS [48].

Principy možných opatření pro jednotlivé vrstvy následovné [4,19,22,25,47]:

1. ***Prevence abnormálního provozu a selhání.*** V návrhu, výstavbě a konstrukci inherentně používat principy bezpečného projektu, tj.:
   - All-Hazards-Approach, 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).
2. ***Řízení / ovládání abnormálního provozu a detekce selhání.*** Řídicí systém objektu musí mít základní řídící funkce, alarmy a reakce operátora zpracované tak, aby technologický objekt byl udržen v normálním (stabilním) stavu za normálních podmínek.
3. ***Řízení / ovládání havárií pomocí projektových opatření.*** Technologický 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 odolnost. Předmětné systémy udržují bezpečný provoz i za změny podmínek nebo mají schopnost zajistit normální provoz po aplikaci nápravných opatření (vyčištění, oprava…).

4. ***Řízení / ovládání kritických podmínek včetně prevence dalšího rozvoje havárie a zmírnění dopadů havárie.*** Pro případ, že se vyskytnou kritické podmínky, které způsobí, že dojde ke ztrátě ovládání objektu, musí mít technologický objekt systém opatření pro vnitřní nouzovou odezvu, zmírnění dopadů, a pro návrat do normálního provozu (plán kontinuity a vnitřní nouzový / havarijní plán).
5. ***Zmírnění dopadů havárie vně objektu.*** Pro případ, že dopady ztráty ovládání technologického systému postihnou okolí techno-logického objektu, musí mít technologický systém opatření i pro vnější odezvu, zmírňující opatření pro prevenci ztrát v objektu; a kapacitu pro překonání obtíží.

2.3.5 Řízení bezpečnosti v dopravě

Systémy řízení bezpečnosti v dopravě jsou částečně definovány Evropskými směrnicemi a následně příslušnou legislativou členských zemí. Legislativa je rozdělená pro každou oblast dopravy zvlášť a je velmi stručná nebo v mnoha případech nejasná či nedostatečná [19].

V průmyslu se pro řízení bezpečnosti uplatňují především systémy řízení kvality založené na procesním a projektovém řízení TQM, s implementovaným procesem analýzy rizik, respektive standardu ISO 9001 [49] s rozšířenými požadavky pro kvalitu i bezpečnost výrobků v dané oblasti. Pro elektronické systémy, tj. elektrické / elektronické / programovatelné (E/E/PE) se v průmyslu zavádí mezinárodní standard funkční bezpečnosti IEC 61508 [50]. Uvedené přístupy a standardy systémů řízení jsou pro každou průmyslovou oblast upraveny a doplněny příslušnými standardy uvedenými v následujících odstavcích.

Pouze velmi úzká skupina subjektů zahrnutých do kategorie subjekt kritické infrastruktury je podřízena krizovému zákonu [34] tzn., zavádí alespoň základní principy krizového řízení, má povinnost vypracovat plán krizové připravenosti na

základě krizového plánu dotčené oblasti, který je pravidelně přezkoumáván, a je odpovědná za veškerou součinnost s dalšími subjekty uvedenými v zákoně.

Oblasti řízení bezpečnosti zahrnují také systémy řízení bezpečnosti informací (ISMS) a kybernetické bezpečnosti (angl. Cyber Security). Zde je nutné poznamenat, že se ve skutečnosti jedná o zabezpečení informací a zabezpečení kyberprostoru (od anglického slova Security), ale v českých podmínkách se ujal nepřesný pojem bezpečnost informací. Účelem uvedeného systému je zajistit tzv. důvěrnost, integritu (tj. celistvost) a dostupnost informace v organizaci, resp. kybernetickém prostoru jakéhokoliv systému. Povinnost zavádění ISMS mají pouze některé subjekty definované v zákoně o kybernetické bezpečnosti [51], jedná se o vlastníky či provozovatele kritické informační infrastruktury nebo provozovatele kritické infrastruktury dle zákonem stanovených kritérií. Standardů v této oblasti existuje mnoho, základními jsou normy řady ISO/IEC 27000 [52] pro systémy řízení bezpečnosti založené na systému řízení standardů řady ISO 9001 [32]. ISO norma řady 27000 [52] je uznávaná zmíněným kybernetickým zákonem [51]. Další normou je IEC 62443 [53] pro zabezpečení průmyslové automatizace a řídicích systémů, která obsahuje jak procesně organizační požadavky, tak i technické požadavky na výrobky v průmyslových sítích zvyšující jejich kybernetickou bezpečnost. Dále jsou známé standardy pro hodnocení úrovně zabezpečení produktů v informačních technologií ISO/IEC 15408 [54], z angličtiny Common Criteria (CC). Kromě leteckého průmyslu se v průmyslových oblastech v dopravě informační, resp. kybernetická bezpečnost nezavádí vůbec nebo pouze v dílčích a úzce zaměřených oblastí. V leteckém průmyslu se doporučuje integrace systémů řízení, kde vedle systému řízení bezpečnosti (SMS) je integrován i systém zabezpečení (SeMS) nejen pro plnění požadavků předpisu L17 [55]. V rámci SeMS lze požadavky normy ISO/IEC 27000 uplatnit.

Výše uvedená fakta implikují tvrzení, že jsou současné dopravní systémy zabezpečené z hlediska funkční bezpečnosti, ale nepřipouští, že se mohou vyskytnout i jiné nepředvídatelné události. Například kybernetický útok a další pohromy (i živelní) mohou uvažovaný systém uvést do abnormálních a kritických podmínek, které výrazným způsobem ohrožující své okolí, dle obrázku 2 v podkapitole 2.1.4.

Následující odstavec se, vzhledem k tématu případové studie v disertační práci, zaměřuje pouze na SMS v železniční dopravě. Porovnání přístupů SMS v ostatních oblastech dopravy je uvedeno ve zdrojích [19,47].

2.3.6 SMS v železniční dopravě

V rámci železniční dopravy je základním dokumentem Směrnice o bezpečnosti železnic [56]. Uvedená směrnice vedle SMS zavádí i společné bezpečnostní cíle (angl. Common Safety Targets – CST) a společné bezpečnostní metody (angl. Common Safety Methods – CSM), např. dle [57] při jakékoliv technické, provozní a organizační změně je nutné tuto změnu zdokumentovat, posoudit a odůvodnit její vliv na bezpečnost, tj. ***aplikovat metodu analýzy a řízení rizik***.

Část výše uvedené směrnice vztahující se k SMS [56] byla v ČŘ transponována do Vyhlášky o systému bezpečnosti provozování dráhy a železniční dopravy a postupech při vzniku mimořádných událostí na dráhách [58]. SMS má dle této Vyhlášky povinnost zavádět pouze provozovatel dráhy, s tím, že při tom respektuje pouze systém za normálních podmínek a při tzv. mimořádných událostech. Mimořádné události se ohlašují Drážní inspekci, která události vyšetřuje a je-li potřeba, navrhuje bezpečnostní opatření.

Drážní průmysl není vždy povinen, ale je konkurenčním prostředím stimulován k zavedení drážního standardu IRIS [59], který je integrován do stávajícího systému řízení. IRIS rozšiřuje požadavky systému řízení jakosti (dle ISO 9001 [49]) s důrazem na kvalitu a bezpečnost vyvíjených a instalovaných systémů v jejich celém životním cyklu, tj. mimo jiné implementuje požadavky EN 50126 pro prokázání bezporuchovosti, dostupnosti, udržovatelnosti a bezpečnosti systému (RAMS) [60]. Principy funkční bezpečnosti jsou dále rozšířené normou EN 50129 [61] pro bezpečnostně relevantní systémy (zabezpečovací zařízení) a EN 50128 [62] pro jakýkoliv software aplikovaný na drahách. Uvedené evropské normy jsou založené na funkční bezpečnosti dle IEC 61508 [50]. Bližší informace o požadavcích standardu IRIS a jemu příbuzných norem jsou uvedeny v práci [48].

2.4 Informační systémy a technologie

Informace, informační systémy a technologie zahrnují velmi širokou oblast. Informace jsou dnes vedle materiálních, energetických a finančních zdrojů řazeny k základním faktorům, které určují pokrok, a to nejen technologický, ale také pokrok v ostatních oblastech lidských aktivit [63,64]. Informační toky v systémech vytváří důležitá spojení a spřažení elementů a celých systémů v komplexních technologických objektech [10,25,33,63]. Bez jisté úrovně informace není možné vytvářet ani spravovat procesy v technických dílech a v lidské společnosti [16].

Disertační práce se zaměřuje především na systém řízení provozu pražského metra a informační podporu pro zvyšování bezpečnosti za použití informačních technologií, tj. zvyšování informačního výkonu, který na základě míry znalosti zajistí správné a včasné rozhodnutí, které je důležité především za abnormálních a kritických podmínek. Tímto informační výkon zvyšuje bezpečnost systému. Proto následující odstavce popisují využití informačních systémů, teorii vzniku informace, parametry použitých technologií, míru informace, informační výkon a zabezpečení informačních systémů.

Bližší popis problematiky informačních systémů a technologií v oblasti řízení bezpečnosti technických děl je uveden v pracích [10,16,65].

2.4.1 Využití informačních systémů na drahách

Informační technologie a systémy jsou nástroje pro řízení, anebo v případě automatizovaných provozů, sami řídí kvalitativní i bezpečnostní parametry. Informační systémy a technologie jsou nedílnou součástí drážních systémů.

Tabulka 3 uvádí příklady využití informačních systémů v různých oblastech drážní dopravy, do které spadá i provoz metra na který se disertační práce zaměřuje, dle [65].

Tabulka 3 Příklady využití informačních systémů na drahách [65].

Oblast použití	**Použití pro**
Řízení a plánování (management)	vyhodnocování dat z provozu, tvorbu jízdních řádů rozpis služeb zaměstnanců

	rozhodovací, ekonomické, účetní činnosti komunikace se záchrannými složkami a s policií
Řízení provozu	centrální dohled a řízení, dispečerské činnosti staniční a traťové technologie sběr a zpracování dat na trase vlaků komunikace mezi stacionárními a vlakovými systémy zabezpečovací zařízení
Provoz vlaku	řízení vlaku, vlakový počítač, datové přenosy mezi vlakovými zařízeními sledování a řízení vlakových zařízení (dveře, klimatizace, vlakový rozhlas, energetická zařízení) rozhraní technik – strojvedoucí
Cestující:	informační tabule, systémy odbavení cestujících zábavná zařízení ve vlaku, Wi-Fi navigační systémy – směrové tabule, systémy pro hendikepované

2.4.2 Proces vzniku informace

Vznik informace je podmíněn sledováním jistých vlastností pozorovaného objektu nebo společných vlastností skupiny objektů. Každý informační systém sleduje vlastnosti entit použitím určitého jazyka, což slouží k vytvoření informace o pozorovaném objektu [64,65]. Podle způsobu interpretace takto získaných informací se rozlišují typy informačních systémů [64,65]:

- syntaktické informační systémy, které vytváří množinu informačních obrazů stavových veličin pozorovaného objektu,
- procesní informační systémy, které reprezentují množinu procesů.

Akční informační systémy pak zpětnou vazbou ovlivňují původní pozorovaný objekt [64],[65]. Pro účely předložené práce a v rámci řízení drážní dopravy se uplatňují především akční procesní informační systémy.

Proces vzniku informace, informačního systému, proces vzniku nového objektu nebo modifikace objektu je původního složen z následujících podprocesů, respektive množiny vazeb a jejich relací [64], které jsou popsané Tabulka 4.

Tabulka 4 Proces vzniku informace a informační technologie [65].

	Podproces vzniku informace / množiny objektů	***Dotčené abstraktní uzly***	***Použité informační technologie***	***Vstupy procesu***	***Výstupy procesu***
1	Identifikace objektu	Objekt, pozorovatel	Fyzické receptory (senzory, čidla)	Pozorované stavové (fyzické) veličiny objektu	Signály
2	Pozorování	Pozorovatel, jazyk (syntaxe)	Vzorkování, kvantování, kódování/dekódování	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, nebo příjemce), množina informací (řádek 6)	Ontologie, jazyk	Data	Informace
5	Vazby funkcí a strukturálního uspořádání objektu, ověření celistvosti (integrity)	Množina informací (řádek 6), objekt	Akční člen systému, akční informační systém	Objektu, informace	Správnost informace, změna objektu
6	Množina informací v množině informačních systémů	Informační systémy	Informační systémy	Informace	Informace
7	Proces interpretace	množina informací (řádek 6), nový objekt	Signalizace a technologie reprezentace informace, umělá inteligence	Informace	Obraz objektu, nový objekt

Proces vzniku informačního obrazu lze také vyjádřit pomocí Freggeho funkcionálního konceptu vzniku informačního obrazu [64], který je složen z množin:

- O_i – množina stavových veličin na objektu,
- P_i – množina stavů (pozorovatelů),
- Φ_i – množina syntaktických řetězců (tok dat),
- I_i – množiny informačních obrazů stavových veličin,

a jejich vzájemných vztahů popsaných v práci [64], které určují kvalitu procesu vzniku informačního obrazu:

- OP – identifikace,
- PO – invazita (nebezpečí narušení integrity stavových veličin na objektu),
- PΦ – projekce v množině symbolů a syntaktických řetězců,
- ΦP – korekce a identifikace neurčitelnosti,
- ΦI – interpretace, vznik informace,
- IΦ – reflexe jazykových konstruktů,
- IO – relace funkčních a strukturální uspořádání,
- OI – verifikace integrity.

Z tabulky 4 a dle zdroje [64] lze odvodit následující definice:

- ***data*** – neinterpretované údaje o stavu objektu,
- ***informace*** – interpretovaná data, údaje, signály vedoucí ke změně uspořádanosti v systémech reálného světa či vědomí.

2.4.3 Kvalitativní vlastnosti informačních systémů a technologií

Kvalitativní vlastnosti informačních systémů a technologií lze ovlivňovat vhodným nastavením jejich parametrů, kterými jsou např. množství informace dané množstvím možných zpráv omezených počtem znaků, parametry přenosové matice definované vzorcem (11) níže, která určuje schopnost interpretace a filtrace, komunikativnost systému a propustnost informací [65].

Pro praxi je důležité ocenit „velikost informace“ [65]. Míru informace dle [64] charakterizujeme nejčastěji Hartleyovou mírou informace pro binární systém symbolů (tj. pro většinu současných kyber-fyzických systémů). Vyjadřujeme ji vztahem:

$$\boldsymbol{I} = \frac{\mathbf{1}}{\boldsymbol{ln}(\mathbf{2})} \cdot \boldsymbol{ln}(\boldsymbol{N}) \,, \tag{8}$$

ve kterém ***N*** reprezentuje počet možných zpráv (údajů):

$$\boldsymbol{N} = \boldsymbol{S}^{\boldsymbol{n}} \,, \tag{9}$$

ve kterém ***S*** je počet znaků v abecedě ***A (A1,A2,...AS)*** a ***n*** je počet prvků v množině znaků.

Procesní informační systémy charakterizujeme dle [64] grafy přiřazenými relacím:

$$\boldsymbol{I_i} \sim \boldsymbol{F}[\boldsymbol{P}(\boldsymbol{t}), \boldsymbol{\Phi}(\boldsymbol{t})], \tag{10}$$

ve kterých $\boldsymbol{I_i}$=1,2..n je informační obraz stavových veličin, množina stavů ***P*** a syntaktických řetězců (informačních toků) $\boldsymbol{\phi}$ v čase ***t***.

Předmětné přiřazení umožňuje strukturální interpretaci složitých informačních systémů, hodnocení zpětných vazeb a kvalitu převozu a zpracování informace v dílčích informačních systémech [64] a jeho informační segment vychází z maticového vyjádření [65]:

$$\underbrace{\begin{pmatrix} \boldsymbol{I_2} \\ \boldsymbol{\Phi_2} \end{pmatrix} \approx \begin{pmatrix} \boldsymbol{t_a t_b} \\ \boldsymbol{t_c t_d} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{I_1} \\ \boldsymbol{\Phi_1} \end{pmatrix}}_{[\check{T}_i]}, \tag{11}$$

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

V reálném systému ze vztahu (10) vyplývá, že informace nebo množina informací $\boldsymbol{I_i}$ je propojena s množinou stavů sytému a informačních toků v čase. Informační segment ze vztahu (11) můžeme přiřadit například systému sběru dat, kde ***I1*** jsou vstupní (počáteční) informace, $\boldsymbol{\phi_1}$ vstupní informační tok a na druhé straně na výstupu daného systému ***I2*** jako vstupní informace a přenesený informační tok $\boldsymbol{\phi_2}$ [65]. Parametry t lze získat jak kvantitativní, tak i kvalitativním způsobem [63,65] a v předmětném příkladu dle zdroje [64] představují:

$\boldsymbol{t_a}$ – schopnost interpretace (pro ta < 1 má systém velmi malou znalost a schopnost interpretace, pro $\boldsymbol{t_a}$=1 má schopnost interpretace vlastností objektu v informačním systému, pro $\boldsymbol{t_a > 1}$ se jedná o expertní systém se schopností reprezentace vlastních informací o objektu na základě získaných údajů a dat),

t_b – schopnost filtrace (v případě $t_b < 1$ systém na svém výstupu interpretuje menší množství informací než které získá na jeho vstupním informačním toku, pro $t_b > 1$ naopak),

t_c – komunikativnost (schopnost poskytnout výstupní informační tok na základě vstupních informací),

t_d – propustnost informačního systému (schopnost převést vstupní informační tok na jeho výstupní informační tok, v případě redundance je td mnohem větší než 1).

2.4.4 Informační výkon a jeho vztah k bezpečnosti

Pro zajištění bezpečnosti systému systémů je důležité vytvářet taková spřažení mezi systémy, které poskytují vysokou úroveň kvality propojení, tj. kvalitativních parametrů systémů [65], kterými jsou dle [25,63]:

- bezpečnost vystupující na úrovni systému systémů,
- celistvost (integrita) opatření,
- spolehlivost systému systémů,
- kvalita aktivních a pasivních opatření zvyšujících bezpečnost jednotlivých systémů,
- dostupnost určitého systému či zařízení vždy v případě potřeby,
- kontinuita procesu aplikace opatření,
- přesnost provádění opatření.

Uvedené systémové parametry jsou přímo závislé na efektivnosti informačních systémů, které zajišťují požadovanou správnost a včasnost informace a v případě akčních informačních systémů také rychlost správného rozhodnutí. Úroveň efektivnosti informačního systému se vyjadřuje pomocí veličiny informačního výkonu [63-65]:

$$\boldsymbol{P_i(t) = I_i(t) * \Phi_i(t)}, \tag{12}$$

kde $P_i(t)$ je okamžitý informační výkon [63-65]. Informační výkon P vyjadřuje obsah přenesené dekódované zprávy I v informačním toku Φ. Informační výkon je také roven velikosti míry odstranění nejistoty E znalosti (tj. z fyziky množství práce) na jednotku času t [64]:

$$\boldsymbol{P = I * \Phi = \frac{E}{t}.} \quad (13)$$

Pro složité (komplexní) systémy, kvůli nehomogenitě informačních typů (množství, obsahu, správnosti, validity informací), je obtížné informační výkon jasně kvantifikovat. Kvůli výše uvedenému je nutné informační výkon neustále zlepšovat tak, aby byla zajištěna co nejvyšší míra kvality prováděné funkce řídicího systému [63-65]. Pro zvyšování informačního výkonu, a minimalizování zdrojů nutných pro tvorbu předmětných systémů, se v praxi využívá řada metod, kterými jsou například [63-65]:

- COBIT pro audit informačních systémů z hlediska vrcholového řízení [66],
- ITIL pro správu informačních systémů a služeb,
- refaktoring, tj. změny SW systému, které zlepšují jeho interní strukturu a využívání zdrojů, ale neovlivňují jeho vnější funkční chování [64].

Pro zajištění bezpečnosti řídicích systému je proto důležité provozovat takové informační systémy, které poskytují co nejrychlejší a správné rozhodnutí, což úzce souvisí s informačním výkonem [64].

Pravděpodobnost správného výběru variantního řešení z množiny řešení a pravděpodobnost správného rozhodnutí v provozu řídicího systému, tj. PCD (Probability of Proper Decision), je dána funkcí závislé na úrovně znalosti funkce „k“ a informačního toku v čase „$\boldsymbol{\Phi(t)}$“ [63-65]:

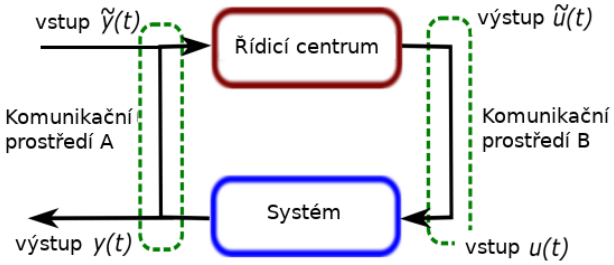
$$\boldsymbol{CD = F[\Phi(t), k].} \quad (14)$$

Z uvedeného vyplývá, že řídicí systémy, které se opírají o vyšší úroveň znalostí, jsou schopné rychlejšího správného rozhodnutí při menší zátěží, tj. rozhodují rychleji [65].

Správně zvolené parametry informačních technologií a systémů zajišťují velikost jejich informačního výkonu, tj. kvalitu informace umožňující efektivní reakci systému na případné nežádoucí stavy. Tímto zlepšují bezpečnost drah, a to nejen v normálních podmínkách, ale i v abnormálních a zejména kritických podmínkách [63,65].

2.4.5 Kvalita přenosového systému

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 4). Uvažujme proto řídicí systém se zpětnou vazbou vyjádřený obrázkem 8 v souladu s [10,67,68].



Obrázek 8. Vazby řídicího systému v kybernetickém systému dle [68].

Kvalita funkcionality uvedeného kybernetického systému je tedy ovlivněna dvěma základními faktory [10]:

- 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 [69] a Bayesovu teorii (podmíněnou teorii pravděpodobnosti) [10,23].

Obrázek 9. Gaussův přenosový kanál [69].

