ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ

Bc. Tomáš Kertis

Bezpečnostní plán vybrané stanice pražského metra

Diplomová práce

2015

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
d ě k a n
Konviktská 20, 110 00 Praha 1

K623 .....Ústav bezpečnostních technologií a inženýrství

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Tomáš Kertis

Kód studijního programu a studijní obor studenta:

N 3710 – LO – Logistika, technologie a management dopravy

Název tématu (česky): **Bezpečnostní plán vybrané stanice pražského metra**

Název tématu (anglicky): Security Plan of Selected Station of Praha Metro

Zásady pro vypracování

Při zpracování diplomové práce se řiďte osnovou uvedenou v následujících bodech:

- Úvod
- Soubor poznatků o rizicích a jejich dopadech na systémy
- Data o pražském metru a jeho řídícím systému
- Metody zpracování dat založené na rizikovém inženýrství
- Bezpečnostní plán
- Plán řízení rizik
- Závěr
- Seznam literatury

Rozsah grafických prací: dle doporučení vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: D. Procházková: Krizové řízení pro technické obory. ČVUT, Praha 2013; Analýza a řízení rizik. ČVUT, Praha 2011; Základy řízení bezpečnosti kritické infrastruktury. ČVUT, Praha 2013,; : Metody, nástroje a techniky pro rizikové inženýrství. ČVUT, Praha 2011; Bezpečnost kritické infrastruktury. ČVUT, Praha 2012, 318p.

Vedoucí diplomové práce: **doc. RNDr. Danuše Procházková, DrSc.**

Datum zadání diplomové práce: **30. června 2014**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **31. května 2015**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Ing. Václav Jirovský, CSc.
vedoucí
Ústavu bezpečnostních technologií a inženýrství

prof. Dr. Ing. Miroslav Svítek
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Tomáš Kertis
jméno a podpis studenta

V Praze dne..... 30. června 2014

Poděkování

Velmi rád děkuji všem, kteří mi jakkoliv pomohli při vypracování diplomové práce a přispěli svými radami a materiály během studia na vysoké škole. V první řadě děkuji rodičům a své přítelkyni za jejich podporu a trpělivost během studia.

Za poskytnutí odborných konzultací, cenných kontaktů a literatury děkuji vedoucí práce paní doc. RNDr. Danuši Procházkové, DrSc., a dále zaměstnancům Dopravního podniku hl. m. Prahy, Magistrátu hl. m. Prahy, Úřadu MČ Prahy 18 za poskytnuté podklady a konzultace.

Prohlášení

Předkládám tímto k posouzení a obhajobě diplomovou práci, zpracovanou na závěr 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 25. 5. 2015

.....

podpis

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

Bezpečnostní plán vybrané stanice pražského metra

DIPLOMOVÁ PRÁCE

Tomáš Kertis

květen 2015

Abstrakt

Předložená diplomová práce se soustřeďuje na zabezpečení kritické infrastruktury, která vytváří základnu pro kvalitní život a také pro přežití lidí za kritických podmínek. Na základě současného poznání se zabývá riziky spojenými s vybranou stanicí metra a stanovuje bezpečnostní plán na základě konceptu integrální bezpečnosti, který následně srovnává s dnešní praxí. Na základě posouzení shody identifikuje jevy, které mohou ohrozit předmětnou stanici a nejsou dosud z hlediska bezpečnosti řešeny. Ukazuje jejich dopady a pro případy závažných rizik navrhuje opatření a činnosti odezvy pro případ jejich výskytu.

Klíčová slova

Ochrana zdraví a majetku, bezpečnost státu, chráněná aktiva, kritické systémy, kritická infrastruktura, řízení rizik, analýza rizik, bezpečnostní plán, prevence, krizový plán, pražské metro, stanice metra, bezporuchovost, dostupnost, udržovatelnost, bezpečnost, zabezpečení, All-Hazard-Approach, Defence-In-Depth, vypořádání rizik.

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

Security Plan of Selected Station of Praha Metro

DIPLOMA THESIS

Tomáš Kertis

May 2015

Abstract

The Diploma Thesis is focused on security of critical infrastructure which is the base for quality of life for people and human survival at critical conditions. Regarding to present knowledge the Thesis is addressed to the risks of metro station. It establishes particular security plan on the basis of the integral safety concept which then compares with a current practice. On the basis of conformity assessment it identifies phenomena (triggers) which can endanger a given station and which have not been solved yet in the context of safety. It shows their consequences and for the cases of occurrence of critical risks, it recommends measures and activities for response.

Key words

Protection of health and property, national security, protected assets, critical systems, critical infrastructure, risk management, risk analysis, security plan, prevention, crisis plan, Praha metro, metro station, reliability, availability, maintainability, safety, security, All-Hazard-Approach, Defence-In-Depth, trade-off with risks.