Pro komunikační kanál bez paměti (bez ohledu na výstup v čase menším, než je bod t) dle [10] platí:

$$\boldsymbol{p}\big(\boldsymbol{y}(\boldsymbol{t}) \vee \boldsymbol{x}(\boldsymbol{t})\big). \tag{15}$$

Pro komunikační kanál s pamětí (např. kanál se zpětnou vazbou), s daty do času ***M***, dle [10] platí:

$$\boldsymbol{p}\big(\boldsymbol{y}(\boldsymbol{t}) \vee \boldsymbol{y}(\boldsymbol{t}-\boldsymbol{1}), \boldsymbol{y}(\boldsymbol{t}-\boldsymbol{2}),\ldots, \boldsymbol{y}(\boldsymbol{t}-\boldsymbol{M}), \boldsymbol{x}(\boldsymbol{t})\big). \quad (16)$$

Pro kybernetický systém popsaný na obrázku 8 s parametry $\boldsymbol{\Theta} = \{\boldsymbol{\theta}, \boldsymbol{\theta_2},\ldots, \boldsymbol{\theta_N}\}$ byly v [10] odvolené následující vztahy:

- systém:

$$\boldsymbol{p}(\boldsymbol{y}(\boldsymbol{t}) \vee \boldsymbol{y}(\boldsymbol{t}-\boldsymbol{1}),\ldots, \boldsymbol{y}(\boldsymbol{t}-\boldsymbol{M}), \boldsymbol{u}(\boldsymbol{t}),\ldots, \boldsymbol{u}(\boldsymbol{t}-\boldsymbol{M}), \boldsymbol{\Theta}), \quad (17)$$

- řídicí centrum:

$$\boldsymbol{p}\big(\boldsymbol{u}(\boldsymbol{t}) \vee \boldsymbol{y}(\boldsymbol{t}-\boldsymbol{1}),\ldots, \boldsymbol{y}(\boldsymbol{t}-\boldsymbol{M}), \boldsymbol{u}(\boldsymbol{t}-\boldsymbol{1}),\ldots, \boldsymbol{u}(\boldsymbol{t}-\boldsymbol{M})\big), \quad (18)$$

- komunikační prostředí A:

$$\boldsymbol{p}\big(\boldsymbol{y}(\boldsymbol{t}) \vee \boldsymbol{y}(\boldsymbol{t})\big), \boldsymbol{p}\big(\boldsymbol{y}(\boldsymbol{t}) \vee \boldsymbol{y}(\boldsymbol{t})\big), \quad (19)$$

- komunikační prostředí B:

$$\boldsymbol{p}\big(\boldsymbol{u}(\boldsymbol{t}) \vee \boldsymbol{u}(\boldsymbol{t})\big), \boldsymbol{p}\big(\boldsymbol{u}(\boldsymbol{t}) \vee \boldsymbol{u}(\boldsymbol{t})\big). \quad (20)$$

2.4.6 Zabezpečení kyber-fyzických systémů

Paralelně ke zvyšování informačního výkonu se v praxi, a zejména v případě kritické infrastruktury, zvyšují nároky také na bezpečnost a zabezpečení. Bezpečnost kyber-fyzických systémů spočívá v zabezpečení informací systému tak, aby mohl řízený systém vykonávat své funkce bezpečně, tj. aby svými poruchami neohrozil sám sebe ani své okolí. Proces zajištění bezpečnosti informací (resp. Jejich zabezpečení) spočívá v ochraně důležitých aktiv kybernetického (informačního) systému tak, aby byla pro důležité informace zajištěna požadovaná úroveň dostupnosti, integrity a důvěrnosti (z angličtiny známé jako CIA – Confidentiality, Integrity, Availability) [52,65]. Na rozdíl od systémového pojetí uvedeného v předchozí kapitole, z hlediska informačních technologií zajištění CIA dle [52] znamená zajištění:

- důvěrnosti – informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům,
- integrity – informace je úplná a přesná,
- dostupnosti – přístupnost a použitelnost informace vždy na žádost oprávněné entity.

Dostupnost a integritu lze vyjádřit například pomocí pravděpodobnostních parametrů ve vztazích (15) až (20) uvedených výše.

Důvěrnost v sobě zahrnuje další atributy a metody pro své zajištění. Často jsou předmětné metody v protikladu se zajištěním dostupnosti a integrity, protože se zajištěním důvěrnosti zvyšujeme například časové nároky na kódování a dekódování, přenos, autentizaci a podobně [52,65]. U procesních informačních systémů v dopravě fungujících v reálném čase, na rozdíl od jiných informačních systémů, převládají především požadavky na dostupnost a integritu, kdežto důvěrnost nemá tak velkou prioritu [52,65].

Pro zajištění kvality, informačního výkonu a bezpečnosti kybernetických systémů se aplikují přístupy procesního a projektového řízení typu TQM [8], ze kterých vychází výše uvedené metodiky i mezinárodní a evropské standardy pro systémy řízení [10,63,65]. Účelem předmětných systémů řízení je najít ekonomicky efektivní procesy zajišťující jistou míru kvality a bezpečnosti kyber-fyzických systémů, a to především ve fázi jejich návrhu, analýzy, vývoje, provozu i obnovy a likvidaci.

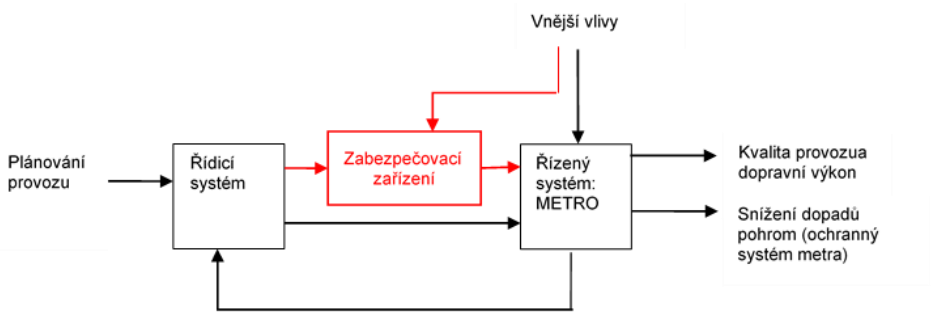
Každý systém pracuje správně pouze za jistých předpokladů, tj. okolních podmínek. Proto musí mít kyber-fyzické systémy stanovené jisté limity a podmínky, které podmiňují jejich kvalitativní parametry (tj. bezpečnost, spolehlivost, dostupnost, celistvost, kontinuita a přesnost) [22,41].

Návrh procesního modelu pro zabezpečení kyber-fyzických systémů je uveden například ve zdrojích [10,63,65,70,71].

3 Data o provoz metra v Praze a jeho řídicích systémů

Pražské metro je velký komplexní, tzn. velmi složitý, systém. Každý složitější systém se skládá z několika subsystémů, vazeb a toků mezi nimi. Subsystémy lze dělit z hlediska řízení na řízené a řídicí. Další oblastí jsou systémy zabezpečovací, které plní bezpečnostní funkce, tj. zmírňují rizika, anebo plní důležitou funkci, jejíž výpadek nebo špatné provedení vede k zvýšení rizika nebo přímo k nehodě [4]. Systém pražského metra lze obecně rozdělit na samostatné provozní subsystémy (stanice, vlaky, infrastruktura), řídicí systémy (vozové počítače, dispečerská ovládací centra, sdělovací technika) a systémy zabezpečovací, které zmírňují dopady při realizace rizik (zabezpečovací zařízení, návěstidla, automatická stavědla).

Obrázek 10 popisuje vztahy mezi řídicími, zabezpečovacími a řízenými systémy. Vnější vlivy přímo ovlivňují systémy a mohou způsobit vnitřní chyby systému, které mohou vést k nebezpečným událostem. Z těchto důvodů se mezi řídicí a řízené systémy instalují systémy zabezpečovací, plnící bezpečnostně relevantní funkce, které využívají vstupů řídicích systémů nebo identifikují nepřijatelné poruchy systému či nepřijatelné vnější vlivy a vykonají svojí funkci tak, aby řízený systém uvedli do bezpečného stavu, tj. stavu v které neohrozí sebe ani své okolí.



Obrázek 10. Schéma řízení systému pražského metra [4].

Systém řízení metra, tak jako i jiné systémy řízení městské kolejové dopravy, jsou systémem distribuovaným. ***Distribuované systémy*** jsou složeny ze subsystémů (uzlů), které vykonávají dané funkce samostatně bez vazby na druhé, ale jejich propojením lze plnit jiné funkce na vyšších úrovních. Subsystémy distribuovaných

systémů tedy vykonávají některé funkce samostatně a jiné funkce až po propojení více subsystémů (uzlů), čímž dostaneme komplexní distribuovaný systém se vzájemnými závislostmi [4].

Bez ohledu na vykonávanou funkci, lze subsystémy metra dále rozdělit do kategorií:

- stacionární systémy – traťové, staniční a dispečerské,
- mobilní systémy – vlaky a jejich zařízení.

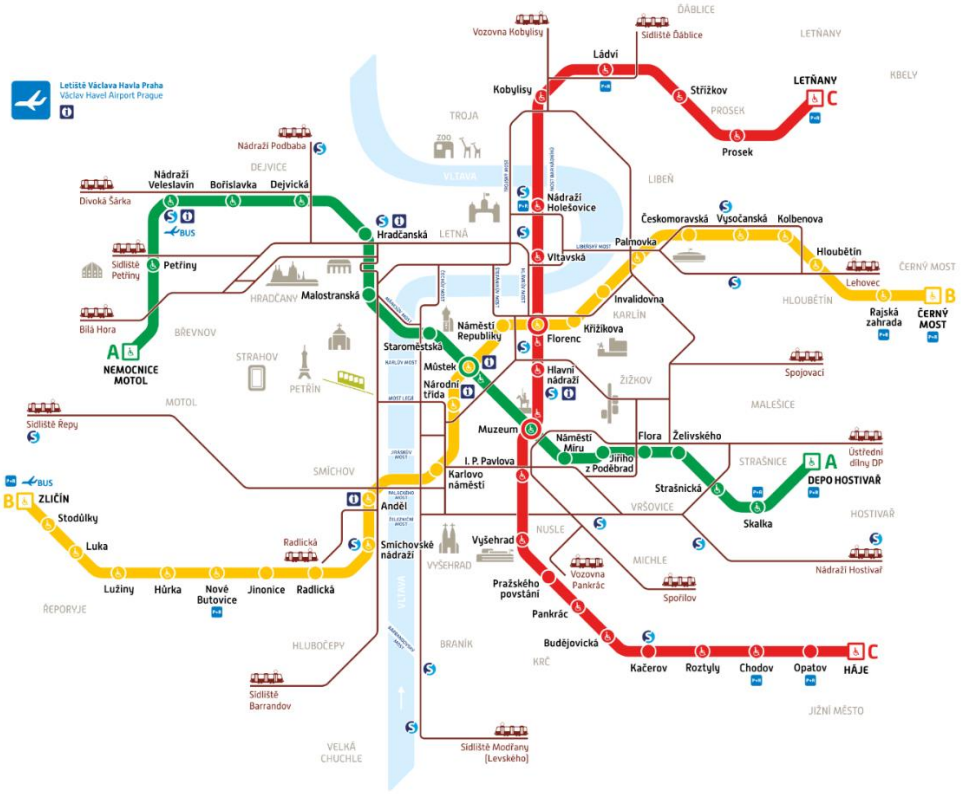
Dále uvedený popis pražského metra vychází z práce [4].

3.1 Pražské metro jako řízený systém

Systém řízení pražského metra plní dvě základní funkce – dopravní a ochrannou. Ochranná funkce snižuje dopady pohrom. Dopravní funkce je řízena ze střediska plánování městské dopravy, ze kterého vychází požadavky v podobě jízdních řádů a požadavků na kvalitu provozu. Uvedené požadavky jsou plněny řízenými systémy, tj. infrastrukturou (dopravními cestami a stanicemi), dopravními prostředky a návaznými pomocnými systémy.

Síť metra tvoří páteř celého systému MHD v Praze. Cestující mohou využívat 61 stanic na třech linkách A, B, a C, jejichž délka činí cca 65 km [4,11]. Doprava je vedena na trati umístěné v tunelu, odděleného od okolního prostředí. Pouze v některých úsecích v oblasti depa je provoz vlaku ve venkovním prostoru. Trať je fyzicky oddělená od okolní infrastruktury a neumožňuje přímé napojení jiných dopravních prostředků městské a příměstské dopravy (vlaky příměstské dráhy).

Vozový park čítá dle zdroje [11] cca 730 vozidel, rozmístěných ve 3 depech: Kačerov, Zličín a Hostivař. V pražském metru se používají dva základní typy vozů spojovaných do pětivozových souprav. Vozy typu M1 zajišťují provoz na lince C a jsou vypravovány z depa Kačerov. Druhý používaný typ, zajišťující provoz linek A B, nese označení 81-71M a jedná se o vozy vzniklé rekonstrukcí starších sovětských vozů typu 81-71 [4,11]. Rozložení tras metra je znázorněno v mapě na obrázku 11.



Obrázek 11. Metro Praha – mapa linek [11].

Technologie řízeného systému tvoří samostatné jednotky, které zajišťují hlavní nebo podpůrné funkce provozu. Předmětné jednotky jsou ovládané (řízené) z místa na ovládacím pultu jednotky (tzv. místní ovládání) nebo ze vzdáleného, centralizovaného ovládacího střediska. Zmíněná střediska jsou buď umístěna v technologických místnostech stanic, nebo na centrálním dispečinku metra. Z výše uvedeného je patrné, že do technologické části patří řídící a zabezpečovací systémy metra, ale pro účely předložené práce jsou řídicí a zabezpečovací systémy rozděleny do zvláštních kategorií [4]. Technologické systémy metra dle [4,72] zahrnují:

- ***energetická zařízení:***
  - měnírny a distribuční transformovny (trasy stanice metra jsou napájeny několika napájecími zdroji 22 kV, každá stanice má navíc svůj záložní zdroj UPS pro případ výpadku elektrické energie, zabezpečovací a řídicí systémy mají také vlastní nezávislé zdroje),

- ***zabezpečovací zařízení*** (staniční, traťové a jejich napájení),
- ***sdělovací zařízení:***
  - sdělovací kabely,
  - VKV spojení s vlaky,
  - zařízení pro automatické odbavování cestujících,
  - zařízení průmyslové televize, telefonní zřízení, rozhlasové zařízení,
  - hodinové zařízení, elektrickou požární signalizaci,
  - elektrickou zabezpečovací signalizaci,
- ***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,
- ***ASDŘ – automatizovaný systém dálkového řízení,***
- ***mobilní stroje a zařízení:***
  - vozový park,
  - zařízení a prostředky pro čištění odpadu, která 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.

3.2 Zabezpečovací zařízení

Zabezpečovací zařízení v drážním provozu, konkrétně v provozu metra zajišťují bezpečný provoz vlaků na trati. Jejich hlavním úkolem je snížit realizace rizik spojených s nepřiměřenou rychlostí vlaku, špatným nastavením jízdní cesty (obrana

proti střetu vlaků) a podobně. Zabezpečovací zařízení se dělí do tří základních skupin [4]:

- staniční zabezpečovací zařízení (SZZ),
- traťová zabezpečovací zařízení,
- vlaková zabezpečovací zařízení (VZZ).

Účelem ***staničních zabezpečovacích zařízení*** je zabezpečení vlakových jízdních cest tak, aby se zabránilo střetu vlaků, tj. aby se zajistil bezpečný průjezd navolenou jízdní cestou. V pražském metru se provozuje reléové zabezpečovací zařízení AŽD 71 přizpůsobené pro provoz metra. V nových stanicích a ve vybraných stanicích metra s kolejovým větvením se provozuje elektronické zařízení (SZZ) typu ESA 11 M s napojením na reléová zařízení. Ve vybrané typové stanici je instalováno zařízení ESA 11 M, které se ovládá buď místně z ovládacího PC zařízení, nouzově z nouzového panelu, vzdáleně na zařízení ASDŘ-D ve stanici pracovníkem SPT (samostatný provozní technik) nebo pomocí systému ASDŘ-D na pracovišti vlakového dispečera z centrálního dispečinku. Staniční nebo traťové zabezpečovací zařízení se také označuje angl. Interlocking [4].

Traťové zabezpečovací zařízení zabezpečuje jízdu následných vlaků a vylučuje jízdu protisměrných vlaků na jedné koleji. V případě pražského metra provozované reléové zařízení AŽD 71 a ESA 11 M [4].

Vlaková zabezpečovací zařízení zabezpečuje příjem návěstních znaků hlavních návěstidel a návěstidel autobloku na vlak a samočinné zabrzdění vlaku, jestliže strojvedoucí nereaguje na návěst nařizující snížení rychlosti nebo zastavení. V mezinárodním pojetí jsou VZZ součástí systému ATC (Automatic Train Control), která se dělí na části ATP (Automatic Train Protection) a ATO (Automatic Train Operation) [4,71,73]. Systém ATP je umístněný ve stanici a na trati, který zasílá řídicí zprávy do mobilní části ATP na vlaku. Vlak příslušná data přijímá a pomocí jednotky ATP zpracovává informace, vyhodnocuje je a provádí příslušné operace. Mobilní jednotka ATP spolupracuje s jednotkou ATO, která ovládá jízdu vlaku, zajišťuje tzv. automatické vedení vlaku podle režimu, na který je režim jízdy vlaku nastaven. V plně automatickém režimu, jednotka ATO ovládá rozjezdy a plynulou jízdu. Často jednotka ATO vykonává i běžné funkcemi vlaku, jako je automatické

hlášení, otevírání a zavírání dveří a podobně. V případě manuálního provozu metra, systém provádí pouze bezpečnostní funkce, kterými jsou například hlídání maximální povolené rychlosti (udaní jízdním profilem, snížené strojvedoucím nebo vzdáleně jiným pracovníkem skrze systém ATP a podobně). Dalšími bezpečnostními funkcemi systému je například povolení průjezdu vlaku stanicí, povolení odjezdu vlaku ze stanice a rušení příkazů. Může sloužit také k přenášení zpráv do vlaku s informací o čísle vlaku nebo dokonce i s informacemi o jízdních řádech a podobně [4,71,73]. V pražském metru se provozují tři systémy VZZ, tj. zařízení LZA, ARS a zařízení MATRA [4].

3.3 Řídicí systém metra a UGTMS

Řídicí systémy pražského metra nesou název ASDŘ, což znamená automatizovaný systém dopravního řízení. Z hlediska evropských norem se nejedná o zcela přesný název, ale je již v provozu pražského metra řadu let zaveden. Dispečerská pracoviště jsou umístěna na následujících stanovištích pro každou trasu metra A, B a C zvlášť [4]:

- ASDŘ-D vlakového dispečera (pro řízení provozu),
- ASDŘ-E energetický dispečer,
- ASDŘ-T technologický dispečink,
- ASDŘ-O systém osvětlení,
- dispečink sdělovací a zabezpečovací,
- dispečink hasičů,
- dispečink depa se správou vozového parku.

Z hlediska řízení provozu je důležitý systém ASDŘ-D, které slouží k zajištění automatických ovládání některých funkcí technologií a zabezpečovacích zařízení. Například pro SZZ systém ASDŘ-D provádí automatické stavění jízdních cest, to znamená, že na základě zvoleného začátku a konce cesty systém ASDŘ-D vygeneruje sled příkazů pro postavení jízdní cesty [4].

Další funkcí ASDŘ-D jsou vzdálená ovládání technologií a zabezpečovacích zařízení, zde jde o bezpečnostně relevantní příkazy, které plní určité bezpečnostní funkce, protože chybné provedení procesu může zapříčinit nehodu. Například:

- chybná volba rychlostního stupně vlaku nebo neoprávněný či neprovedený příkaz STOP může způsobit nehodu, buď srážku vlaku s osobou anebo vykolejení a podobně,
- špatné hlášení cestujícím ve stanici v případě požáru nebo jiných mimořádných událostí může způsobit paniku, zranění či ztráty na životech, tj. ovlivnit bezpečnost.

V případě budoucího rozvoje metra a požadavku na automatizovaný provoz budou požadavky na bezpečnostní funkce systému ASDŘ vzrůstat, jak je vidět z funkcí řídicích systému dopravy dle evropského standardu EN 62290 [74], popsaného dále.

Systémy pro řízení městské a příměstské dráhy (angl. Urban Guided Transport Management and Command/Control System – UGTMS) jsou definovány normou EN 62290 [74]. Norma je rozdělena do tří částí. První část definuje stupně automatizace řízení, takzvané GOA (angl. Goal Of Automation) a stanovuje obecné požadavky na řídicí systémy. Druhá část normy obsahuje seznam povinných a volitelných funkčních požadavků, které má systém UGTMS splňovat. Část třetí obsahuje bezpečnostní požadavky na systém.

V případě plně automatizovaného provozu, bez strojvedoucího nebo bez obsluhy, jsou specifikované bezpečnostní požadavky na systém v normě EN 62267 [75].

Použitím současného řídicího systému ASDŘ lze provoz pražského metra zařadit ke GOA 2, což znamená polo-automatizovaný provoz. popisuje základní funkce UGTMS a rozdělení odpovědností mezi člověkem a elektronickým systémem dle stanoveného GOA.

Tabulka 5 Stupně automatizace UGTMS dle [74].