OBSAH

OBSAH 5
Seznam zkratek 7
Úvod 9
1 Bezpečnost technologií a infrastruktury 11
1.1 Práce s riziky a zajištění bezpečnosti 11
1.2 Pohromy a jejich dopady 14
1.2.1 Pohromy, jejich dopady a kategorizace 14
1.2.2 Členění pohrom dle jejich vlastností 17
1.3 Řízení bezpečnosti 19
1.3.1 Vrcholové řízení bezpečnosti 19
1.3.2 Řízení bezpečnosti pro konkrétní území 21
1.3.3 Systém řízení bezpečnosti (SMS) pro systémy systémů (SoS) 22
1.3.4 Řízení bezpečnosti drážních systémů v praxi 24
1.4 Úmyslné útoky na dopravní systém 25
1.5 Řízení rizik projektů 26
2 Data o pražském metru a jeho řídicím systému 29
2.1 Obecný popis systému metra 29
2.2 Pražské metro jako řízený systém 30
2.2.1 Provozní režimy řízeného systému 31
2.2.2 Mimořádné události v systému pražského metra 32
2.2.3 Technologie řízeného systému 32
2.2.4 Zabezpečovací zařízení 33
2.2.5 Řídicí systém pražského metra 34
2.2.6 Systémy UGTMS dle EN 62290 35
3 Metody zpracování dat 39
3.1 Standardní metody zpracování dat 39
3.2 Procesní model 40
3.2.1 Získání informací o entitě (chráněná aktiva, specifické zranitelnosti) 40
3.2.2 Hledání relevantních pohrom náležících vybrané entitě 41
3.2.3 Stanovení ohrožení a identifikace četností dle zdroje 41
3.2.4 Metoda What, IF pro určení dopadů na chráněná aktiva 41
3.2.5 Matice odpovědnosti 43
3.2.6 Bezpečnostní plán 44
3.2.7 Plán řízení rizik 44
4 Bezpečnostní plán 45
4.1 Stručný popis entity 45
4.1.1 Obecné informace 45
4.1.2 Místopis 48
4.1.3 Chráněná aktiva veřejná (okolí) 49

4.1.4 Chráněná aktiva stanice ... 51
4.2 Seznam pohrom, které mohou entitu postihnout ... 53
4.3 Scénáře dopadů dvou vybraných pohrom ... 54
4.3.1 Výpadek elektřiny (black out) ... 54
4.3.2 Teroristický útok (na tok informací) ... 58
4.4 Bezpečnostní plán pro případ velkého výpadku elektřiny ... 61
4.4.1 Prevence ... 61
4.4.2 Ochrana - zmírnění ... 62
4.4.3 Scénáře odezvy - nouzové plány ... 62
4.4.4 Evakuační plány ... 64
4.4.5 Varovací systém ... 64
4.4.6 Cvičení a výcvik ... 64
4.4.7 Konkrétní plány a postupy při odezvě ... 65
4.5 Bezpečnostní plán pro případ velkého teroristického útoku (útok na tok dat) ... 65
4.5.1 Prevence ... 65
4.5.2 Ochrana - zmírnění ... 67
4.5.3 Scénáře odezvy - nouzové plány ... 68
4.5.4 Evakuační plány ... 69
4.5.5 Varovací systém ... 69
4.5.6 Cvičení a výcvik ... 69
4.5.7 Konkrétní plány a postupy při odezvě ... 70
4.6 Plány obnovy po pohromách většího rozsahu ... 70
5 Srovnání výsledků práce se současným stavem ... 71
5.1 Současný stav bezpečnosti stanic metra ... 71
5.2 Porovnání nároků pětistupňového modelu SMS s platnou legislativou ... 72
5.3 Prvky pro zajištění bezpečnosti chráněných aktiv ... 74
6 Plán řízení rizik ... 79
6.1 Obecný plán řízení bezpečnostních rizik ... 80
6.2 Plán řízení bezpečnostních rizik vybrané stanice metra ... 82
Závěr ... 85
Seznam literatury a zdroje ... 87
Seznam obrázků ... 91
Seznam tabulek ... 92

Seznam zkratek

ALARA	(As Low As Reasonably Achievable) princip snižování rizika „tak nízko, jak je rozumně dosažitelné“
ALARP	(As Low As Reasonably Practicable) princip snižování rizika „tak nízko, jak je rozumně proveditelné“
AP	(Access Points) přístupové body – zpravidla do technologické sítě
ASDŘ	automatický systém dopravního řízení
ATC	(Automatic Train Control) automatické řízení vlaku - součást VZZ
ATO	(Automatic Train Operation) automatický provoz vlaku - součást VZZ
ATP	(Automatic Train Protection) automatická ochrana vlaku - součást VZZ
CC	(Common Criteria) standard pro hodnocení počítačové bezpečnosti
CBRNE	chemické, jaderné, radiologické, biologické a explozivní látky
CSIRT	(Computer Security Incident Response Team) tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích
DSM	dopravní systém metra
EAL	(Evaluation Assurance Level) hloubka hodnocení zabezpečení IT
E/E/PE	(Electrical/Electronic/Programmable Electronic) elektronická, elektrotechnická a programovatelná zařízení
FMEA	(Failure Mode and Effects Analysis) analýza možného výskytu a vlivu vad
HAZOP	(Hazard and Operability Study) analýza ohrožení a provozuschopnosti
IAD	Individuální automobilová doprava
IDS	(Intrusion Detection System) systém detekce průniku, systémy pro sledování podezřelých aktivit na síti
KI	kritická infrastruktura
LCC	(Life Cycle Cost) náklady životního cyklu
MHD	městská hromadná doprava
OSM	ochranný systém metra
P+R	(Park+Ride) parkoviště typu „zaparkuj a jeď“