Základní funkce provozu vlaku			Provoz vlaku podle rozhledu	Neautomatizovaný provoz vlaku	Poloautomatizovaný provoz vlaku	Provoz vlaku bez strojvedoucího (řidiče)	Provoz vlaku bez obsluhy
			GOA0	GOA1	GOA2	GOA3	GOA4
Zajištění bezpečného pohybu vlaků	Zajištění bezpečné jízdní cesty		x (řízení výhybek v systému)	systém	systém	systém	systém
	Zajištění bezpečného rozestupu vlaků		x	systém	systém	systém	systém
	Zajištění bezpečné rychlosti		x	x (částečný dohled prováděný systémem)	systém	systém	systém
Řízení vlaku	Řízení zrychlování a brzdění		x	x	systém	systém	systém
Sledování vodicí dráhy	Zabránění střetu s překážkami		x	x	x	systém	systém
	Zabránění střetu s osobami na kolejích		x	x	x	systém	systém
Sledování pohybu cestujících	Ovládání dveří pro cestující		x	X	X	X	systém
	Zabránění úrazům osob mezi vozy nebo mezi nástupištěm a vlakem		X	X	X	X	systém
	Zajištění podmínek bezpečného rozjezdu		x	x	x	x	systém
Provozování vlaku	Uvádění vlaku do provozu a odstavování z provozu		x	x	x	x	systém
	Sledování stavu vlaku		x	x	x	x	systém
Zajištění detekce a řešení nouzových situací	Provádění diagnostiky vlaku, detekce ohně/kouře a detekce vykolejení, detekce nežádoucího rozpojení vlaku, řešení nouzových situací (hlášení/evakuace, dohled)		x	x	x	x	systém a/nebo personál v OCC
POZNÁMKA x = odpovědnost provozního personálu (může být realizována systémem UGTMS) systém = musí být realizován systémem UGTMS							

Tabulka 6 obsahuje požadavky na rozhraní systému, tj. rozděluje základní funkce systému podle dané stupně automatizace. Jestliže pražské metro definujeme jako systém režimu GOA2 dle [74], řídicí systém musí plnit základní funkce pro zajištění bezpečného pohybu vlaků, řízení vlaku. Další funkce mohou plnit jiné nezávislé subsystémy. Dle normy EN 62290 musí být systém UGTMS (tj. ASDŘ-D) schopen tvořit rozhraní se subsystémy uvedenými v předmětné normě, pokud jsou použity. Tabulka 6 popisuje rozhraní, prostředí a systémové hranice v souladu se zmiňovanou normou [74] a srovnává je s reálným stavem provozu Pražského metra; detaily jsou v práci [4].

Tabulka 6 Požadavky na rozhraní systému [4].

Legenda tabulky:

Tučně vyznačené položky jsou v řízeném systému využívány a jsou součástí řídícího systému (ASDŘ-D).

Kurzívou jsou označeny položky, na které má řídící systém návaznosti.

~~Přeškrtnuté~~ funkce či subsystémy nejsou pro provoz pražského metra uvažovány.

ASDŘ-D (UGTMS)	**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, komunikaci mezi traťovým zařízením a vlakovým zařízením)
Řízení	**Ústřední rozhraní s personálem**
	Místní rozhraní s personálem
	Traťová zařízení (např. výhybky, návěstí a návěstidla, kolejové obvody, čítače náprav, traťová zařízení kontrolující rychlost, sousední řídící střediska, automatické zastavení, přejezdy)
	Stávající uzávorování
	Plánování provozu
Informační systémy komunikace	*Zvuková komunikace (např. komunikace s personálem, s cestujícími)*
Stanice	*Pomocná zařízení (např. výtahy/eskalátory)*
	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 nechráněného prostoru, odbavovací tlačítko/vlak připraven k odjezdu)
	Monitorování pomocí CCTV
	Informace pro cestující na trati
	Zvuková komunikace
Vlak	*Dveře, pohon, brzdy, zařízení propojující vlak (např. elektrické mezi vozidlové propojky)*
	Rozhraní s personálem obsluhy vlaku
	Zařízení pro detekci překážek, vykolejení, ohně/kouře
	Detekce nechráněného prostoru, zařízení pro uzavření nechráněného prostoru
	Rukojeť pro nouzové zastavení uvolnění dveří/nouzové tlačítko
	Rozhraní s jinými zařízeními (např. s osvětlením, vytápěním, větráním, klimatizací (HVAC), baterií)
	Diagnostika vlaku (pro údržbu)
	Stav vlaku (z hlediska způsobilosti k provozu)
	~~Vybírání jízdného (informace o lokalizaci)~~
	Monitorování pomocí CTTV
	Informace pro cestující ve vlaku
	Zvuková komunikace
Infrastruktura	*Kolej (např. detekce zlomené kolejnice)*
	Větrání tunelu (například detekce ohně a kouře)
	Systém detekce narušení
	Rozhraní s jinými zařízeními (např. tlakovými uzávěry)
Trakční napájení	*Řízení trakčního napájení*
	Vysokonapěťový vypínač
Údržba	**Systém údržby**

Funkce pro automatické vybírání jízdného s lokalizací a nástupištní dveře uvedené v tabulce nejsou v systému pražského metra zatím instalované, nicméně v případě dalšího rozvoje (například pro plánovanou trasu D, které cílí na GOA 4) je nutné uvedené funkce a bezpečnostní opatření dle EN 62267 [75] zvažovat.

3.4 Přenosový systém řídícího systému metra a UGTMS

Obecný popis systému metra vychází z popisu systému řízení pražského metra ASDŘ [4], a evropského standardu pro definici funkcí a parametrů řídicího systému pro řízení městské kolejové dopravy [74], tj. systém UGTMS. Z technického úhlu pohledu můžeme sytém metra rozdělit na systémy řídicí, řízené a ochranné či

zabezpečovací, které mají vzájemné vazby a některé společné vstupy a výstupy, jak je uvedeno výše. 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 [4].

Tabulka 7 obsahuje obecný systém metra dle [4] a obsahuje přiřazení bloků a rozhraní systému (technických a funkčních) dle UGTMS, v návaznosti na obrázek 10, tabulku 6, a dle [63].

Tabulka 7 Obecný model systému metra.

Oblast	***Vstupy***	***Výstupy***
Řídicí systém	vnější vlivy, plánování provozu, řízený systém METRO	zabezpečovací zařízení, řízený systém METRO
Zabezpečovací systém	vnější vlivy, řídicí systém	Řízený sytém
Řízený systém METRO	vnější vlivy, zabezpečovací systém, řídicí systém	řídicí systém, kvalita provozu a dopravní výkon, snížení dopadů pohrom (ochranná funkce metra)

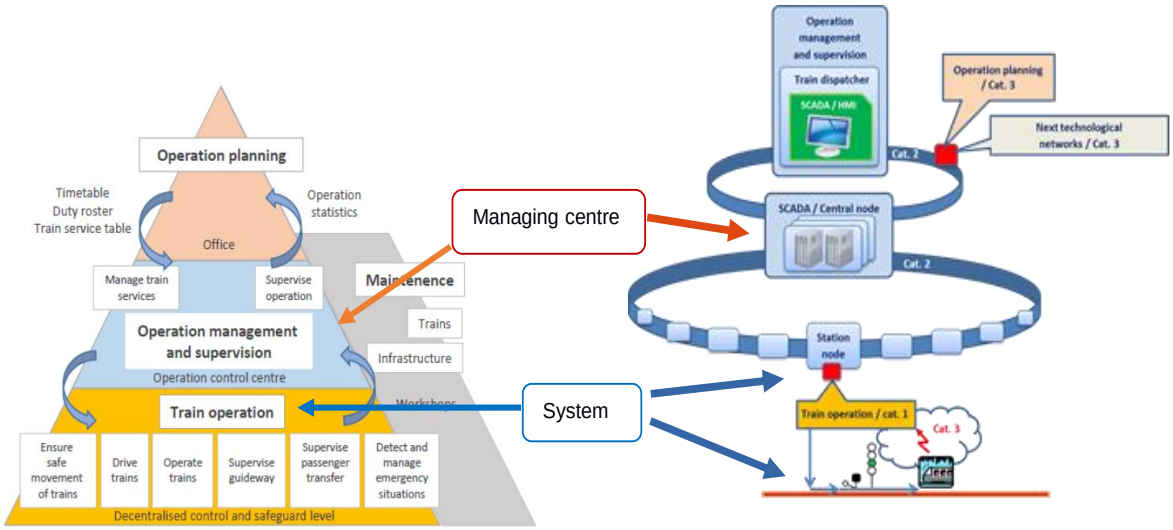
Uvedené funkce a členění dle UGTMS slouží pro vysokoúrovňové zadávací požadavky na systém. Neposkytují však detailní popis vazeb funkcí, parametrů jednotlivých subsystémů, nároků na bezpečnost a kvalitu. Zmíněné vlastnosti je nutné vždy specifikovat dle lokálních požadavků a podmínek návazných a nadřazených systémů, včetně vazeb na povrchovou dopravu, geologických a klimatických podmínek, míry ohrožení všech relevantních pohrom apod.

Dále se vymezíme především na požadavky a vlastnosti jádra systému UGTMS, které je kritickou částí systému řízení a jeho rozhraní, tj.:

- 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 12 popisuje vztah mezi teorií (odstavce 2.4.5 a 3.3), tj. obecným popisem systému a reálným stavem dle [10].



Obrázek 12. Model systému dle EN 62290 a reálný stav [10,63,74].

Na levé straně obrázku 12 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 11 značí kritická komunikační rozhraní a přenosové prostředí dle [63]. Označení Cat. 1-3 znamená kategorii přenosového prostření (systému) dle drážního standardu EN 50159 [76].

Při jisté míře abstrakce lze ke klasifikaci kyber-fyzického systému dle obrázku 8 z odstavce 2.4.5 přiřadit bloky systému UGTMS a reálné prvky řídicího systému ASDŘ-D pražského metra [63]:

- řídicí centrum (obrázek 8) – provozní řídicí zařízení – centrální uzly systému ASDŘ-D (respektive staniční řídicí uzly),

- systém (obrázek 8) – traťové a vlakové zařízení – staniční systémy a rozhraní, traťové přístupové body, vlakové komunikační jednotky, vlakové počítače,
- přenosové prostředí A, B (obrázek 8) – systémy datové komunikace – síť dispečerského centra, síť staničních a traťových uzlů, rádiové přenosové prostředí.

3.5 Výsledky analýzy znalostí a praxe z drážního prostředí a provozu metra

Předchozí práce v rámci magisterského a doktorského studia jsou zaměřené na:

- modelové případy (modelová stanice metra) [1,4,20,77,78],
- případové studie [10,63],
- analýzy příčin a následků železničních nehod [16,43,73,79,80],
- porovnání shody normativu a současné praxe v dopravě a průmyslu s legislativou a jejich kritické posouzení [21,40,78,81-83],
- induktivní a deduktivní analýzy [43,48,84].

Uvedené práce analyzovaly mnoho nedostatků a kritických míst drážního systému, na která ve většině případech navrhují konkrétní procesní i technická opatření.

Na základě výše uvedených výsledků, a hlavně podle porovnání shody normativů a praxe lze konstatovat, že v praxi ***jsou zásadní nedostatky***:

1. Není řádně zavedeno vrcholové řízení s proaktivním přístupem a přístupem k integrálnímu riziku.
2. Chybí mezioborová komunikace a vazba mezi jednotlivými vrstvami SMS.
3. Požadavky na bezpečnost nejsou řešeny komplexně; nemusí být identifikována všechna prioritní (tzn. významná) rizika.
4. Ve všech vrstvách řízení bezpečnosti chybí koncept All-Hazard-Approach.
5. Absence konceptu Defence-In-Depth pro kritické objekty.
6. Přístup k bezpečnosti a zabezpečení je v české i evropské legislativě pojat odděleně a neřeší vzájemné závislosti, které mohou ovlivnit bezpečnost.
7. Drážní předpisy a normy dostatečně neřeší zabezpečení drážních zařízení.
8. Neuvažují se vazby a toky za hranicemi systému.

Z hlediska systému řízení byly identifikované následující organizační zranitelnosti:

1. Špatně provedená procesní analýza, špatně nastavené procesy a pracovní instrukce nerespektující moderní přístupy řízení bezpečnosti.
2. Nedostatečná organizace, neflexibilní organizační struktura.
3. Neznalosti požadavků z vyšších vrstev SMS nebo jejich nepochopení.
4. Nedostatečná mezioborová komunikace, nejednotnost v terminologii.
5. Nedostatečný monitoring, matoucí informace o zdrojích rizik systému směrem k vyšším vrstvám řízení a naopak.
6. Nedostatečné vazby mezi procesy a rolemi v projektu, vzájemné závislosti jednotlivých rolí.
7. Nedostatečnost kompetencí v dané roli, nejasná definice rolí a jejich odpovědnosti, nedostatečné vzdělání, školení a trénink.

Současná legislativa požaduje rozsáhlou množinu technických i organizačních opatření pro zmírnění známých slabin systému, zejména pokud se jedná o řízení provozu ***za normálních podmínek***, případně při výskytu známých dopravních mimořádností, tzn. dle přístupu Defence-In-Depth (odstavec 2.1.7) jde o zabezpečený provoz při odchylkách nebo v abnormálních podmínkách. Jestliže okolní podmínky přesáhnou očekávanou a známou mez, například ***při kritických pohromách***, legislativní požadavky, a tím i organizační schopnosti podniků ***začínají selhávat***. Dalším aspektem vedoucím k selhání je také míra vynucování legislativy (tj. vynucování zajištění bezpečnosti).

Případové studie na systém řízení z pohledu kyber-fyzických systémů dále ukazují na následující fakta:

1. Prvky aktivní a pasivní bezpečnosti jsou implementovány pouze na základě zkušeností, tj. nekoncepčně, bez stanovení stupnic kritičností aktiv a rizik, bez zohlednění propojení s důležitými okolními a nadřazenými systémy; z hlediska integrální bezpečnosti se jedná o jasné zranitelnosti v oblasti bezpečnosti systému.
2. Není možné zajistit neomezenou dostupnost systému kvůli velkému počtu subjektů, které se na provozu podílejí za různých okolních podmínek; nicméně dostupnost systému lze zlepšit zvýšením informačního výkonu.
3. Vzhledem k rozhraním systémů různých povah jsou včasnost a validita zpráv o poruchách směrem k uživatelům značně limitované (systémy mají různé

požadavky na důvěrnost, dostupnost a integritu informací, jiné principy a opatření).

4. Kontinuita provozu systému je ovlivněna dostupností systému, to znamená, že závisí také na informačním výkonu; každý subjekt zavádí do systému jisté nejistoty a neurčitosti, které degradují informační výkon, a proto je kontinuita systému ve skutečnosti závislá na subjektu s nejhorší mírou informačního výkonu.
5. Přesnost systému je vždy méně či více omezena rozsahem, který zužován nízkým informačním výkonem, horším zajištěním informačních aktiv a vyšší systémovou komplexitou (složitostí).

Na základě analýzy příčin a následků železničních nehod byly analyzované následující problémy:

1. Problémy na rozhraní člověk – stroj (HMI, angl. Human Machine Interface).
2. Problémy na rozhraních systémů kyber-fyzických.
3. Problémy na rozhraních systémů socio-technických.
4. Stanovení odpovědností, a to ne jenom mezi subjekty, ale také mezi procesy systémů, tj. technologických děl.

Výše uvedené skutečnosti, zranitelnosti a problémy ukazují právě na složitost SoS, které jsou charakteristické svojí provázanosti, tj. interdependence. Interdependence dle znalostí uvedených v Kapitole 2 jsou dle jejich povahy fyzické, kybernetické, místní a logické [6] a za podmínek abnormálních a kritických (nadprojektových) vedou ke ztrátám systému, a způsobují, že systémy řádně neplní svoje funkce a ohrožují sebe a své okolí.

Zvláštní problémy, které vzájemně interagují, a je potřeba je na základě uvedených analýz v rámci SMS zvažovat, jsou:

- ***nehomogenity a anizotropie*** systémů a jejich prostředí – vedou k hysterezím,
- ***rozhraní systémů a procesů*** (HMI, kyber-fyzické, socio-technické, různé kritičnosti, aj.) - různé povahy rozhraní a jejich neurčitost stavů za jistých podmínek vedou k selháním,
- ***kaskádové jevy*** – vedou k eskalaci a vyšším dopadům selhání.

4 Popis použitých metod a nástrojů – návrh řešení

Předmětem analýzy je SoS, tj. měkký systém, který nemá přesně definované hranice a rozhraní s jinými systémy, resp. má proměnlivé hranice na různých úrovních abstrakce. Předmětný systém nelze analyzovat přesnými (exaktními) metodami a je nutné jej analyzovat pomocí metody vhodné pro analýzu měkkých systémů [85], tj. proto je nutné vybírat z heuristických metod, konkrétně metod expertních [23] a provést vhodné zpracování získaných dat pro jejich následnou analýzu. Metody jsou detailně popsány v [5,16,23].

4.1 Expertní metoda použitá pro sběr dat

Expertní metody dle [86] využívají znalosti a praktické zkušenosti expertů v příslušném oboru k získání: odhadů neměřitelných veličin, odhadů údajů, které nejsou k dispozici a jejichž získání by bylo neúměrně náročně, odhadů budoucího vývoje (stavu), návrhu tvůrčích řešení, apod. Typickým využitím expertů jsou v uvedené množině metod úzké specializované problémy, anebo zejména obecné, složité a komplexní problémy (tj. složitě a špatně strukturované, slabě formalizované, jedinečné a neopakovatelné, s nedostatkem či úplnou absencí objektivní kvalitativní informace, apod.) [86]. Expertní šetření probíhalo v následujících fázích:

1. Výběr expertů.
2. Získání expertních výpovědí.
3. Vyhodnocení expertních výpovědí.

Kvalita výběru expertů přímo ovlivňuje kvalitu získaných výsledků analýzy. Rozhodujícími vlivy jsou počet expertů (tj. pro statistickou významnost získaných výsledků) a jejich relevantní vlastnosti (např. kompetentnost, kreativita, vztah k tématu, konformita, analytické myšlení a šíře myšlení, konstruktivnost, sebekritičnost, tolerance) [86]. Určení počtu expertů a výběr vhodných vlastností jsou parametry závislé na výběru metody pro získání expertních výpovědí a zároveň tímto ovlivňují náklady na analýzu, tj. finanční i časové.

Získání expertních výpovědí může probíhat více způsoby, a to dle [86] podle: způsobu komunikace organizátorů s experty, úrovně komunikace mezi experty

během expertního šetření, opakovanosti zjišťování informací, stupně standardizace.

Pro účely disertační práce byla zvolena vícestupňová metoda Delphi.

4.1.1 Vícestupňová metoda Delphi

Uvedená vícestupňová metoda Delphi [23,86] je metodou získání expertních výpovědí s následujícími vlastnostmi [86]:

- více kolové anketní šetření se zpětnou vazbou,
- dochází k systematickému zpřesňování názoru skupiny expertů,
- anonymita expertů,
- zpětná vazba informací,
- experti mají před dalším kolem k dispozici skupinový názor i netypické názory,
- možnost přihlížet k okolnostem, které si expert dříve neuvědomoval, resp. možnost přehodnocení netypického názoru,
- pokud expert trvá na netypickém názoru, musí jej odůvodnit.

Získání výpovědí probíhá ve více kolech, ve kterých dochází k postupnému upřesňování posledních výsledků. Ukončení metody nastává při dosažení "shody" expertů, nebo je-li dosaženo stability individuálních výpovědí [86]. Nevýhodou metody Delphi je její časová náročnost a vyšší pracnost zpracování otázek se zacílením k požadovaným výsledkům, zpracování anketních dotazníků a interpretace výsledků pro jejich doplnění v dalším kole, resp. stupni odpovědí.

Vyhodnocení expertních výpovědí probíhá dle [86] ve dvou fázích: určení skupinového názoru, a posouzení kvality získaných informací. Určení skupinového názoru lze provést pomocí kvantitativních (aritmetický průměr, modus nebo medián, rozdělení, statistické charakteristiky – rozptyl, kvantilové rozpětí, intervalové odhady, charakteristiky rozdělení) nebo kvalitativních odhadů (nominální stupnice, převod na bodovou kvantitativní stupnici, formalizace a kvantifikace odpovědí).

4.1.2 Využití metody Delphi pro bezpečnostní výzkum provozu metra

Cílem výzkumu provedeného ve spolupráci se zaměstnanci Dopravního podniku hl. m. Prahy bylo ověření metod pro hodnocení kritické infrastruktury a určení kritičností prvků systému. Výzkum probíhal formou expertního šetření. Každý expert byl dotazován pomocí elektronického formuláře [5,16], k jeho vyplnění byl dotázán e-mailem.

Skupina expertů byla volena na základě referencí od vybraných zaměstnanců provozovatele metra a od vybraných poskytovatelů služeb a dodavatelů klíčových zařízení potřebných pro provoz metra. Každý, takto oslovený expert měl možnost doporučit další vhodné experty v následujících oblastech: bezpečnost práce a ochrana zdraví personálu, ochrana majetku, ekonomika provozu, ochrana cestujících, technická a funkční bezpečnost provozu.

Podmínkou pro doporučení experta do expertního týmu byla jeho dlouholetá znalost provozu metra s praxí v různých oblastech uvedených výše a na různých úrovní řízení, tj.: strategické řízení, taktické a projektové řízení, operativní řízení, technický pracovník, technické práce.

Celkem bylo osloveno 18 expertů, kteří byli před zahájením šetření požádáni o vyplnění krátkého dotazníku pro určení kvalifikace experta dle [86].

Dotazování metodou Delphi bylo členěno celkem do 3 fází:

1. Identifikace aktiv (funkce, místa a části systému metra, která jsou důležitá pro jeho bezpečný provoz).
2. Určení důležitosti a zranitelnosti.
3. Scénáře dopadů vybraných pohrom.

Po skončení každého kola dotazování byly výsledky vyhodnocené, a v případě neshod se provedlo upřesnění a odůvodnění, které probíhalo i v několika iteracích. Průběh šetření a jednotlivé otázky pro každé kolo jsou uvedené v příloze A.

4.1.3 Použité stupnice

V uvedeném bezpečnostním výzkumu a v předložené disertační práci pracujeme s kritičností ***K***, jakožto funkce důležitosti ***D*** a zranitelnosti ***Z***, v souladu s definicí v odstavci 2.1.3:

$$K = D \times Z \quad (21)$$

Uvedené veličiny jsou závislé na tom, v jaké úrovni systému řízení bezpečnosti danou veličinu posuzujeme, tj. dle přístupu Defence-In-Depth (odstavec 2.1.7 a 2.3.4) a podle zdroje [18] sledujeme následující úrovně (podrobnější popis úrovní pro účely předmětného výzkumu je v příloze A):

1. Bezpečný provoz metra za normálních podmínek (**úroveň řízení L1**).
2. Bezpečný provoz metra za abnormálních podmínek (**úroveň řízení L2**).
3. Bezpečný provoz metra při větších odchylkách / zvládání havárií (**úroveň řízení L3**).
4. Řízení provozu a aktiv metra v případě kritických podmínek (**úroveň řízení L4**).
5. Řízení provozu a aktiv metra v případě extrémních podmínek (**úroveň řízení L5**).

Pro veličiny ***D a Z*** byly použité ordinální škály, tj. stupnice v rozmezí 1 až 3, se zvážením kritérií pro kritickou infrastrukturu [34,35]. Popis každé číselné hodnoty je uveden v odstavci A.2.1 přílohy A.

Rozdělení pohrom do kategorií relevantní, specifické a kritické dle přístupu All-Hazard-Approach (odstavec 2.1.2 a 2.1.7).

4.2 Zpracování a analýza dat

Pro odvození závislostí ve složité kritické infrastruktuře, v případě použití, tj. infrastruktura metra, je v předložené práci použita teorie citlivostí, kterou lze ocenit sílu jednotlivých závislostí, tj. míru jejich zranitelnosti, což znamená schopnosti závislostí způsobit selhání (KI, metra). Matice jsou pro jejich následnou analýzu transformované do grafu.

4.2.1 Teorie citlivosti

Z důvodů lepší interpretace a práce s informačními systémy lze zranitelnost definovat také jako citlivost s využitím teorie citlivostí [87,88], kterou lze poptat následujícím vztahem [89]:

$$S_i = \frac{\partial y}{\partial x_i}, \quad (22)$$

kde ***Si*** je absolutní citlivost výstupní funkce y na parametr vstupní funkce x_i. Přičemž dle zdroje [90] je ve smyslu elektronických systémů ***y = f(x1,..,,xi,…,xN)*** síťovou (resp. systémovou) funkcí, jež je závislá na obvodovém parametru x_i. Změna výstupní funkce systému je tedy závislá na její citlivosti a na změně vstupních parametrů x_i, uvedený vztah se z praktických důvodů zapisuje v maticovém tvaru, tj. pomocí matice citlivostí ***S*** [90]:

$$\Delta Y = S \cdot \Delta X. \quad (23)$$

U elektrických, elektronických a programovatelných elektronických systémů (dále jen E/E/PE) je výhodné počítat s relativní citlivostí a s relativní změnou parametru, protože umožňuje výpočet tolerancí výstupní veličiny, návrhu tolerancí vstupních parametrů, optimalizaci citlivosti elektrického obvodu, hledání nejcitlivějších prvků, tj. prvků s největším vlivem na změny výstupní veličiny [90].

Pro práci s aktivy je vhodné pracovat s citlivostí absolutní, protože ačkoliv jsou dané stupnice pro hodnocení kritičností normalizované, každá funkce aktiva má jiný fyzikální základ.

4.2.2 Maticový zápis a kodifikace názvů

Zvyklost praxe je uvádět vztahy jednotlivých prvků v tabulkách. V našem případě se jedná o citlivost, tedy vztah vstupních veličin (pohromy, resp. aktiva a výstupních veličin (funkce systému, resp. aktiv):

- aktiva jsou v řádcích tabulky,
- pohromy jsou ve sloupcích.

Pro lepší přehlednost je použit maticový zápis znázorněn tabulkou 8.

Tabulka 8 Formát tabulky kritičností aktiv pro jednotlivé pohromy.

	Pohroma 1	***. …***	***Pohroma n***
Aktivum 1	S11	. …	Sn1
…	.	. …	.
Aktivum m	S1m	. …	Snm

Tabulku 8 převedeme do maticového tvaru, ve které y_i označuje aktiva a x_i označuje pohromy. Maticový zápis umožňuje provádět patřičné operace a převod matice do grafu pro analýzu scénářů.

$$\begin{pmatrix} \Delta y_1 \\ \cdot \\ \cdot \\ \Delta y_m \end{pmatrix} = \begin{pmatrix} S_{x_1}^{y_1} \cdot S_{x_n}^{y_1} \\ \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \\ S_{x_1}^{y_m} \cdot S_{x_n}^{y_m} \end{pmatrix} \cdot \begin{pmatrix} \Delta x_1 \\ \cdot \\ \cdot \\ \Delta x_n \end{pmatrix} \tag{24}$$

Vstupní parametry x_i mohou ve skutečnosti představovat také výstupní parametry jiných aktiv (funkcí). V případě, že chceme zobrazit souvislosti více do hloubky, lze kombinací vstupních a výstupních parametrů na obou stranách rovnice vytvořit zřetězení, tj. pro účely práce „zřetězené matice citlivostí“, které v technice znamenají míru zranitelností závislé na míře propojení veličin nebo parametrů [6,33].

V praxi uvedené tabulky a matice mohou nabývat velkých rozměrů a pro zajištění jejich čitelnosti je vhodné zavést přiměřenou kodifikaci názvů. V disertační práci je použito číselné označení pohrom uvedené v příloze B. Použité označení skupin aktiv je uvedeno v Tabulce 9.

Tabulka 9 Použité označení skupin aktiv.

Skupina	***Označení***
Konstrukce	AK
Technika	AT
Personál	AP
Místa	AM
Funkce	AF
Vazby a toky	AV
Organizace a ekonomika	AO

Číselné označení dílčích tříd aktiv použitých níže v disertační práci je z důvodu jejich velkého rozsahu uvedeno v příloze C.

4.2.3 Transformace matic do grafu

Využitím teorie grafů, popsané např. v práci [91], můžeme zranitelnosti zobrazit pomocí ohodnoceného orientovaného grafu. Pro vytvoření grafu je třeba:

- použít matice citlivostí, uvedené v předchozích odstavcích 4.2.1 a 4.2.2,
- transformovat matice citlivosti do matic sousedností, které vyjadřují míry těsnosti propojení sledovaných veličin. Předmětné matice jsou základem pro generování grafů, které vyjadřují míry propojení příslušných veličin.

Pro vytvoření matic sousedností je použit nástroj MS Excel, export souboru s maticemi je dále importován do nástroje určeného pro práci s grafy – Gephi verze 9.0.2 [92].

Proces transformace do grafu lze rozdělit do následujících kroků:

1. Sestavení matic sousedností (měr těsnosti propojení) z matic citlivostí (měr zranitelností).
2. Sestavení orientovaného grafu – grafická interpretace.
3. Ohodnocení hran (zranitelnost dané vazby – propojení) a uzlů (zranitelnost, resp. kritičnost sledovaných veličin, aktiv).
4. Analýza grafu a grafická interpretace výsledků.

4.2.3.1 Sestavení matic sousedností z matic citlivostí

Matice sousedností [91] vyjadřuje relace mezi dvěma objekty (v uvedeném případě vstupních a výstupních parametrů funkce, respektive mezi uzly, které reprezentují aktiva či pohromy). Jejich sloupce i řádky vyjadřují tutéž množinu objektů ve stejné posloupnosti. Aby bylo možno použít matice citlivostí, je nutné začít se vstupními parametry funkce a následně pak s výstupními parametry funkce takto: ***APdii02***; ***ATv***; ***Atzb***; ***AVi06*** (použitá označení jsou vysvětlená v příloze C).

Podle teorie matic postupujeme tak, že do prázdné matice sousedností dosadíme transponovanou matici citlivostí a za předpokladu, že jde o podklad pro konstrukci orientovaného grafu, ve kterém vztahy jsou jednosměrné, do ostatních pozic matice doplníme nuly „0“. Tabulka 10 reprezentuje výslednou matice sousedností, modře podbarvené buňky tabulky znázorňují transponovanou matici citlivostí.

Tabulka 10 Matice sousedností pro vztah (44) (odstavec 6.1.3).

	APdii02	ATv	ATzb	AVi06
APdii02	0	0	0	1
ATv	0	0	0	1
ATzb	0	0	0	1
AVi06	0	0	0	0

Předmětný algoritmus lze aplikovat pro všechny předchozí jednoduché vztahy, ve kterých nejsou některé vstupní a výstupní parametry společné. Pro zřetězené matice je nutné brát v potaz právě společné vstupní a výstupní parametry a vytvářet posloupnost uzlů obezřetně. Zápis zřetězené matice je uveden v tabulce 11

Tabulka 11 Matice sousedností pro zřetězené matice (vztah (45) a 6.1.3).

	AKs01	AKk06	ATv	AVi06	ATe	AMtp03	APdii02	ATzb	AVm01
AKs01	0	0	0	0	0	0	0	0	0,5
AKk06	0	0	0	0	0	0	0	0	0,5
ATv	0	0	0	1	0	0	0	0	0,5
AVi06	0	0	0	0	0	0	0	0	0,5
ATe	0	0	0	0	0	0	0	0	0,5
AMtp03	0	0	0	0	0	0	0	0	0,5
APdii02	0	0	0	1	0	0	0	0	0
ATzb	0	0	0	1	0	0	0	0	0
AVm01	0	0	0	0	0	0	0	0	0

4.2.3.2 Sestavení orientovaného grafu – grafická interpretace

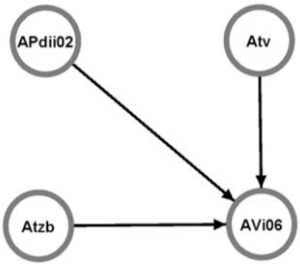
Orientovaný graf je dle definice [91] vyjádřen uspořádanou trojicí:

$$\vec{G} = \langle \boldsymbol{H}, \boldsymbol{U}, \boldsymbol{\sigma} \rangle, \tag{25}$$

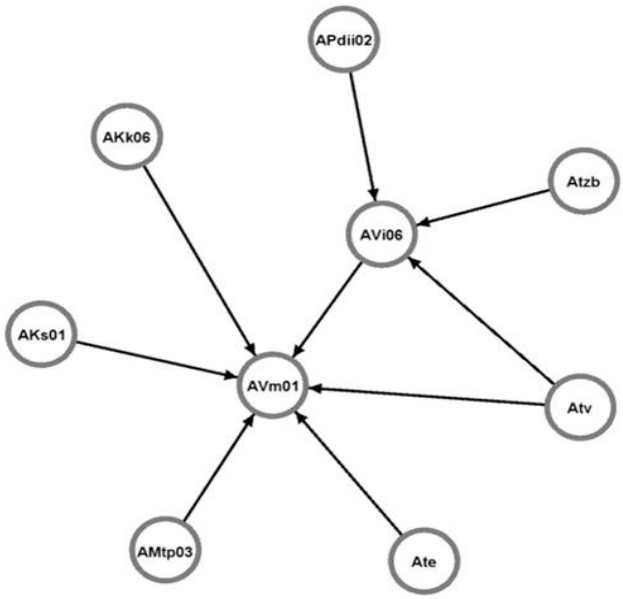
kde $\boldsymbol{H}$ je množina hran, $\boldsymbol{U}$ je množina uzlů a $\boldsymbol{\sigma}$ je incidenční relace vyjádřená vztahem:

$$\boldsymbol{\sigma}(\boldsymbol{h}) = \langle \boldsymbol{u}, \boldsymbol{v} \rangle, \quad (26)$$

kde ***u*** je počáteční vrchol a ***v*** je koncový vrchol. Graf ***G*** lze plně odvodit z matic sousedností [91]. Graf pro tabulku 10 je na obrázku 13 a pro tabulku 11 je na obrázku 14.



*Obrázek 13. Graf pro tabulku 3 (**AVi06)**, [3].*



*Obrázek 14. Graf pro tabulku 4 (**Avi06-m01**), [3].*

4.2.3.3 Ohodnocení hran (zranitelnost dané vazby) a uzlů (zranitelnost, resp. kritičnost)

Obrázky 13 a 14 znázorňují grafy dle uvedených matic sousedností, ale nereprezentují ohodnocení hran a parametrů uzlů. Ke každé hraně a uzlu lze textem

připsat požadované informace (ohodnocení pomocí váhy hrany, resp. zranitelnost či kritičnost uzlu). S využitím SW nástroje [92] lze navíc uvedené parametry různě interpretovat graficky, tj. změna velikosti či barvy hran a uzlů podle jejich vlastností. Váha hrany je pro účely předložené práce ohodnocení mírou propojení čili mírou citlivosti (resp. zranitelnosti) cílové ho aktiva na vstupní parametr (funkce aktiva či pohroma).

Textové ohodnocení uzlů v disertační práci znázorňuje kritičnost, pokud je pro danou analýzu potřeba (např. Obrázek 21 v odstavci 6.2.3).

Rozměry a barvy uzlů a hran použité v disertační práci jsou popsané v následujícím odstavci.

4.2.3.4 Analýza grafu a grafická interpretace výsledků

Pro zobrazení grafu byl použit nástroj Gephi 0.9.2 [92]. Výchozí zobrazení (rozmístění) uzlů na ploše v nástroji není ideální, proto je nutné rozložení vhodně upravit. Lze využít manuálního rozmisťování uzlů podle potřeby a typu uzlu nebo je také možnost využít známých algoritmů. Zároveň barevné rozlišení uzlů a hran a jejich velikost je vhodné upravit podle jejich stupně, vah a dalších parametrů.

Pro analýzu grafů bylo zvoleno následující nastavení volitelných parametrů, které nástroj umožňuje [92]:

1. ***Rozložení:***
   - silově zaměřené Fruchterman-Reingold [93],
   - oblast: 10000; gravitace: 10; rychlost 1, které ovlivní výsledné rozložení uzlů a hran na pracovní ploše (resp. na plátně) v SW nástroji.
2. ***Uzly:***
   - velikost dle „Stupně dovnitř“; min: 10; max: 50; exponenciálně, uvedené nastavení na pracovní ploše exponenciálně zvětší uzly, které mají více vstupujících hran,
   - barva dle „Stupně dovnitř“; min: černá; max: červená; lineárně, uvedené nastavení na pracovní ploše červeně zabarví uzly, které mají více vstupujících hran,

- ***„stupeň dovnitř“*** vyjadřuje počet vstupujících hran do daného uzlu bez ohledu na jejich váhu,
- ***„stupeň ven“*** vyjadřuje počet vystupujících hran z daného uzlu bez ohledu na jejich váhu.

3. Hrany:

- ve výchozím nastavení tloušťka dle váhy,
- barva dle „Váhy“; min: černá; max: červená; v intervalu mezi minimem a maximem lineárně rozložená.

4.3 Zvýšení bezpečnosti s využitím znalosti a metody řízení rizik

Pravděpodobnost včasného a správného rozhodnutí (odstavec 2.4.3) k zabránění nebo zmírnění dopadů nepříznivých událostí, a to především za abnormálních a kritických podmínek, lze dle [64] dosáhnout:

- vyšší znalostí problémů a zranitelností (uvedených v předchozím odstavci), tj. znalost struktury systémů jejich vazeb, rozdílů a prostředí,
- vyšším informačním výkonem.

Znalost systému a informační výkon spolu souvisí a jsou limitované fyzikálními vlastnostmi systémů, proto je nutné hledat vhodnou rovnováhu. Informační výkon zvýšíme buď mírou informace nebo informačním tokem. Míra informace závisí na znalosti systému a jeho schopnosti interpretace syntaktických řetězců v datovém toku [64]. Informační tok v čase zvýšíme přenosovou rychlostí a kapacitou přenosového média (které jsou taktéž limitované). Systémy s vyšší mírou znalosti potřebují nižší informační tok, jelikož ten obsahuje vyšší míru informace (např. jeden bit může znamenat jednu konkrétní událost na kterou musí systém reagovat). Naopak znalost systému je limitován jeho výpočetním výkonem, pamětí, ontologií a/nebo kognitivními schopnostmi. Záleží, zda znalost přiřazujeme přirozeným či umělým systémům (člověk/stroj, fyzika/kybernetika, společnost/technika a technologie) [64].

Zvyšování včasného a správného rozhodnutí znamená zvyšování bezpečnosti, tj. zavádíme opatření pro zvýšení bezpečí lidí (odstavec 2.1.4). Zvýšení bezpečnosti vede ke snížení kritičnosti – což je jedním ze základních cílů předložené práce.

Výsledky zpracování dat metodami uvedenými v předchozích odstavcích po jejich správné interpretaci zvyšují znalost o systému a jeho provozních rizicích ve vztahu k bezpečnosti, tj. správná interpretace dat a řízení rizik vede ke zvýšení bezpečnosti systému. Pro řízení rizik se v praxi používá plán řízení rizik.

Plán řízení rizik je nástrojem řízení rizik, popsán a použit například v pracích [4,20,22,24,30,41,43,77]. Plán řízení rizik vybraného objektu KI se musí zabývat jednotlivými vrstvami řízení bezpečnosti, riziky plynoucí ze vzájemných souvislostí mezi vrstvami, závislostmi mezi bezpečností a zabezpečením, závislostmi mezi vnitřními subsystémy a vnějším okolím, tj. oblasti rizik. Jednotlivá rizika z uvedených oblastí představují pravděpodobnost selhání a jejich dopady na kritických místech v systému, jak z hlediska řízení, stavby, techniky, organizace, lidí, míst, vazby a toky a rozhraní, jedná se o tzv. prioritní rizika. Účelem plánu řízení rizik je jejich zvládání, proto musí poskytovat základní rozdělení oblastí, popis rizika, ohodnocení, návrh opatření na zmírnění rizika a kdo je za implementaci opatření odpovědný, kdy a za pomocí jakých nástrojů.

Pro řízení rizik objektu KI, je tedy nutné, aby plán řízení rizik obsahoval:

- oblasti rizik,
- popis rizika,
- pravděpodobnost výskytu a dopady rizika,
- opatření na zmírnění rizika, která jsou podpořena, zajištěním techniky, postupem provedení, personálem, odpovědnostmi a financemi.

5 Bezpečnostní výzkum provozu pražského metra

Následující kapitola obsahuje výsledky použití metod a nástrojů z kapitoly 4.1. Níže uvedené výsledky byly dále prezentovány v [5,16]. Následující kapitoly obsahují postup a důležité průběžné výsledky jednotlivých kol.

5.1 Aktiva provozu pražského metra

První kolo bezpečnostního výzkumu metodou Delphi ve spolupráci se experty z řad zaměstnanců Dopravního podniku hl. m. Prahy bylo zaměřené na identifikaci aktiv důležitých pro bezpečný provoz metra v pěti úrovních řízení bezpečnosti (L1 až L5, definované v odstavci 4.1.3, a A.2.1 přílohy A). Pro kolekci všech identifikovaných aktiv bylo zapotřebí tří iterací, jelikož experti na základě znalosti z praxe identifikovali více stejných aktiv s jinými názvy anebo neidentifikovali aktiva, která jsou z hlediska řízení bezpečnosti důležitá a zřejmě v systému řízení metra chybí. Otázky, na které experti odpovídali jsou uvedené v příloze A.

Po prvním kole bezpečnostního výzkumu metodou Delphi byla identifikována aktiva v následujících skupinách:

- konstrukce (stavby a konstrukční technologie),
- technika (vzduchotechnika, osvětlení, energetika, dopravní zařízení, dopravní prostředky, informační systémy, signalizační, sdělovací a zabezpečovací zařízení, vodohospodářství a kanalizace, kolejová technika, zařízení Ochranného systému metra, jiné – především pro L2-L3),
- personál (staniční, depa, traťoví a ostatní, dispečink I. až III. stupně),
- místa (veřejné prostory stanice, ostatní veřejné prostory, jiné neveřejné prostory stanice, technologické prostory, prostory dispečinku, tunely, prostory depa),
- funkce (staniční, technologické, personální),
- vazby a toky (informační, energetické, materiálové),
- organizace a ekonomika (jednotky a odbory, předpisy a plány, procesy, vlastnosti řídicích a odpovědných pracovníků, záchranné a bezpečnostní sbory, ekonomika).

Aktiva, která nebyla dostatečně identifikována, jsou například:

- některé obecné plány pro zvládání kritických podmínek (L3-5), tj. obecné plány kontinuity, plány čištění a dekontaminace apod., simulace mimořádných událostí a tréning,
- ekonomické – fondy, hmotné rezervy, rozpočet pro pravidelné kontroly, přezkoumávání a hodnocení organizačních, technických a procesních parametrů, rozpočet pro zajištění zabezpečení kritických aktiv (tj. pro kontinuální snižování kritičnosti = ochrana a zabezpečení výše uvedených aktiv).

Aktiva byla identifikována pro L1-L3 ve všech skupinách, pro L4 a L5 pouze ve skupině Organizace a ekonomika.

5.2 Zranitelnosti, důležitosti a kritičnosti aktiv

Pro identifikaci zranitelností a důležitostí aktiv byly použité stupnice uvedené v odstavci 4.1.3, s omezením na zranitelnosti, které jsou v tomto kole identifikovány jako citlivost na selhání okolních aktiv. Otázky, na které experti odpovídali jsou uvedené v příloze A. Výsledek je medián odpovědí expertů, v případě výrazných odchylek byla korekce předmětem další iterace. V případě menších odchylek a v případě lichého počtu odpovědí jsou možné i poloviční hodnoty, tj. 1,5 nebo 2,5.

Z hlediska dílčích kritičností, tj. součin výsledné důležitosti a zranitelnosti aktiva na funkci aktiv okolních, lze na základě výstupů výzkumu uvést jako nejkritičtější následující aktiva:

- osvětlení,
- vzduchotechnika (při řízení L3),
- dopravní zařízení,
- veřejné prostory a zabezpečení únikových východů,
- informační a materiálové toky (především ve vztahu k vzduchotechnice a technickému stavu objektů dopravních prostředků a zařízení),
- v případě L3-L5 potom součinnost a kvality (připravenost) záchranných a bezpečnostních sborů.

Výsledky pro skupinu aktiv Vazby a toky (jedna z nejkritičtějších skupin) jsou uvedené v tabulce 12. Aktiva v tabulce 12 jsou označená dle kodifikace podle odstavce 4.2.2 a jsou uvedené v příloze C. Ostatní konkrétní výsledky jsou neveřejné a byly poskytnuté DPP ve formě zprávy [7].

Tabulka 12 Výsledky pro skupinu aktiv Vazby a toky, dle [5,7,16].

Aktiva / úrovně řízení L	**Důležitost** 1-3: 1. základní důležitost, 2. větší důležitost, 3. vysoká důležitost			**Zranitelnost** na okolní aktiva 1-3.	**Dílčí kritičnost** = důležitost x zranitelnost		
	L1	L2	L3	L1-L5	L1	L2	L3
AVi01	3	3	3	2,5	7,5	7,5	7,5
AVi02	0	3	3	2,5	0	7,5	7,5
AVi03	2	3	3	2,5	5	7,5	7,5
AVi04	2	2	3	3	6	6	**9**
AVi05	3	3	3	2	6	6	6
AVi06	1	2	3	3	3	6	**9**
AVi07	1	2	3	2,5	2,5	5	7,5
AVi08	2	3	3	2,5	5	7,5	7,5
AVi09	2	3	3	2	4	6	6
AVi10	3	3	3	2	6	6	6
AVe01	3	3	3	2,5	7,5	7,5	7,5
AVe02	2	3	3	2	4	6	6
AVe03	3	3	3	2	6	6	6
AVe04	2	3	3	2,5	5	7,5	7,5
AVe05	2	3	3	2	4	6	6
AVe06	3	3	3	2	6	6	6
AVm01	1	3	3	3	3	**9**	**9**
AVm02	1	3	3	2,5	2,5	7,5	7,5

AVm03	1	2	3	2	2	4	6
AVm04	1	2	3	3	3	6	**9**

Tučně označená aktiva v tabulce 12 výše, mají nejvyšší kritičnost, proto vyžadují vyšší pozornost nežli ostatní. Ze skupiny Vazby a toky se tedy jedná o:

- ***AVi04***: Informační vazby (technický stav vlaků a objektů – depo – dispečink),
- ***AVi06***: Informační vazby (vzduchotechnika – TCHDM a ASDR-T),
- ***AVm01***: Materiálové toky (vzduch),
- ***AVm04***: Materiálové toky (provozní materiál ve stanicích (dozorčí provozu)).

Dílčí kritičnost závisí na zranitelnosti a důležitosti v jednotlivých režimech provozu L1-L5 a také na tom, při jaké události k výpadku aktiva může dojít, na to se zaměřuje další kolo výzkumu, popsané v následujícím odstavci.

5.3 Reálný stavu zabezpečení systému vůči specifickým a kritickým pohromám

Třetí kolo bezpečnostního výzkumu metodou Delphi bylo zaměřeno na určení dopadů pohrom, pro tvorbu jejich scénářů. Otázky třetího kola jsou rozděleny dle tří hlavních cílů tohoto kola:

1. Ověření kritičností pohrom, tj. rozřazení pohrom do skupin relevantní, specifické, kritické dle odstavce 2.1.2. Při vyhodnocení se porovnávala shoda s Tabulkou 1 v odstavci 2.1.2.
2. Identifikace nedostatků pro specifické pohromy, tj. zranitelnosti systémů (technologických a řídicích aktiv). Při vyhodnocení se porovnávala shoda s výsledky pro modelovou stanici metra [1,4].
3. Identifikace slabin v případě kritických pohrom, tj. hledání ochranných opatření proti kritickým pohromám.

Poslední kolo bylo ve skutečnosti limitované počtem odpovědí expertů a jejich koncentrací v případě většího množství otázek (v příloze A), tj. kvality odpovědí. Ve třetím kole se totiž berou v potaz jak veškerá aktiva, tak i všechny relevantní, specifické a kritické pohromy, což vede k velkému množství kombinací, které musí expert zvažovat. Výše uvedené je limitem metody Delphi, což vede k závěru, že je

zvolená metoda sice vhodná, ale je nutné ji doplnit o další hodnocení, například porovnání shody s modelovými případy, případovými studiemi a následnou diskusí. Po porovnání shody výsledků třetího kola s prací [1,4] zaměřených na aktiva a bezpečnost modelové stanice metra (ne reálného provozu) lze uvést následující zjištění rozdělených dle výše uvedených cílů.

V porovnání s tabulkou 1:

1. ***Experti nepovažují za relevantní*** následující pohromy: vichřice; ztekucení podloží; pandemie; epidemie; porucha stability lidské společnosti; ozbrojený konflikt; válka; průmyslová havárie; havárie při přepravě či skladování nebezpečných látek; pohroma v infrastruktuře; pohroma v infrastruktuře služeb, zásobování a spojení; ztráty obslužnosti; porušení; stability podloží vlivem vibrací; rychlé variace klimatu; selhání toků surovin a výrobků.
2. Za specifické, ale ne kritické pohromy experti považují:
   - kriminalitu a útok – ve shodě; zohledněné v rámci preventivních organizačních opatření,
   - havárie při dopravě – v tabulce označené za kritické; zohledněné v rámci preventivních technických a organizačních opatření,
   - pohromu v kybernetické infrastruktuře – ve shodě; zohledněné v rámci preventivních organizačních opatření,
   - selhání technologií – v tabulce označené za kritické; zohledněné v rámci preventivních technických opatření,
   - kontaminace ovzduší a vody – ve shodě; zohledněné v rámci preventivních technických opatření,
   - migrace velkých skupin lidí – v tabulce označené pouze za relevantní; zohledněné v rámci preventivních organizačních opatření,
   - organizační havárie, selhání toků energií a informací – v tabulce označené za kritické; zohledněné v rámci preventivních organizačních opatření,
3. Za kritické pohromy experti považují:
   - povodeň – ve shodě; jsou zavedena reaktivní opatření,
   - útok za použití CNRB zbraní – ve shodě; jsou zavedena reaktivní opatření,

- pohroma v oblasti kritické infrastruktury – v tabulce uvedené pouze za specifické,
- pohroma v územní infrastruktuře – v tabulce uvedené pouze za relevantní.

Odpovědi expertů se shodují se závěry prací [1,4], tj.:

- technologický systém má ve většině případech zapracované principy inherentní bezpečnosti, tj. bezpečného designu (stavby, materiály a konstrukce, které zmírňují dopady pohromy) – tj. mimo jiné bezpečný provoz metra za normálních podmínek (úroveň řízení L1) je zajištěn,
- řídicí systém má zavedeny řídicí funkce, alarmy a reakce operátora pro udržení normálního (stabilního) stavu za abnormálních podmínek (úroveň řízení L2), systém řízení obsahuje také bezpečnostní instrukce a fyzické bariéry, které při větších odchylkách zabrání výskytu dalších nežádoucích jevů (úroveň řízení L3) – ovšem implementace uvedených systémových funkcí jsou limitované a mohou se při nežádaných událostech vyskytnout nezajištěná místa,
- systém rovněž obsahuje některé instrukce a mechanizmy pro případ ztráty kontroly, tj. opatření pro nouzovou odezvu při kritických podmínkách při kterých se zajistí schopnost návratu do normálního stavu (úroveň řízení L4) – to platí jen pro vybrané události (povodně a útok za použití CNRB zbraní), nezahrnuje všechny pohromy,
- pro případ ztráty kontroly, tj. pro 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 (úroveň řízení L5) – tato úroveň je zajištěna nejméně a provoz je v případě extrémních podmínek značně zranitelný. Chybí plán kontinuity, který by ochránil kritická technická zařízení metra; v rámci krizového plánu města Prahy je řešena pouze ochrana životů a zdraví lidí.

V předmětné části se experti shodli na tom, že ochranná opatření a činnosti pro ochranu zaměstnanců a lidí jsou zajištěné pro případ povodně, havárii při dopravě. Dále pouze jeden z expertů uvedl, že:

- jsou zajištěna ochranná opatření a činnosti pro provoz technologie v případě povodně a selhání toků energií,
- pro řadu pohrom jsou zajištěna ochranná opatření a činnosti pro obnovu provozu do 14 dnů,
- u organizační havárie jsou zajištěny postupy pro špatnou odezvu.

Z odpovědí expertů vyplývá že s největší pravděpodobností nejsou zajištěna ochranná opatření a činnosti pro ochranu životního prostředí a lidí v okolí objektu a nejsou zajištěny ochranné postupy pro špatné řízení provozu.

Na základě výše uvedených výsledků lze na základě volby nejhoršího případu a pro potřeby předložené disertační práce dosavadní znalosti o pohromách aktualizovat, jak je uvedeno v Tabulce 13.

Tabulka 13 Rozdělení pohrom – relevantní, specifické, kritické (aktualizované).

	Relevantní	***Specifické***	***Kritické***
Výsledky procesů probíhající vně i uvnitř Země			
Povodeň	ano	ano	ano
Vichřice	ano	ano	
Zemětřesení	ano		
Ztekucení podloží	ano	ano	ano
Výstup plynu na zemský povrch	ano		
Výsledky procesů v lidském těle, v chování lidí a procesů v lidské společnosti			
Epidemie	ano	ano	ano
Pandemie	ano	ano	ano
Porucha stability lidské společnosti	ano	ano	
Kriminalita	ano	ano	
Útok	ano	ano	
Teroristický útok	ano	ano	ano
Útok za použití chemických, jaderných, radiologických a biologických (CNRB) zbraní	ano	ano	ano
Ozbrojený konflikt	ano	ano	ano
Válka	ano	ano	ano
Výsledky procesů a činností instalovaných lidmi			
Průmyslová havárie	ano		
Havárie při přepravě či skladování nebezpečných látek	ano		
Havárie při dopravě	ano	ano	ano
Pohroma v oblasti kritické infrastruktury	ano	ano	(ano)
Pohroma v ekonomice	ano		
Pohroma v územní infrastruktuře	ano	(ano)	(ano)
Pohroma v kybernetické infrastruktuře	ano	ano	

Pohroma v infrastruktuře služeb, zásobování a spojení	ano		
Selhání technologií	ano	ano	ano
Ztráty obslužnosti	ano		
Interakce planety Země a životního prostředí na činnosti lidí			
Porušení stability podloží vlivem vibrací	ano	ano	ano
Kontaminaci ovzduší	ano	ano	
Kontaminace vody	ano	ano	
Rychlé variace klimatu	ano		
Migrace velkých skupin lidí	ano	(ano)	
Vnitřní závislosti v lidském systému přirozené nebo lidmi vytvořené			
Organizační havárie	ano	ano	ano
Selhání toků surovin a výrobků	ano		
Selhání toků energií	ano	ano	ano
Selhání toků informací	ano	ano	ano

5.4 Diskuse výsledků s DPP

Vzhledem k tomu, že pro SoS používáme heuristické metody, nelze s jistotou tvrdit, že jsme docílili optimálnímu výsledku, ale snahou těchto metod je se optimálnímu výsledků co nejvíce přiblížit. Proto je před zavedením navržených opatření nutné schválení, a to na základě finální diskuse výsledků panelem expertů. Proto byly konkrétní výsledky uvedeného výzkumu shrnuté do závěrečné zprávy [7] a rozeslané zúčastněným expertům DPP. Předmětná zpráva slouží k uvedené diskusi, kde každý expert může výsledky komentovat buď svojí odpovědí na výzkum anebo mohou zaměstnanci DPP výsledky využít v rámci postupného zavádění opatření na základě ***plánu řízení rizik*** (podkapitola 4.3) pro zvýšení bezpečnosti provozu metra.

6 Výsledky, jejich interpretace a posouzení

Následující kapitola obsahuje výsledky použití metod a nástrojů z kapitoly 4.2. Níže uvedené výsledky byly dále prezentovány v [3]. Procesní postup v rámci aplikace dat je následující:

1. interpretace výsledků pomocí matic citlivostí a jejich analýza,
2. transformace matic citlivostí do grafu za použití aparátu teorie grafů,
3. analýza scénáře dopadů na vybranou kritickou pohromu.

6.1 Interpretace a vyhodnocení výsledků získaných pomocí matic citlivostí

Data získaná studiem systému metra a jeho chování jsou zobrazena pomocí matic citlivostí v souladu s kapitolou 4.2. Matice, která obsahuje všechna kritická aktiva, pohromy a jejich vazby, je velmi rozsáhlá a nečitelná, a proto je rozdělená do několika dílčích matic dle:

- skupin aktiv,
- citlivostí (aktiva, pohromy),
- typu pohrom (relevantní, specifické, kritické),
- úrovně řízení L1-5.

Aby bylo možné zachytit závislosti mezi aktivy různých skupin, je vytvořena zvlášť matice, která zahrnuje pouze aktiva, která jsou na sobě silně závislá a jejichž vazby mají výrazný vliv na bezpečnost – tj. aktiva ve skupině Vazby a toky.

6.1.1 Matice citlivostí – vnější citlivost (zranitelnost vůči pohromám)

Matice vstupních parametrů obsahuje vnější události, přesněji změny okolních podmínek (výskyt pohrom). Následující vztahy v (27) definují pomocí matic množinu pohrom kritických $\boldsymbol{P_k}$ a specifických $\boldsymbol{P_s}$.

Matice (28-30) ukazují odchylku ve výstupní funkci skupiny aktiv $\boldsymbol{\Delta_L A_{(Pk)\vee(Ps\setminus k)}}$ (dle Tabulky 13) v závislosti na specifických pohromách. Předmětná odchylka výstupní funkce skupiny aktiv vyplývá z matice absolutních citlivostí $\boldsymbol{S}$ (na základě dat z [1,4,7]) a výskytu pohromy $\boldsymbol{P}$ ve formě odchylky od normálního stavu $\boldsymbol{\Delta_L P_{(k)\vee(s\setminus k)}}$, kde

L v indexu označuje uvažovanou úroveň systému řízení bezpečnosti a ***"k"*** nebo ***"s\k"*** kategorizaci pohrom (kritická nebo specifická) dle vztahu (27).

$$\boldsymbol{P_K} = \begin{pmatrix} \boldsymbol{PZ01} \\ \boldsymbol{PZ04} \\ \boldsymbol{PL01} \\ \boldsymbol{PL02} \\ \boldsymbol{PL06} \\ \boldsymbol{PL07} \\ \boldsymbol{PL08} \\ \boldsymbol{PL09} \\ \boldsymbol{PP03} \\ \boldsymbol{PP04} \\ \boldsymbol{PP06} \\ \boldsymbol{PP09} \\ \boldsymbol{PS01} \\ \boldsymbol{PI01} \\ \boldsymbol{PI03} \\ \boldsymbol{PI04} \end{pmatrix}; \boldsymbol{P_{S\backslash K}} = \begin{pmatrix} \boldsymbol{PZ02} \\ \boldsymbol{PL03} \\ \boldsymbol{PL04} \\ \boldsymbol{PL05} \\ \boldsymbol{PP07} \\ \boldsymbol{PS02} \\ \boldsymbol{PS03} \\ \boldsymbol{PS05} \end{pmatrix}; \boldsymbol{P_S} = \boldsymbol{P_K} \vee \boldsymbol{P_{S\backslash K}} \tag{27}$$

Pro považovanou úroveň řízení bezpečnosti Lx je uvažována pohroma ***P*** o takové velikosti, která je schopna vyžadovat aktivaci vyšší úrovně řízení bezpečnosti Lx+1. Výsledkem jsou matice:

$$\begin{pmatrix} \boldsymbol{\Delta_{L1}AK_{Pk}} \\ \boldsymbol{\Delta_{L1}AT_{Pk}} \\ \boldsymbol{\Delta_{L1}AP_{Pk}} \\ \boldsymbol{\Delta_{L1}AM_{Pk}} \\ \boldsymbol{\Delta_{L1}AF_{Pk}} \\ \boldsymbol{\Delta_{L1}AV_{Pk}} \\ \boldsymbol{\Delta_{L1}AO_{Pk}} \end{pmatrix} = \begin{pmatrix} \mathbf{1100111111011111} \\ \mathbf{1100111111011111} \\ \mathbf{1133111111011110} \\ \mathbf{1100111111011111} \\ \mathbf{1100111111111111} \\ \mathbf{1100111111111111} \\ \mathbf{1111111111111111} \end{pmatrix} \cdot \boldsymbol{\Delta_{L1}P_k}; \begin{pmatrix} \boldsymbol{\Delta_{L1}AK_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L1}AT_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L1}AP_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L1}AM_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L1}AF_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L1}AV_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L1}AO_{Ps\backslash k}} \end{pmatrix} = \begin{pmatrix} \mathbf{11111001} \\ \mathbf{11111111} \\ \mathbf{11110111} \\ \mathbf{11111111} \\ \mathbf{11111001} \\ \mathbf{11111111} \\ \mathbf{11111001} \end{pmatrix} \cdot \boldsymbol{\Delta_{L1}P_{S\backslash K}} \tag{28}$$

$$\begin{pmatrix} \mathbf{\Delta_{L2}AK_{Pk}} \\ \mathbf{\Delta_{L2}AT_{Pk}} \\ \mathbf{\Delta_{L2}AP_{Pk}} \\ \mathbf{\Delta_{L2}AM_{Pk}} \\ \mathbf{\Delta_{L2}AF_{Pk}} \\ \mathbf{\Delta_{L2}AV_{Pk}} \\ \mathbf{\Delta_{L2}AO_{Pk}} \end{pmatrix} = \begin{pmatrix} \mathbf{1100211122012212} \\ \mathbf{1200233233031233} \\ \mathbf{1133222222011211} \\ \mathbf{1200222222011212} \\ \mathbf{1100211211111212} \\ \mathbf{1122211211211212} \\ \mathbf{1122111211111312} \end{pmatrix} \cdot \mathbf{\Delta_{L2}P_k}; \begin{pmatrix} \mathbf{\Delta_{L2}AK_{Ps\backslash k}} \\ \mathbf{\Delta_{L2}AT_{Ps\backslash k}} \\ \mathbf{\Delta_{L2}AP_{Ps\backslash k}} \\ \mathbf{\Delta_{L2}AM_{Ps\backslash k}} \\ \mathbf{\Delta_{L2}AF_{Ps\backslash k}} \\ \mathbf{\Delta_{L2}AV_{Ps\backslash k}} \\ \mathbf{\Delta_{L2}AO_{Ps\backslash k}} \end{pmatrix} = \begin{pmatrix} \mathbf{12111111} \\ \mathbf{22333212} \\ \mathbf{11222221} \\ \mathbf{12222111} \\ \mathbf{12112111} \\ \mathbf{12112321} \\ \mathbf{12112112} \end{pmatrix} \cdot \mathbf{\Delta_{L2}P_{S\backslash K}} \tag{29}$$

$$\begin{pmatrix} \boldsymbol{\Delta_{L3}AK_{Pk}} \\ \boldsymbol{\Delta_{L3}AT_{Pk}} \\ \boldsymbol{\Delta_{L3}AP_{Pk}} \\ \boldsymbol{\Delta_{L3}AM_{Pk}} \\ \boldsymbol{\Delta_{L3}AF_{Pk}} \\ \boldsymbol{\Delta_{L3}AV_{Pk}} \\ \boldsymbol{\Delta_{L3}AO_{Pk}} \end{pmatrix} = \begin{pmatrix} \mathbf{2300331222013312} \\ \mathbf{3300333233032333} \\ \mathbf{2333333233023321} \\ \mathbf{2200333222012312} \\ \mathbf{3100221222221223} \\ \mathbf{3122321222321323} \\ \mathbf{2122222211221312} \end{pmatrix} \cdot \boldsymbol{\Delta_{L3}P_k}; \begin{pmatrix} \boldsymbol{\Delta_{L3}AK_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L3}AT_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L3}AP_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L3}AM_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L3}AF_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L3}AV_{Ps\backslash k}} \\ \boldsymbol{\Delta_{L3}AO_{Ps\backslash k}} \end{pmatrix} = \begin{pmatrix} \mathbf{12221112} \\ \mathbf{23333323} \\ \mathbf{23333333} \\ \mathbf{13332222} \\ \mathbf{12112112} \\ \mathbf{23122322} \\ \mathbf{23112113} \end{pmatrix} \cdot \boldsymbol{\Delta_{L3}P_{S\backslash K}} \tag{30}$$

Z uvedených matic citlivostí určíme nejcitlivější (nejzranitelnější) skupiny aktiv. Na první pohled ze vztahu (28) lze například usuzovat, že je nejzranitelnější personál v rámci epidemických / pandemických událostí; tj. řádek $\Delta_{L1}AP_{Pk}$ (značí skupinu aktiv personál), 3. a 4. sloupec vyjadřující dle (27) ***PL1*** (epidemie) a ***PL2*** (pandemie).

V případě úrovně L1 jde pouze o lokální přenosy infekcí na člověka, tj. na personál, který v případě nákazy se může chovat nepředvídatelně a v důsledku nedostatku může způsobit selhání. Z uvedeného důvodu má daná pohroma navíc dopad i na organizační aktiva označená ***AO*** s nižší zranitelností. Uvedená událost je pouze částečně ošetřena základními hygienickými pravidly zavedenými v dopravním systému metra.

Vzhledem k tomu, že se jedná pouze o skupiny aktiv, resp. rozsáhlé množiny dílčích aktiv, nelze jednoduše určit jednotlivé kritičnosti, a tím i nejkritičtější místa. V daném případě jsou ovšem vhodné následující operace:

Součet řádků – Celková zranitelnost skupiny aktiv na pohromy.

Následující výsledky jsou uvedeny pro součty řádků citlivostních matic pro tři úrovně systému řízení bezpečnosti (SMS) L1 až L3 a pohromy specifické P_s i kritické, tj. $P_k \cup P_{s \setminus k}$.

$$\sum_{i=1}^{n} \begin{pmatrix} s_{[1i]} \\ s_{[2i]} \\ s_{[3i]} \\ s_{[4i]} \\ s_{[5i]} \\ s_{[6i]} \\ s_{[7i]} \end{pmatrix} = \begin{pmatrix} 13 \\ 13 \\ 18 \\ 3 \\ 14 \\ 14 \\ 16 \end{pmatrix} + \begin{pmatrix} 6 \\ 8 \\ 7 \\ 8 \\ 6 \\ 8 \\ 6 \end{pmatrix} = \begin{pmatrix} 19 \\ 21 \\ 25 \\ 11 \\ 20 \\ 22 \\ 22 \end{pmatrix}; proL1aP_S \tag{31}$$

$$\sum_{i=1}^{n} \begin{pmatrix} s_{[1i]} \\ s_{[2i]} \\ s_{[3i]} \\ s_{[4i]} \\ s_{[5i]} \\ s_{[6i]} \\ s_{[7i]} \end{pmatrix} = \begin{pmatrix} 19 \\ 32 \\ 26 \\ 22 \\ 18 \\ 23 \\ 22 \end{pmatrix} + \begin{pmatrix} 9 \\ 18 \\ 13 \\ 12 \\ 10 \\ 13 \\ 11 \end{pmatrix} = \begin{pmatrix} 28 \\ 40 \\ 39 \\ 34 \\ 28 \\ 36 \\ 33 \end{pmatrix}; proL2aP_S \tag{32}$$

$$\sum_{i=1}^{n} \begin{pmatrix} s_{[1i]} \\ s_{[2i]} \\ s_{[3i]} \\ s_{[4i]} \\ s_{[5i]} \\ s_{[6i]} \\ s_{[7i]} \end{pmatrix} = \begin{pmatrix} 28 \\ 37 \\ 40 \\ 28 \\ 27 \\ 34 \\ 28 \end{pmatrix} + \begin{pmatrix} 12 \\ 22 \\ 23 \\ 18 \\ 11 \\ 17 \\ 14 \end{pmatrix} = \begin{pmatrix} 40 \\ 59 \\ 63 \\ 46 \\ 38 \\ 51 \\ 42 \end{pmatrix}; proL3aP_S \tag{33}$$

Ze vztahů (31) až (33) vyplývá, že nejcitlivější, resp. nejzranitelnější na specifické (zároveň i na kritické) pohromy je personál, a to téměř ve všech úrovních řízení – systému řízení bezpečnosti (SMS). Předmětný výsledek je v souladu s údaji a výsledky získanými pro ostatní technická díla [24]. Pouze pro L2 o jeden citlivostní bod ho převyšuje skupina technologických aktiv, což může být dáno například tím, že v případě abnormálních podmínek se dle používaných postupů (norem) stále spoléhá na standardní technologie provozu bez vyšších požadavků na jejich bezpečnost.

Součet sloupců – Rozsah potenciálních dopadů pohromy podle zranitelnosti skupiny aktiv (pro lepší čitelnost jsou hodnoty v maticích níže oddělené čárkou).

$$\sum_{i=1}^{m}\left(s_{[i1]} \dots s_{[i24]}\right) = (7,7,4,4,7,7,7,7,7,7,3,7,7,7,7,6,7,7,7,7,6,4,4,7); proL1 \wedge P_S \quad (34)$$

$$\sum_{i=1}^{m}\left(s_{[i1]} \dots s_{[i24]}\right) = (7,9,7,7,13,11,11,13,12,12,4,9,8,15,9,14,8,14,11,11,14,11,9,9); proL2 \wedge P_S \quad (35)$$

$$\sum_{i=1}^{m}\left(s_{[i1]} \dots s_{[i24]}\right) = (17,14,7,7,20,19,14,14,15,15,7,13,13,21,12,16,11,19,14,15,15,15,12,17); proL3 \wedge P_S \quad (36)$$

$$max\left[\sum_{i=1}^{m}\left(s_{[i1]} \dots s_{[i24]}\right)(L2), \sum_{i=1}^{m}\left(s_{[i1]} \dots s_{[i24]}\right)(L3)\right] = (15,21); i = 7. \quad (37)$$

Nejvyšší rozsah dopadů na aktiva bude mít v uvedeném případě dle výpočtu (37) čtrnáctý součet pro L2. Na čtrnáctém místě je dle vztahu (34) až (36) pohroma ***PI01***, tj. selhání antropogenního řízení označované v dnešní praxi jako organizační havárie. Z výše uvedeného výpočtu vyplývá, že právě organizační havárie ovlivňují nejvíce aktiv; z toho vyplývá, že na selhání lidského faktoru v oblasti řízení jsou téměř všechna aktiva zranitelná.

Z výsledků pro součet sloupců vyplývá, že u některých specifických pohrom se vyskytují vyšší hodnoty nežli u pohrom kritických. Předmětný údaj je důsledkem množství dotčených aktiv, resp. jejich skupin. Pro určení kritičnosti je nutné zvážit také důležitost aktiva ve skupině pro danou úroveň systému řízení bezpečnosti SMS, což bude předmětem další podkapitoly.

6.1.2 Hodnocení vazeb – vnitřní citlivost (zranitelnost vůči výpadku okolních aktiv)

Scénáře selhání aktiva při výpadku okolních aktiv sledujeme podle zranitelností Vazeb a toků, tj. na základě analýzy dat o provozu metra a dat o technické struktuře metra. Výsledky výzkumu [7] získané za pomocí expertů pro vazby a toky a aktiva, která jsou jimi dotčená (uvedená v příloze C) převedeme do vyjádření pomocí matic citlivosti. Při sestavování matic citlivostí uvažujeme celou množinu ***AVx*** (“Vazby a toky”, uvedené v příloze C) se vnější citlivostí resp. zranitelností na odchylku ve funkci (resp. ztrátu funkce) okolích aktiv označují symbolem ***Sm(AVx)*** a sjednocení množin vázaných okolních aktiv se označuje $\boldsymbol{Ax_x}$, vztahy (38).

$$\mathbf{AV_x} = \begin{pmatrix} \mathbf{AVi01} \\ \mathbf{AVi02} \\ \mathbf{AVi03} \\ \mathbf{AVi04} \\ \mathbf{AVi05} \\ \mathbf{AVi06} \\ \mathbf{AVi07} \\ \mathbf{AVi08} \\ \mathbf{AVi09} \\ \mathbf{AVi10} \\ \mathbf{AVe01} \\ \mathbf{AVe02} \\ \mathbf{AVe03} \\ \mathbf{AVe04} \\ \mathbf{AVe05} \\ \mathbf{AVe06} \\ \mathbf{AVm01} \\ \mathbf{AVm02} \\ \mathbf{AVm03} \\ \mathbf{AVm04} \end{pmatrix}; \sum \mathbf{Sm}\,(\mathbf{AV_x}) = \begin{pmatrix} \mathbf{2,5} \\ \mathbf{2,5} \\ \mathbf{2,5} \\ \mathbf{3} \\ \mathbf{2} \\ \mathbf{3} \\ \mathbf{2,5} \\ \mathbf{2,5} \\ \mathbf{2} \\ \mathbf{2} \\ \mathbf{2,5} \\ \mathbf{2} \\ \mathbf{2} \\ \mathbf{2,5} \\ \mathbf{2} \\ \mathbf{2} \\ \mathbf{3} \\ \mathbf{2,5} \\ \mathbf{2} \\ \mathbf{3} \end{pmatrix}; \mathbf{Ax_x} = \begin{pmatrix} \mathbf{AKk01} \\ \mathbf{AKk02} \\ \mathbf{AKk04} \\ \mathbf{AKk05} \\ \mathbf{AKk06} \\ \mathbf{AKk07} \\ \mathbf{AKs01} \\ \mathbf{AKs02} \\ \mathbf{AKs03} \\ \mathbf{AKs05} \\ \mathbf{ATdp01} \\ \mathbf{ATdz} \\ \mathbf{ATe} \\ \mathbf{ATis01} \\ \mathbf{ATkt} \\ \mathbf{ATv} \\ \mathbf{ATvk} \\ \mathbf{ATzb} \\ \mathbf{APd01} \\ \mathbf{APd02} \\ \mathbf{APdii01} \\ \mathbf{APdii02} \\ \mathbf{APdii03} \\ \mathbf{APdii04} \\ \mathbf{APs01} \\ \mathbf{APs02} \\ \mathbf{APs03} \\ \mathbf{APto02} \\ \mathbf{APto06} \\ \mathbf{AMtp03} \\ \mathbf{AMtp04} \\ \mathbf{AMov01} \\ \mathbf{AOzs01} \\ \mathbf{AMv01} \\ \mathbf{AMv02} \\ \mathbf{AMn01} \\ \mathbf{AMn02} \\ \mathbf{AMn03} \end{pmatrix} \tag{38}$$

Podle výše zmíněného postupu nejprve zkonstruujeme matici citlivostí s neznámými parametry s_{mn}, které reprezentující vazby, a tam kde dané aktivum vazbu nemá, zapíšeme 0; vztah (39).

$$\Delta AV_x = \begin{pmatrix} 0000000000000000S00SSSSSSSS000000000 \\ 0000000000000000S00S000SSS00000S00000 \\ 00000000000S000S000000000000000000000 \\ 000000000S000000SSSS0000000000000000 \\ 0000000000000000S00S0000S000000000000 \\ 00000000000000S0000S0000S000000000000 \\ 0000000000000000SS000S000000000000000 \\ 000000000S00000S000S000000000000000 \\ 0000000000000000S00S000000000000000 \\ 00000000000000000S000000000000000000 \\ 000000000000S000000000000000000000000 \\ S00000SS0000S000000000000000000000000 \\ SS0000SS0S00S000000000000000000000000 \\ 00000000S000S000000000000000000000000 \\ 000000S00000S000000000000000000000000 \\ 00000000000S000000000000000000000000 \\ 0000S0S00000S00S0000S0000S000S00000000 \\ 00000000S000S000S000000000000S0000000 \\ 00SS0000S000S000S000000000000S0000000 \\ 00000S00S00S000000000000S000000S0SSSS \end{pmatrix} \cdot \Delta Ax_x \qquad (39)$$

Z předchozích vztahů dosadíme číselné hodnoty zranitelností (citlivostí) na selhání okolních aktiv, tzn. vazeb. Z důvodu proveditelnosti, jelikož nemáme detailní výsledky výzkumu na rozdělení jednotlivých zranitelností na daná aktiva, rozdělíme zranitelnosti rovnoměrně:

S = Sm(AVx) / počet vazeb. (40)

To znamená například pro první řádek, že pro ***AVi01*** je dle (38) zranitelnost 2,5 [7], ve vztahu (38) se nám citlivostní koeficient ***S*** vyskytuje desetkrát čili dle vzorce (40) pro každé ***S*** píšeme 0,25. Výsledná matice je znázorněna ve vztahu (41).

Matice (41) ukazuje jednotlivé citlivosti, a tam, kde je číslo vyšší, a to zejména >1, by měla být soustředěna pozornost, jelikož jde o nejzranitelnější vazby. S odvoláním na teorii citlivostí a větu o invarianci citlivostí [89], předmětné veličiny je třeba patřičně ošetřit, a to buď převedením funkce vazby na jiná méně zranitelná místa, resp. zavést nové redundantní vazby, kterými se citlivost sníží, aniž by se měnila

výstupní funkce. V technické praxi [6,24,41] se obvykle v daných případech u důležitých technologií vkládají do systému zálohy.

$$\Delta AV_x = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,25 & 0 & 0 & 0,25 & 0,25 & 0,25 & 0,25 & 0,25 & 0,25 & 0,25 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,42 & 0 & 0 & 0,42 & 0 & 0 & 0 & 0,42 & 0,42 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1,25 & 0 & 0 & 1,25 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,6 & 0 & 0,6 & 0,6 & 0,6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,67 & 0 & 0 & 0 & 0 & 0,67 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1,250 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2,5 & 0 & 0 & 0,5 & 0 & 0 & 0,33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,83 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,6 & 0 & 0 & 0 & 0 & 0,33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,6 & 0 & 0 & 0 & 0 & 0,6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,5 & 0,5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0,5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,5 & 0,5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0,33 & 0,33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,33 & 0,33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1,25 & 0 & 0 & 1,25 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,43 & 0 & 0 & 0,43 & 0 & 0 & 0,43 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,63 & 0 & 0 & 0,63 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0,33 & 0,33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,33 & 0 & 0 & 0,33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0,43 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0,43 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0,3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \cdot \Delta Ax_x \tag{41}$$

Vzhledem k větě o invarianci citlivostí [89] lze konstatovat, že systém s rovnoměrně rozdělenými citlivostními koeficienty je nejstabilnější, a podle toho lze systém optimalizovat. Aktivum, které je závislé pouze na jedné vazbě, je nutné dále ošetřit, a to buď najít zanedbanou vazbu anebo připojit vazbu redundantní.

U koeficientů s nižším číslem a větším rozdělení jsme se dopustili velké nepřesnosti, protože nevíme, na které vazbě dané aktivum závisí více a na které méně a také neanalyzujeme společné příčiny a vazby. Vzhledem k množství aktiv, vazeb a možných pohrom (událostí) není možné udělat přesnější rozdělení pro všechna aktiva a pohromy. Proto je nutné použít další metody, např. metodu FTA (Fault Tree Analysis) [23] nebo analýzu grafů, uvedenou v následující podkapitole zohledňující nejen zranitelnost, ale i důležitost pro nejkritičtější místa, tj. prioritní rizika a zároveň výsledky ověřit diskusí s experty.

6.1.3 Hodnocení vybraných aktiv – řetězení matic citlivostí

Pro detailní studium jsme zvolili ***AVm01***, jako jednu z nejkritičtějších vazeb systému [7], a to ventilaci – distribuci vzduchu, a návazná aktiva mající přímý vliv na uvedené aktivum [5,7]. Vnitřní zranitelnost aktiva je dle vztahu (38) ***Sm(AVm01) = 3*** [7]. Hodnoty zranitelností pro ostatní aktiva jsou převzatá z neveřejné části výsledků výzkumu [5,7]. tj. vztah (42).

$$\sum \boldsymbol{S_m^{AVm01}} \begin{pmatrix} \boldsymbol{AKs01} \\ \boldsymbol{AKk06} \\ \boldsymbol{ATv} \\ \boldsymbol{AVi06} \\ \boldsymbol{ATe} \\ \boldsymbol{AMtp03} \end{pmatrix} = \begin{pmatrix} \mathbf{2} \\ \mathbf{2,5} \\ \mathbf{3} \\ \mathbf{3} \\ \mathbf{2,5} \\ \mathbf{3} \end{pmatrix}; \sum \boldsymbol{S_m^{AVi06}} \begin{pmatrix} \boldsymbol{APdii02} \\ \boldsymbol{ATv} \\ \boldsymbol{ATzb} \end{pmatrix} = \begin{pmatrix} \mathbf{2} \\ \mathbf{3} \\ \mathbf{2,5} \end{pmatrix} \tag{42}$$

Zranitelnost ***AVm01*** lze interpretovat citlivostí, kde citlivostní matice při rovnoměrně rozložené citlivosti vypadá následovně:

$$\boldsymbol{\Delta AV_{m01}} = (\mathbf{0, 50, 50, 50, 50, 50, 5}) \cdot \boldsymbol{\Delta} \begin{pmatrix} \boldsymbol{AKs01} \\ \boldsymbol{AKk06} \\ \boldsymbol{ATv} \\ \boldsymbol{AVi06} \\ \boldsymbol{ATe} \\ \boldsymbol{AMtp03} \end{pmatrix} \tag{43}$$

Aktivum ***AVi06*** je ze stejné skupiny, proto pokračujeme v jeho analýze:

$$\boldsymbol{\Delta AV_{i06}} = (\mathbf{111}) \cdot \boldsymbol{\Delta} \begin{pmatrix} \boldsymbol{APdii02} \\ \boldsymbol{ATv} \\ \boldsymbol{ATzb} \end{pmatrix} \tag{44}$$

Je zřejmé, že aktivum ***ATv*** (technologie vzduchotechniky) je společné, a proto při více společných vstupních aktivech lze matice spojit – zřetězit tak, aby byly společné vazby zřejmé.

$$\Delta \begin{pmatrix} \boldsymbol{AV_{m01}} \\ \boldsymbol{AV_{i06}} \end{pmatrix} = \begin{pmatrix} \mathbf{0,50,50,50,50,50,500} \\ \mathbf{0\ \ 0\ \ 1\ \ \infty\ \ 0\ \ 0\ \ 11} \end{pmatrix} \cdot \boldsymbol{\Delta} \begin{pmatrix} \boldsymbol{AKs01} \\ \boldsymbol{AKk06} \\ \boldsymbol{ATv} \\ \boldsymbol{AVi06} \\ \boldsymbol{ATe} \\ \boldsymbol{AMtp03} \\ \boldsymbol{APdii02} \\ \boldsymbol{ATzb} \end{pmatrix} \tag{45}$$

Nekonečno ve vztahu (45) znamená citlivost aktiva na změnu jeho samého. Další iterací může být zřetězení dalšího důležitého aktiva, kterým mohou být:

- společná aktiva (***ATv***),
- nejkritičtější aktiva (pro L1 až L3),
- jiná důležitá nebo zranitelná aktiva dle posouzení.

Kritičnost vyjádřit maticí lze, ale pro expertní posouzení se hůře analyzuje.

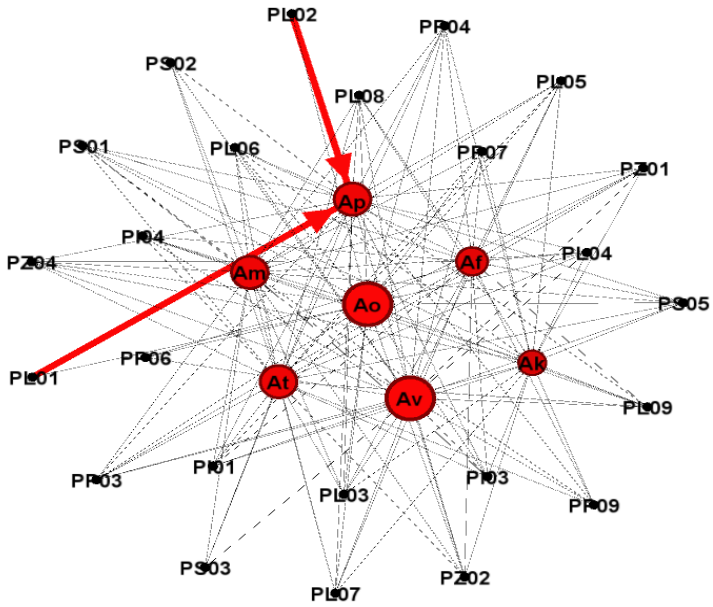
6.2 Transformace matic citlivostí do grafů a jejich vyhodnocení

Matice citlivostí zobrazují pouze zranitelnost a nezvažují důležitost ***D***, tj. nereprezentují kritičnost. Navíc při velkém množství aktiv, pohrom a jejich vzájemných vazeb a závislostí není rozsáhlá matice přehledná. Proto využíváme teorií grafů [91,92], ve které uvedené závislosti přehledně zobrazujeme. Navíc lze v grafech společně se zranitelností aktiv vyjádřit i jejich důležitost pro danou úroveň řízení bezpečnosti, a tím i jejich kritičnost.

6.2.1 Vyhodnocení vnějších citlivostí

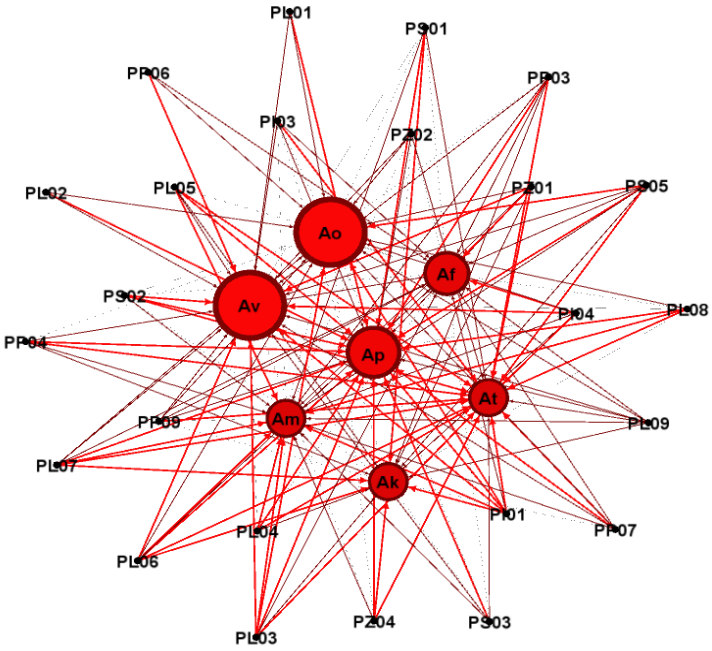
Pro analýzu vnější citlivosti jsou vstupními daty matice vyjádřené vztahy (28) až (30). Pro úroveň řízení L1 až L3 lze vnější citlivosti (tj. citlivost, resp. zranitelnost skupin aktiv na specifické pohromy) vyjádřit grafy, které jsou uvedeny na obrázcích 15-18.

Obrázek 15 pro úroveň řízení L1 jednoznačně ukazuje vazby ***PL01*** a ***PL02*** (epidemie a pandemie) ke skupině aktiv ***AP*** (personál). Na druhou stranu, skupiny ***AO*** (organizace a ekonomika) a ***AV*** (vazby a toky) se zobrazují jako největší, což znamená, že předmětné skupiny aktiv jsou citlivé (zranitelné) na větší množství událostí.

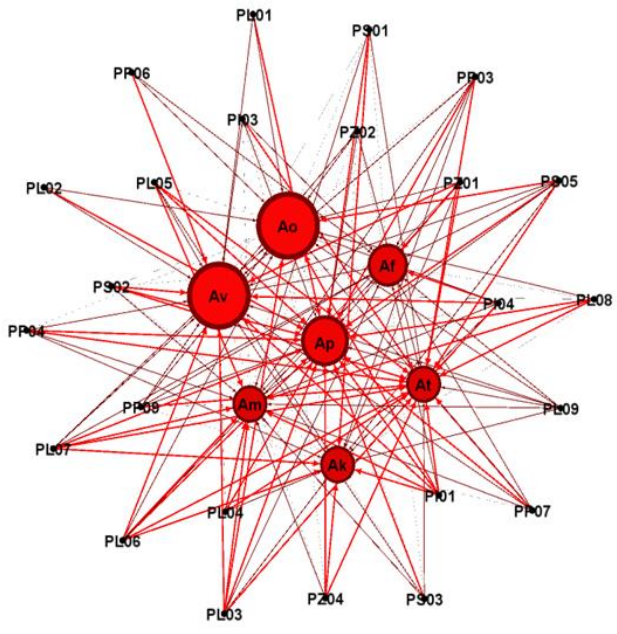


Obrázek 15. Graf vnějších citlivostí pro úroveň řízení L1. Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v odstavci 4.2.3, [3].

Citlivost skupin ***AO*** a ***AV*** se nemění ani pro úrovně řízení L2 a L3 (obrázky 16 a 17), ovšem vazby s větší zranitelností se pro úroveň řízení L2 od personálu přesouvají více ke skupině aktiv ***AT*** čili technologie a pro úroveň řízení L3 zpět k personálu.

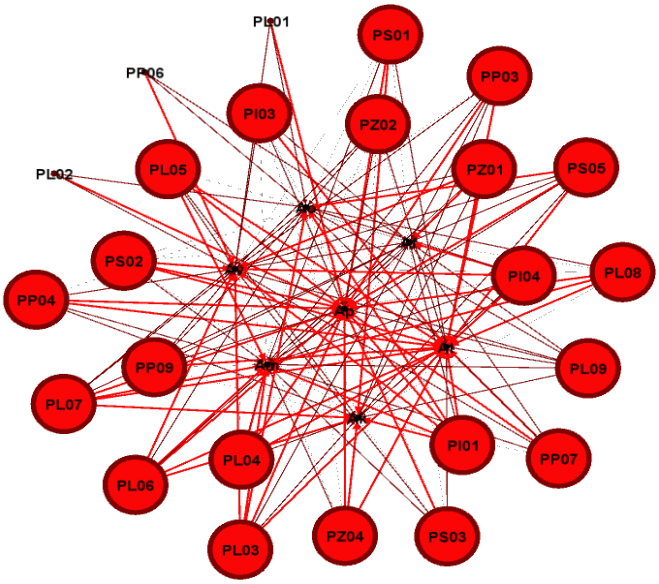


Obrázek 16. Graf vnějších citlivostí pro úroveň řízení L2. Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v odstavci 4.2.3, [3].



Obrázek 17. Graf vnějších citlivostí pro úroveň řízení L3. Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v odstavci 4.2.3, [3].

Pomocí grafů můžeme také zobrazit kritičnost pohromy, například pro úroveň řízení L3, standardní nastavení zobrazení grafu lze pozměnit tak, že pro uzly zvýrazníme stupeň ven. Výsledkem je graf znázorněný v následujícím obrázku 18.

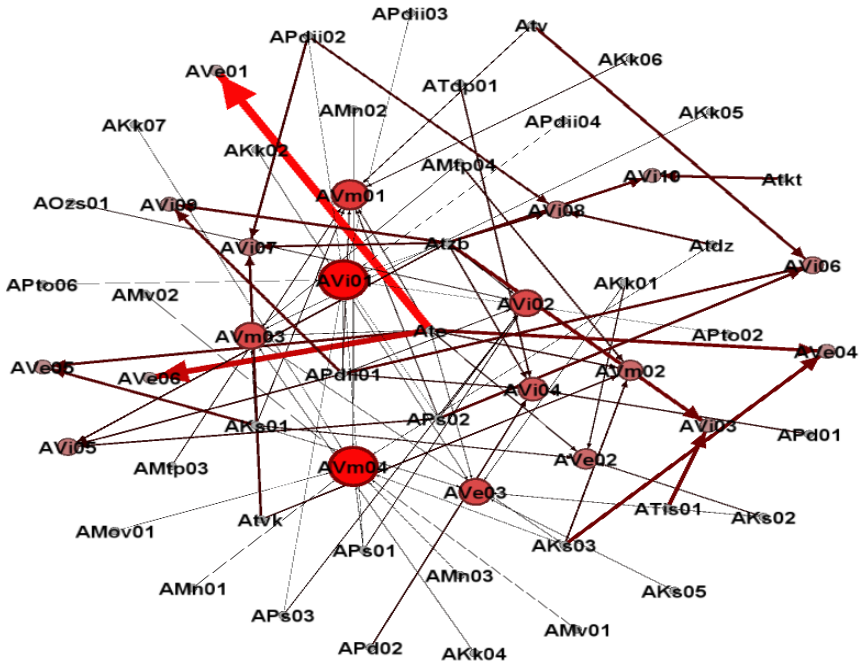


Obrázek 18 . Graf vnějších citlivostí pro úroveň řízení L3 – reverzní (stupeň ven). Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v odstavcích v odstavci 4.2.3 s modifikací pro zvýraznění uzlu s větším stupněm ven, tj. uzel, který má větší počet výstupních hran he větší a zbarven do červena, [3].

Z obrázku 18 vyplývá, že téměř všechny pohromy dopadají na stejný počet aktiv. Výjimkou jsou pohromy ***PL01*** a ***PL02*** (epidemie a pandemie), které přímo ovlivňují téměř jenom personál, a ***PP06*** (pohroma v územní infrastruktuře) mající vliv na funkce systémů a provozu, organizaci, a především na nejzranitelnější vazby a toky. Velmi výraznými uzly jsou ***PL03*** (stabilita lidské společnosti), ***PL04*** (kriminalita) a ***PL06*** (teroristický útok), které mají nejvyšší počet výstupních hran s nejvyšší vahou, tj. mají dopad na velký počet aktiv, která jsou na uvedené jevy nejvýše citlivá (zranitelná).

6.2.2 Hodnocení vnitřních citlivostí

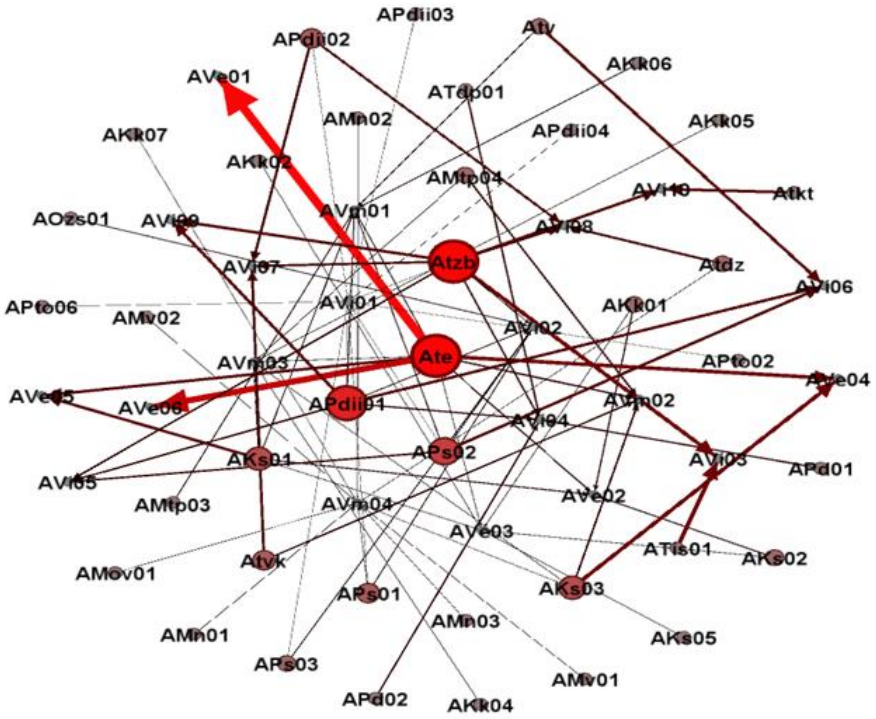
Pro hodnocení vnitřních citlivostí jsou vstupními daty údaje z matice ve vztahu (39). Obrázek 19 ukazuje výchozí zobrazení ve kterém se klade důraz především na aktiva ***AVi01, AVm04, AVm01***, která mají nejvíce vstupních vazeb. Předmětné vazby jsou slabé, tj. nemusí být uvedená aktiva nejzranitelnější (např. u ***AVi01*** jde o hodnotu 2,5 ze 3 [7]). ***AVm05 a AVm01*** se zranitelností na hodnotě 3 představují vyšší riziko.



Obrázek 19. Graf vnitřní citlivosti. Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v odstavci 4.2.3, [3].

V uvedeném případě je užitečné analyzovat i stupeň ven, jak je znázorněno na grafu v obrázku 18 v předchozím odstavci. Modifikací grafu na obrázku 19 na stupeň ven získáme graf uveden na obrázku 20.

Obrázek 20 ukazuje, že mnoho aktiv je zranitelných na výpadek aktiv ***Atzb, Ate, APdii01***, aj. Především u aktiva ***Ate*** jsou nejvíce ohodnocené hrany k ***AVe01, AVe06 a AVe04***. Aktivum ***AVe*** není samo od sebe nejzranitelnější, ale v daném případě závisí pouze na ***Ate,*** a proto se jeví jako jedno z nejkritičtějších aktiv pro skupinu Vazby a Toky.



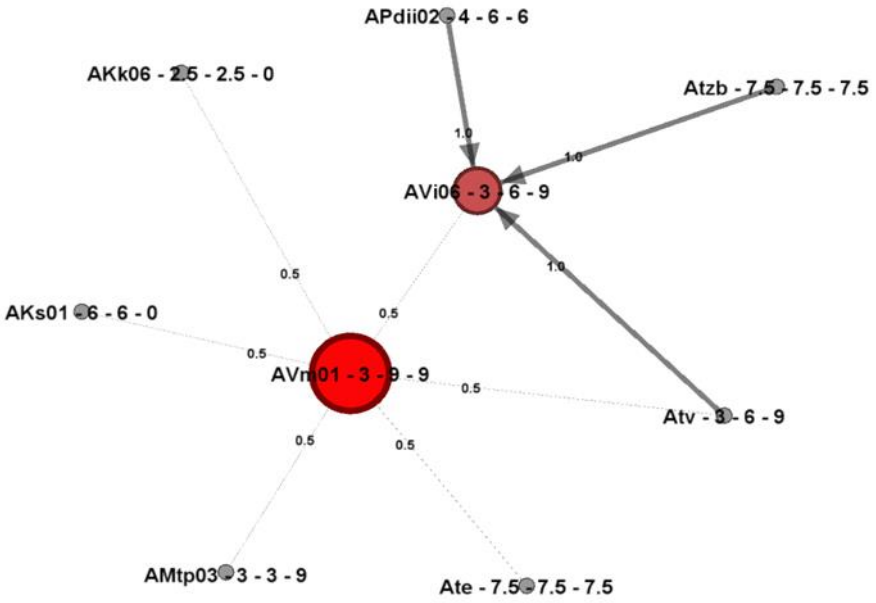
Obrázek 20. Graf vnitřní citlivosti – reverzní (stupeň ven). Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v odstavcích 4.2.3, [3].

Aktivum ***Ate*** (Technologie energetiky) má samo o době zranitelnost 2,5 [7] na všech úrovních řízení L1 až L3, dosahuje nejvyšších důležitostí, tedy kritičnost je pro všechny úrovně na hodnotě 7,5 [7]. Pro L1 a L2 se jedná o nejkritičtější ze skupiny technologií, pro úroveň řízení L3 je z důvodu své zranitelnosti kritičtější ze stejné skupiny vzduchotechnika a pohyblivé schody / plošin. Obdobně to je i pro ***Atzb*** (Signalizační, sdělovací a zabezpečovací technologie).

Z personálu je pro zajištění vazeb a toků jednoznačně nejkritičtější ***APdii01*** (vlakový dispečer), který se svojí zranitelností na hodnotě 2 je nejkritičtějším aktivem s kritičností 6 [7] (úrovně řízení L1 až L3) pro zajištění bezpečného provozu a v uvedeném případě zajištění vazeb a toků. Ze skupiny aktiv, personál má stejnou kritičnost pro úroveň řízení L1 strojvedoucí. Pro úrovně řízení L2 a L3 dále pak výpravčí a ostatní dispečeři.

6.2.3 Hodnocení vybraných aktiv

Pro hodnocení vybraných aktiv jsou vstupními daty matice z odstavce 6.1.3 a graf znázorněný na obrázku 14 v odstavci 4.2.3.2. Obrázek 21 ukazuje kritičnosti pro každý uzel, a to v pořadí Aktivum – kritičnost pro L1 – kritičnost pro L2 – kritičnost pro L3, a také váhy, stupně a ohodnocení hran.



Obrázek 21. Graf vybraných aktiv s vnitřními citlivostmi. Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v odstavcích 4.2.3.2 a 4.2.3.3 s textovým označením kritičností uzlů a citlivostí vazeb, [3].

Vzhledem ke kritičnosti aktiva ***AVm01*** pro úroveň řízení L1 není zapotřebí podrobnější analýzy. Za normálního provozu pro zajištění stejné úrovně bezpečnosti distribuce vzduchu se jeví jako kritická technologie energetiky (***Ate***) a konstrukce staveb tunelů (traťových, staničních a eskalátorových – ***AKs01***).

Pro úroveň řízení L2 mají vysoké kritičnosti aktiva:

- ***AVi06*** (tj. informační toky ohledně stavu vzduchotechniky), které je závislé na ***Ate*** (technologie vzduchotechniky, přímo ovlivňující distribuci vzduchu jako takovou),
- ***Atzb*** (signalizační, sdělovací a zabezpečovací technologie; především systém ASDŘ a SDM) a technologický dispečer.

Pro zabezpečení správné funkce uvedených aktiv v případě mimořádných událostí je zapotřebí snížit rizika jejich výpadku.

Pro úroveň řízení L3 se nepředpokládají výrazné změny ve stavbě (konstrukci tunelů a větracích šachet), pokud byla zajištěna jejich bezpečnost na nižších úrovní SMS (zajištění bezpečných staveb a konstrukcí), které by měli vliv na distribuci vzduchu. Nicméně na kritičnosti nabývá prostor okolo větracích šachet a jejich prostupnost pro distribuci čistého vzduchu (větrací šachty jako aktivum místa). Zároveň jsou na této úrovni velmi kritické technologie vzduchotechniky, tím i jejich informační toky pro případné řešení eskalace problému.

To znamená, že pro zabezpečení vzduchotechniky v případě mimořádných událostí a pohrom pro úroveň řízení L2 a více je nutné:

1. Zajistit místa větracích šachet a jejich prostupnost pro distribuci čistého vzduchu (a to i v případě aktivování tlakových uzávěrů, tj. znemožnění distribuce vzduchu skrze tunely).
2. Zaměřit se na funkčnost distribuce elektrické energie – Energie – technologie energetiky.
3. Zajistit funkčnost technologií vzduchotechniky.
4. Informační toky o stavu technologie vzduchotechniky a umožnit jejich řízení → tj.:
   - technologický dispečer,
   - technologie ASDŘ a SDM (resp. jejich alternativy – manuální řízení technikem na místě, včetně komunikačního zařízení pro spojení s dispečerem),
   - zajištění funkčnosti technologií (bod 3. výše).

6.3 Vybraný scénář dopadů

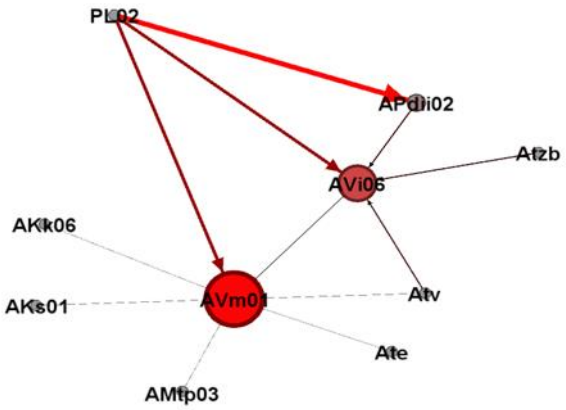
Uvedeme pouze zjednodušený příklad, a to scénář dopadů pandemie a plán odezvy na pandemii. Epidemie a pandemie působí primárně na lidi, tj. cestující a personál. V případě úrovně řízení L1 je nutné zajistit dostatečné personální obsazení a základní hygienická a preventivní opatření. U vyšších úrovních řízení se zvyšuje

riziko osobních selhání, organizačních havárií v případě nedostatku personálu a nákazy či šíření epidemie v provozu i mezi cestujícími.

Vzhledem k analýzám uvedeným v předchozích odstavcích lze tvrdit, že epidemie a pandemie neovlivňuje pouze lidi, ale také další aktiva z oblasti organizace a ekonomiky či vazeb a toků. Z technického hlediska, přímý dopad pandemie a epidemie na bezpečný provoz metra je zapříčiněn kontakty osob s kontaminovanými materiály, jedná se o povrchy či vzduch.

Zaměříme se především na distribuci vzduchu, kterou na základě uvedených analýz výše považujeme za jedno z nejkritičtějších aktiv. Graf vnitřních zranitelností distribuce vzduchu je uveden na obrázku 21 v předchozím odstavci. Původní graf rozšíříme o vnější zranitelnost ***PL02*** (pandemie), která lze z hlediska techniky považovat za totožnou s ***PL01*** (epidemie). Rozdíly z hlediska dopadů a možných opatření z okolí uvažovaného systému v tuto chvíli neuvažujeme, to by bylo předmětem analýzy pro vyšší úrovně systému řízení bezpečnosti SMS pro úrovně řízení L4 a L5.

Z rozšířeného grafu na obrázku 22 už je patrné, že je nejzranitelnější technologický dispečer (***APdii02***) jako hlavní aktivum pro informační toky ohledně stavu vzduchotechniky, ***PL01/02***, vzhledem k zajištění toku informací je nutné zabezpečit také zodpovědný technický personál ve vztahu k ***Atv*** a ***Atzb*** (tj. technici pracující na systému sdělovacího a řízení, a technologiích vzduchotechniky). Přímý vliv má pandemie i na distribuci vzduchu jako takového v případě jeho kontaminace.



Obr. 22. Graf vybraných aktiv s vnitřními citlivostmi a dopady epidemie/pandemie. Grafické vlastnosti hran a uzlů odpovídají údajům uvedeným v podkapitole 4.2.3, [3].

Na základě uvedených skutečností, plány odezvy na případ epidemie/pandemie v metru musí obsahovat plán pro zajištění čistého vzduchu, který obsahuje:

- zajistit základní hygienická preventivní opatření (ve formě zajištění prostředků, pravidel jejich používání, monitoringu/kontroly a jejich vynucení),
- nastavení pravidel pro monitoring a vyhodnocování situace,
- rozšířená hygienická opatření pro technologický dispečink – zajištění technologického dispečera,
- zajištění dostatečných personálních kapacit z hlediska dispečinku, komunikací a obsluhy vzduchotechnických zařízení,
- plány pro pravidelnou dekontaminaci – dezinfekce vstupu a výstupu, distribučních cest a stykových ploch konstrukcí, míst a technologií s personálem, popř. veřejností,
- případná další opatření pro veřejnost jako možný zdroj kontaminace.

6.4 Celkové vyhodnocení a návrh na snížení kritičnosti

Výše uvedené odstavce poskytují výsledky implementace teorie citlivostí, transformace citlivostních matic do grafu a analýzy grafů na základě dat získaných z předchozího výzkumu. Metody zavedené v této práci formalizují zápis platných souvislostí, které umožňují nalezení nejzranitelnějších a nejkritičtějších míst, ve kterých je potřeba provést opatření na zvládání prioritních rizik v rámci řízení bezpečnosti, která vedou ke zvýšení bezpečnosti uvažovaného sytému.

Prioritními riziky jsou následující slabá a kritická místa či vybrané pohromy:

1. Vnější citlivost, tj. zranitelnost vůči pohromám dle kapitoly 6.1.1:
   - nejcitlivější je personál pro úrovně řízení L1 a L3, i technologická aktiva pro úroveň řízení L2,
   - nejkritičtější pohromy jsou: epidemie a pandemie, které nejvíce postihují personál, který je na ně zranitelný již na úrovni řízení L1; organizační havárie, na které je zranitelné největší množství aktiv; teroristický útok.
2. Vnitřní citlivosti, tj. zranitelnost na výpadek funkce okolních aktiv dle kapitoly 6.1.2:

- nejcitlivější jsou vazby a energetické toky (napájecí systémy, distribuce elektrické energie k technologiím ve stanicích a nouzové napájecí systémy),
- na technologii energetiky je závislý největší počet aktiv.

Dle výsledků bezpečnostního výzkumu [7] (kapitola 5), největší kritičnost u Vazeb a toků má distribuce vzduchu, která je v disertační práci analyzovaná podrobněji.

Analýza grafu pro vnější citlivosti dle kapitoly 6.2.1 na rozdíl od analýzy matice citlivostí ukazuje vysokou kritičnost pohrom:

- destabilizace lidské společnosti,
- kriminalita,
- teroristický útok.

Na grafu mají uvedené pohromy nejvyšší počet výstupních hran s nejvyšší vahou, tj. mají dopad na velký počet aktiv, která jsou na uvedené jevy nejvýše citlivá (zranitelná). Destabilizace lidské společnosti a kriminalita jsou dle předchozích analýz pohromy specifické, tj. nespadají do kategorie kritických pohrom, ale vyžadují speciální pozornost.

Analýza grafu pro vnější citlivosti dle kapitoly 6.2.2 ukazuje, že:

- aktiva s nejvyšším počtem vstupních hran jsou informační toky, distribuce vzduchu a provozního materiálu; vzhledem ke kritičnosti uvedených aktiv je vhodné ověřit, zda jsou uvedené vazby redundantní nebo zda systém závisí na každé zvlášť,
- technologie zabezpečovacích zařízení, energetiky a vlakový dispečer jsou aktiva na kterých závisí nejvíce aktiv ze skupiny Vazby a toky,
- u personálu jsou vedle vlakového dispečera nejkritičtější: strojvedoucí, výpravčí a ostatní dispečeři.

Opatření pro snížení kritičnosti jsou následující.

1. Pro nejvíce kritická aktiva snížit jejich kritičnost zavedením redundancí a segmentaci tak, aby byla redundantní aktiva na sobě nezávislá.
2. Pro nejvíce kritická aktiva ošetřit společné příčiny selhání a snížit jejich zranitelnost (tj. zabezpečit vůči pohromám).
3. Pro ostatní kritická aktiva zavést plán řízení rizik (uvedený v odstavci 4.3),

4. Ošetřit relevantní pohromy dle jejich kritičností (relevantní, specifické, kritické), jak je uvedeno v odstavci 2.1.2.
5. Konkrétní opatření pro vybraný scénář dopadů uvedené v odstavci 6.3.

Odstavce 6.1, 6.2 a 6.3 jsou konkrétním příkladem aplikace uvedené metody pro hodnocení konkrétních aktiv a situací a pro zavedení možných opatření. Předmětné výsledky jsou založeny na datech získaných pomocí heuristických (expertních) metod, tj. což znamená, že získané výsledky nemusí být optimální, ale jsou mu blízké [23]. Proto výše uvedené výsledky byly předmětem další diskuse s experty na základě závěrečné zprávy [7].

Závěrem je třeba uvést, že výhodou maticového zápisu je přehledný matematický zápis a následné zpracování nezabírá mnoho místa. Předmětným způsobem lze provádět různé úlohy, např. hledat společnou zranitelnost aktiv. Například události epidemie a pandemie lze v nižších úrovních SMS považovat za stejnou pohromu, protože je řešíme lokálně pro zajištění provozu metra, ovšem u vyšších vrstev, a zejména v případě výskytu ohniska nákazy je pandemická událost na rozdíl od epidemie nadnárodním problémem. Nevýhodou maticových zápisů zůstává pouze jejich kodifikace, kde není na první pohled znatelné, který řádek a sloupec náleží k určitému vstupu a výstupu. Převedení formalizovaných maticových zápisů do grafu umožňuje další analýzu a interpretaci za pomocí využití teorie grafů.

7 Závěr

Kritická infrastruktura zajišťuje základní výrobky a služby pro lidi, proto je její bezpečnost a zabezpečení hlavním veřejným zájmem. Bezpečnost a zabezpečení provádíme metodami pro zajištění bezpečnosti technických děl a za pomocí systémů řízení založených na proaktivních přístupech a zvažování integrální bezpečnosti založené na principech a znalosti integrálních rizik. S ohledem na povahu systému systémů (SoS), který je předmětem řešení, specifik rozhraní dílčích systémů, tj. systémy socio-technické a kyber-fyzické, jsou systémy i systémy řízení bezpečnosti komplexní a zavádění dalších opatření a úhlů pohledu komplexitu zvyšují, a tím i možný vznik emergentních jevů, a to pozitivních i negativních.

Výsledky disertační práce cílím na zvýšení bezpečnosti metodou zvýšení znalosti o problémech a zranitelností. Zvyšování znalostí pozitivním způsobem ovlivňuje informační výkon, a tím vyšší pravděpodobnost včasného a správného rozhodnutí systému, a to zejména při kritické situaci. Proto jsem využil poznatky o informačních systémech a technologií a teorii informací, tj. obor, který prochází všemi rozhraními SoS a nevylučuje použití moderních přístupů a metod pro řízení bezpečnosti SoS.

Zvýšení znalosti jsem v disertační práci docílil rešerší sledovaného problému bezpečnosti a zabezpečení systémů (Kapitola 2), shrnutím dat o sledovaném systému (Kapitola 3) a návrhem metod pro identifikaci a analýzu aktiv KI a jejich kritičností, vhodnou interpretaci a metodu transformace pro následnou analýzu a určení scénářů dopadů vybraných událostí (Kapitola 4). Provedl jsem bezpečnostní výzkum provozu pražského metra s využitím navržených metod. Pro Dopravní podnik Praha jsem zpracoval jak metodiku na zjištění kritičnosti aktiv dopravního systému, tak předložil konkrétní výsledky pro metro. Praktické výsledky výzkumu ukazují na kritické vazby systémů, které mohou v provozu v různých úrovních řízení bezpečnosti způsobovat problémy. Proto uvedené vazby a jejich aktiva je v praxi nutné ošetřit plánem řízení rizik, ve kterém budou uvedena opatření podpořena zajištěním techniky, postupem provedení, personálem, odpovědnostmi a financemi. Pro vypracování uvedeného plánu předložená disertační práce poskytuje základ. Konkrétní výsledky z výzkumu byly předány Dopravnímu podniku hl. m. Prahy pro další použití při ošetření uvedených kritických míst a vazeb.

Disertační práce „Posouzení bezpečnosti vybraného kritického objektu z pohledu integrální bezpečnosti a návrh na snížení kritičnosti objektu“ popsanými výsledky svůj cíl splňuje v teoretické i praktické rovině, vede ke zvýšení znalosti v systémech řízení bezpečnosti a jejich úrovní na základě moderních proaktivních přístupů, a znalostí o aktivech a jejich vazbách v systému řízení bezpečnosti pro provoz metra. Výsledky disertační práce lze navíc prakticky více rozvinout s podporou využití SW nástrojů, vytvoření kontrolních seznamů, plánů řízení rizik i o další konkrétní vyhodnocení dalších scénářů dopadů pohrom. Tím práce poskytuje platformu pro další výzkum a vývoj.

Použitá literatura

[1] KERTIS, T., PROCHÁZKOVÁ, D. *Assets of Model Metro Station and Their Criticality.* Acta Polytechnica CTU Proceedings. IRICoN. ISSN 2336-5382. ISBN 978-80-01-06022-3. Praha: ČVUT 2016, s. 29-37.

[2] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti a udržitelného rozvoje území.* ISBN 978-80-7251-243-0. Praha: PA ČR 2007, 202 s.

[3] KERTIS, T., PROCHÁZKOVÁ, D. Aplikace teorie citlivosti pro zvýšení bezpečnosti kritické infrastruktury. *RRTD 2020*. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, s. 37-65.

[4] KERTIS, T. *Bezpečnostní plán vybrané stanice pražského metra. Diplomová práce*. Praha: ČVUT 2015, 95 s.

[5] KERTIS, T., PROCHÁZKOVÁ, D. Identification of Assets of Metro Operation in Praha and Determination of their Criticality. In: *Proceeding of the 29th European Safety and Reliability Conference*. Singapore: Research Publishing Services 2019. doi: 10.3850/978-981-11-2724-3_0621-cd

[6] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 978-80-01-06180-0, e-ISBN 78-80-01-06182-4. Praha: ČVUT 2017, 364 s. http://hdl.handle.net/10467/72582

[7] KERTIS, T. *Závěrečná zpráva – Bezpečnostní výzkum provozu pražského metra (2016-2021) (neveřejné)*. Praha: ČVUT 2021, 71 s.

[8] UN Human Security Unit. *Human Security in Theory and Practice*. New York: United Nations 2009. Dostupné z: https://www.undp.org/content/dam/turkey/docs/news-from-new-horizons/issue-41/UNDP-TR-HSHandbook_2009.pdf

[9] UN. *Human Development Report*. New York: UN 1994. Dostupné z: www.un.org.

[10] NOVOBÍLSKÝ, P., KERTIS, T., PROCHÁZKOVÁ, D. Cyber Security of Metropolitan Railway Communication Infrastructure. In: *Risk of Business and Territorial Processes*. ISBN 978-80-7561-021-8. Ústí nad Labem: FVTM UJEP 2016, s. 78-91.

[11] DPP. 2020 Dopravní podnik hlavního města Prahy, a.s. [online]. 2020 [cit. 2020-11-28]. Dostupné z: https://www.dpp.cz/spolecnost/o-spolecnosti/dpp-v-datech

[12] FEMA. *Guide for All-Hazard Emergency Operations Planning*. Washington, DC: FEMA 1996. Dostupné z: http://www.fema.gov/pdf/plan/slg101.pdf

[13] PROCHÁZKOVÁ, D. Metodika stanovení závažných živelných a jiných pohrom pro potřeby veřejné správy. V: *Fire Safety 2004*. ISBN 80-86634-43-4. Ostrava: VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, 2004, 78 s.

[14] PROCHÁZKOVÁ, D. *Krizové řízení pro technické obory*. ISBN 978-80-01-05292-1. Praha: ČVUT 2013, 303 s.

[15] ARCHIV HLAVNÍHO MĚSTA PRAHY. Archivní katalog [online]. 2020 [cit. 2020-11-28]. Dostupné z: http://www.ahmp.cz/

[16] KERTIS, T., PROCHÁZKOVÁ, D. Identifikace aktiv provozu pražského metra a stanovení jejich kritičností. *RRTD 2018*. ISBN 978-80-01-06515-0. Praha: ČVUT 2018, s. 92-108.

[17] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. ISBN:978-80-01-04841-2. Praha: ČVUT 2011, 405 s.

[18] KORECKÝ, M., TRKOVSKÝ, V. *Management rizik projektů*. ISBN 978-80-247-3221-3. Praha: Grada 2011, 583 s.

[19] KERTIS, T. Porovnání přístupů pro řízení bezpečnosti v dopravě. V: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN 978-80-01-06033-9. Praha: ČVUT 2016, s. 34-59.

[20] KERTIS, T., PROCHÁZKOVÁ, D. Tools for Risk Management of Model Metro Station. In: *Smart Cities Symposium Prague 2016*. ISBN 9781509011162. New York: IEEE 2016.

[21] PROCHÁZKOVÁ D. *Analýza, řízení a vypořádání rizik spojených s technickými díly*. ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 s. http://hdl.handle.net/10467/78442

[22] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Řízení rizik procesů spojených s provozem technického díla během jeho životnosti*. ISBN 978-80-01-06675-1.

Praha: ČVUT 2019, 465 s. http://hdl.handle.net/10467/85867, doi:10.14311/BK.9788001066 751

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

[24] NOVÁK, M., PŘENOSIL, V., SVÍTEK, M., VOTRUBA, Z. Spolehlivost hybridního systému. V: *Problémy spolehlivosti, životnosti a bezpečnosti systémů*. ISBN 80-903298-2-9. Praha: Neural Network World, 2005, s. 23-24.

[25] PROCHÁZKOVÁ, D. *Safety of Complex Technological Facilities*. ISBN 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing, 2015, 244 s.

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

[27] PROCHÁZKOVÁ, D., PROCHÁZKA, J., KERTIS, T. Bezpečnost složitých kritických technologických systémů. V: *Sborník z Mezinárodní konference Bezpečnostní technologie, systémy a management 2015*. ISBN 978-80-7454-559-7. Zlín: Univerzita Tomáše Bati ve Zlíně 2015, 240 s.

[28] ZAIRI, M. *Total Quality Management for Engineers*. ISBN 9781855730243 Cambridge: Woodhead Publishing Ltd, 1991, 192 s.

[29] PROCHÁZKA, T. *Spolupráce veřejného a soukromého sektoru*. Diplomová práce VŠFS, Praha 2008, 107 s.

[30] KERTIS, T., PROCHÁZKOVÁ, D. Plán řízení rizik spojených s provozem stanice metra. *Sborník z XXV. Mezinárodní vědecké konference soudního inženýrství*. ISBN 978-80-214-5321-0. Brno: VUT 2016, s. 399-416.

[31] GLENDON, I. A., et al. *Human Safety and Risk Management*. ISBN 0-8493-3090-4. Boca Raton: CRC Press 2006, 488 s.

[32] 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. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF

[33] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury*. ISBN: 978-80-01-05103-0. Praha: ČVUT v Praze 2012. 318 s.

[34] ČR. Zákon č. 240/2000, o krizovém řízení a o změně některých zákonů (krizový zákon). V: *Sbírka zákonů*. http://www.zakonyprolidi.cz/cs/2000-240

[35] ČR. Nařízení vlády č. 432/2010 Sb. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury. V: *Sbírka zákonů*. https://www.zakonyprolidi.cz/cs/2010-432

[36] IAEA. Assessment of Defence in Depth for Nuclear Power Plants. In: *Safety Report Series No. 46*. ISBN 92–0–114004–5. Vienna: IAEA, 2005, 119 s.

[37] IEC. ISA IEC 62443-4-1. Security for Industrial Automation and Control Systems, Part 4-1: Secure Product Development Lifecycle Requirements. Geneva: IEC 2018.

[38] INCOSE. [online]. 2020 [cit. 2020-12-23]. Dostupné z: https://www.incose.org/products-and-publications/sos-primerh

[39] BOARDMAN, J., SAUSER, B. System of Systems – the Meaning of of. V: *IEEE/SMC International Conference on System of Systems Engineering*. Los Angeles: CA, 2006. 6 s. doi: 10.1109/SYSOSE.2006.1652284

[40] KERTIS, T., PROCHÁZKOVÁ, D. Reduce of Criticality of Critical Infrastructure Facilities in the Railway Domain. V: *Smart Cities Symposium Prague 2015 Proceedings - Czech Technical University in Prague*. Praha: IEEE 2015. Str. 1-4. doi: 10.1109/SCSP.2015.7181565.

[41] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením technického díla a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 s. http://hdl.handle.net/10467/8446634

[42] IAEA. *IAEA Safety Glossary: 2018 Edition*. Vienna: IAEA 2018. 261 s. Dostupné z: https://www.iaea.org/publications/11098/iaea-safety-glossary-2018-edition

[43] PROCHÁZKOVÁ, D., KERTIS, T., PROCHAZKA, J., PROCHAZKA, Z. Železnice – jejich rizika a nástroje pro řízení bezpečnosti. V: *Řízení rizik procesů spojených s technickými díly*. ISBN 978-80-01-06515-0. Praha: ČVUT 2018, s. 128-169.

[44] BOSSEL, H. Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme. ISBN 3-8334-0984-3. Norderstedt/Germany: Books on Demand 2004, 400 s.

[45] PROCHÁZKOVÁ, D. *Study of Disasters and Disaster Management*. ISBN 978-80-01-05246-4. Praha: ČVUT 2013. 202 s.

[46] 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, 191 s.

[47] KERTIS, T., PROCHÁZKOVÁ, D. Description of Safety Management Systems in Transportation. V: *Journal of Environmental Protection, Safety, Education and Management Vol.5, No 9, June 2017*. ISSN 2453-9813 (Online) De Gruyter 2017, DOI https://doi.org/10.1515/jepsem-2017-0003

[48] KERTIS, T. Introduction of Modern Approaches of Ensuring Safety into Business Processes in Railway Industry. V*: Vybraná rizika podnikových procesů 2015.* ISBN 978-80-01-05831-2. Praha: ČVUT, s 26-38.

[49] ČR. ČSN EN ISO 9001:2015 (01 0321). *Systémy managementu kvality – Požadavky*. Praha: ÚNMZ 2016.

[50] ČR. ČSN EN 61508-1 ed. 2 (180301). *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky*. Praha: ÚNMZ, 2011.

[51] ČR. Zákon č. 181/2014, Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Sbírka zákonů.* http://www.zakonyprolidi. cz/cs/2014-181

[52] ČR. ČSN ISO/IEC 27000 (36 9790) *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: ÚNMZ, 2010

[53] IEC. IEC TS 62443-1-1:2009 *Industrial Communication Networks - Network and System Security - Part 1-1: Terminology, Concepts and Models*. ISBN 978-2-88910-710-0. Geneva: IEC 2009.

[54] ČR. ČSN ISO/IEC 15408-1 *Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a všeobecný model*. Praha: ČNI 2001.

[55] ČR. *Předpisy. Letecká informační služba* [online]. Praha: Řízení letového provozu České republiky. http://lis.rlp.cz/predpisy/predpisy/index.htm

[56] EU. *DIRECTIVE 2004/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive)*. Brussels: EC, 2002.

[57] EU. *Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 Text with EEA relevance*. Brussels: EC, 2013.

[58] ČR. *Vyhláška číslo 376/2006 Sb. o systému bezpečnosti provozování dráhy a železniční dopravy a postupech při vzniku mimořádných událostí na dráhách*. Dostupné z: https://www. zakonyprolidi.cz/cs/2006-376

[59] UNIFE. *IRIS International Railway Industry Standard*. Brussles: UNIFE, 2012. Dostupné z: http://www.iris-rail.org/

[60] ČR. ČSN EN 50126-1 (333502). *Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS) - Část 1: Generický proces RAMS.* Praha: ÚNMZ, 2019.

[61] ČR. ČSN EN 50129 (34 2675). *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Elektronické zabezpečovací systémy*. Praha: ČNI, 2003.

[62] ČR. ČSN EN 50128 ED.2 (34 2680). *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy*. Praha: ÚNMZ, 2012.

[63] KERTIS, T., PROCHÁZKOVÁ, D. Cyber Security of Underground Railway System Operation. V: *Smart Cities Symposium Prague (SCSP). Prague,*

25.05.2017 - 26.05.2017. ISBN 978-1-5386-3825-5. Praha: ČVUT 2017, s. 1-6.

[64] MOOS, P., MALINOVSKÝ, V. *Informační systémy a technologie.* ISBN 80-903298-5-3. Praha: ČVUT Fakulta dopravní. 2006.

[65] KERTIS, T., PROCHAZKOVA, D. Informační výkon a kybernetické příčiny dopravních nehod. V: *Řízení rizik procesů spojených s technickými díly. Praha, 07.12.2017*. ISBN 978-80-01-06351-4. Praha: ČVUT 2017, s. 44-59.

[66] VITOUS, M. Cobit 5 v malých a středních firmách. V: *IT Systems: specializovaný měsíčník o podnikové informatice*. Brno: CCB 2000.

[67] SVOBODA, V., SVÍTEK, M. *Telematika nad dopravními sítěmi*. ISBN 80-01-03087-3. Praha: ČVUT 2004, 263 s.

[68] PROCHÁZKOVÁ, D., SRP, J., PROCHÁZKA, J. Analysis of Cyber Networks in a System Concept. V: *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: Europment 2013, s. 102-109.

[69] MOOS, P., ZELINKA, T., MALINOVSKÝ, V. *Telekomunikační služby.* ISBN 978-80-01-03598-6. Praha: ČVUT 2007, 176 s.

[70] KERTIS, T., PROCHÁZKOVÁ, D. Parameters Strengthening Information Power Supporting the Rail Systems Safety. In: *Safety and Reliability – Safe Societies in a Changing World, Proceedings of ESREL 2018, June 17-21, 2018,* Trondheim Norway. London: CRC Press 2018. doi: https://doi.org/10.1201/9781351174664

[71] EU. *Projekt SESAMO: Security and Safety Modelling* [online]. ARTEMIS Joint Undertaking, c2012-2017 [cit. 2020-12-23]. Dostupné z: http://sesamo-project.eu/

[72] KOLEKTIV PRACOVNÍKŮ METROPROJEKTU PRAHA A. S. *Publikace IV. C2. 2008.* Praha: DISKUS DATASERVIS, spol. s r.o. 2008. Dostupné z: https://www.praha.eu/public/0/a3/da/186337_4_Publikace_IV._C2.pdf

[73] KERTIS, T., PROCHÁZKOVÁ, D. Impacts of Lacks in Design of Control Systems in Rail Transportation. V: *2018 Smart City Symposium Prague*

(SCSP), Prague, 2018, Praha: IEEE 2018. s. 1-6. DOI: 10.1109/SCSP.2018.8402668.

[74] CENELEC. EN 62290-1: *Railway Applications. Urban Guided Transport Management and Command/control Systems. System principles and fundamental concepts.* Brussels: EC for Electrotech. Standardization 2014.

[75] ČR. ČSN EN 62267 (333532) *Drážní zařízení – Automatizovaná městská doprava s vyhrazenou vodicí dráhou (AUGT) - Bezpečnostní požadavky*. Praha: ÚNMZ, 2010.

[76] ČR. ČSN EN 50159 (34 2670). *Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Komunikace v přenosových zabezpečovacích systémech.* Praha: ÚNMZ, 2011.

[77] KERTIS, T., PROCHÁZKOVÁ, D. Risk Management Plan for Metro Station. In: *Risk, Reliability and Safety. Innovating Theory and Practice. 26th European Safety and Reliability Conference ESREL 2016. Glasgow, 25.09.2016 - 29.09.2016*. ISBN 978-1-138-02997-2. Londýn: Taylor & Francis Group. 2017, s. 209-217.

[78] KERTIS, T., PROCHÁZKOVÁ, D. Judgement of Level of Integral Safety that Ensured the Risk Management Plan for Metro Station Operation. V: *Global Existential Risks. Bratislava, 15.11.2016*. ISBN 978-80-89753-10-9. Žilina: STRIX n.f., Žilina. 2017, s. 39-51.

[79] PROCHÁZKA, J., KERTIS, T., PROCHÁZKOVÁ, D. Zdroje rizik pro dopravu na železnici v ČR. In: *JuFos 2017. Junior Forensic Science Brno 2017. Brno, 16.04.2017.* ISBN 978-80-214-5486-6. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2017, s. 283-291.

[80] KERTIS, T., PROCHÁZKOVÁ, D. Railway Accidents in the Czech Republic, Causes of Risks and their Mitigation. V: *Safety and Reliability – Theory and Applications. ESREL 2017. Portoroz, 18.06.2017 - 22.06.2017*. ISBN 978-1-138-62937-0. London: Taylor & Francis. 2018, s. 1667-1673.

[81] KERTIS, T., PROCHÁZKOVÁ, D. Posouzení kritičnosti plánu řízení rizik pro metro. V: *Rizika podnikových procesů 2016. Děčín, 10.11.2016*. ISBN 978-80-01-06033-9. Praha: ČVUT v Praze, Fakulta dopravní, s. 60-75.

[82] KERTIS, T., PROCHÁZKOVÁ, D. Judgement of Conformity Level of Legislation with the Normative for Ensuring the Safety of Railway Systems from the perspective of Integral Safety. In: *ExFoS 2017 – Expert Forensic Science 2017*. Brno, 27.01.2017 - 28.01.2017. ISBN 978-80-214-5459-0. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství 2017, s. 368-374.

[83] PROCHÁZKOVÁ, D., PROCHÁZKA, J., KERTIS, T. Domains of Railway Traffic in the Czech Republic, which need the Safety Improvement. V: *Vol. 11 (2017): Modernization of Railway - IRICoN 2017*. Praha, 10.05.2017. ISBN 978-80-01-06297-5 (online). Praha: Acta Polytechnica CTU Proceedings 2017, s. 53-62. https://doi.org/10.14311/APP.2017.11.0053

[84] KERTIS, T., PROCHÁZKOVÁ, D., PROCHÁZKA, J., PROCHÁZKA, Z. Rizika spojená s provozem na železnici. V: *Sborník příspěvků konference Young Transportation Engineers Conference 2018*. ISBN 978-80-01-06464-1. Praha: ČVUT 2018, s. 1-9.

[85] VOTRUBA, Z., KALIKA, M., KLEČÁKOVÁ, J. *Systémová analýza.* ISBN 9788001040812. Praha: ČVUT 2004, 187 s.

[86] KNÁPEK, J. *Přednášky k předmětu Systémové inženýrství*. Praha: ČVUT 2012.

[87] BODE, H. W. *Network Analysis and Feedback Amplifier Design*. New York: Van Nostrand 1945. 551 s.

[88] GEHER, K. *Theory of Network Tolerances*. Budapest: Akademiai Kiado 1971, 184 s.

[89] GEHER, K. The Theory of Sensitivity Invariants and Their Application to Optimization of Tolerances and Noises. V: *Periodica Polytechnica*. Budapešť: Institute of Telecommunication and Electronics, Technical University Budapest 1974, s. 25-34.

[90] GAJDOŠÍK, L. *Počítačová identifikace obvodů. Studijní podpora*. ISBN 978-80-248-1483-4. Ostrava: VŠB-TUO 2007, 149 s.

[91] KOLÁŘ, J. *Grafy*. Praha: ČVUT 1984, 231 s.

[92] GEPHI – The Open Graph. Gephi.org. 2017. https://gephi.org/

[93] FRUCHTERMAN, T. M. J., & REINGOLD, E. M. Graph Drawing by Force-Directed Placement. V: *Software: Practice and Experience*. John Wiley & Sonns 1991, s. 1129-1164. https://doi.org/10.1002/spe.4380211102