PP	(Protection Profile) profil ochrany
RAMS	(Reliability, Availability, Maintainability, Safety) bezporuchovost, dostupnost, udržovatelnost, bezpečnost
SIL	(Safety Integrity Level) stupeň integrity / úroveň celistvosti bezpečnosti
SZZ	staniční zabezpečovací zařízení
SMS	(Safety Management System) systém pro řízení bezpečnosti
SoS	(System of Systems) systém systémů
TOE	(Target Of Evaluation) cíl hodnocení z hlediska zabezpečení IT
UGTMS	(Urban Guided Transport Management and Command / Control System) systémy řízení městské a příměstské kolejové dopravy
VZZ	vlakové zabezpečovací zařízení
ZZ	zabezpečovací zařízení

Úvod

Všichni lidé si přejí život v bezpečném světě s potenciálem rozvoje. Listina základních lidských práv a svobod, která navazuje na Ústavu České republiky, zaručuje práva a svobody občanů. Čas od času se objevují jevy, které nazýváme pohromy, jelikož působí škody a ztráty lidem a aktivům, na nichž jsou lidé závislí. Zvládnutí vzniklých situací vyžaduje kompromisy mezi základními právy a povinnostmi pro ochranu zdraví, majetku, bezpečnosti státu. Každá pohroma s sebou nese řadu více či méně závažných a různě zřetězených důsledků. Důsledky pohrom jsou vždy závažnější, pokud mají přímý dopad na místa s výskytem velkého množství osob, investičně nákladných a klíčových systémů či systému pro okolí nebezpečných. Předmětná místa jsou kritickými položkami, které musí být speciálně sledovány pro zajištění bezpečí lidí.

Aktivy zajišťujícími přežití lidí jsou kritické infrastruktury. Z hlediska hl. m. Prahy je jedním z hlavních aktiv dopravní infrastruktura města, jež poskytuje služby městské logistiky, přepravy lidí, zboží a zajišťuje základní funkce pro přežití lidí při přepravě zboží, léčiv, složek záchranného systému a podobně.

Systém pražského metra je bezesporu klíčovým chráněným aktivem hl. města Prahy, kde zajišťuje dopravní obslužnost velkého množství cestujících. Nalezneme v něm mnoho nákladných a důležitých systému. Pražské metro je koncipováno také jako ochranný systém v případě výskytu pohrom, především válečných konfliktů. Navíc systém metra obsahuje prvky, při jejichž poruše se můžou stát zdrojem katastrofy. Například nezabezpečený systém řízení metra anebo poruchy drážní techniky (například zabezpečovacího zařízení) mohou zapříčinit vážnou nehodu s úmrtím několika desítek až stovek lidí. Vzhledem k uvedeným skutečnostem je nutností metro a jiné podobné systémy chránit a dbát o jejich bezpečnosti.

V běžné praxi se již používá mnoho metodik a pravidel pro ochranu vyjmenovaných kritických systému, ať už se jedná o samotnou legislativu, systémy řízení kvality nebo dokonce i oborové směrnice a standardy. Předmětné standardy jsou v některých případech nedostatečné, mnohdy jsou nepochopené nebo špatně aplikovatelné, protože jsou poplatné době vzniku, znalostem a zkušenostem osob, které je aplikují do praxe. Pouze v několika málo oborových odvětvích jako je armáda, letectví či jaderná zařízení, se dá mluvit o pokročilém přístupu k rizikům, ale i zde známe mnoho případů lidských pochybení i systémových poruch, které vedly k obrovským katastrofám.

Tématem předložené diplomové práce je bezpečnostní plán vybrané stanice metra. Jedná se o drážní systém, který podléhá požadavkům hned několika na sebe závislých norem a směrnic. Velkou slabinou zmíněných předpisů je přílišná obecnost, kvůli které dochází

k mnoha nedorozuměním a špatné implementaci. I přesto, že má provozovatel dráhy a drážní průmysl povinnost analyzovat zdroje nebezpečí z vnějšího prostředí, není zde dostatečně definován typ nebezpečí a už vůbec ne metodologie, jak chránit veřejnou bezpečnost. Právě zabezpečení drážních systémů je v dnešní době velmi aktuální téma, protože je pravdou, že každý kvalitní systém, jenž není chráněn proti dopadům pohrom, ztrácí na významu tím, že může svému okolí výrazně uškodit a výrazně zhoršit dopady pohromy.

Z výše uvedených řádků je patrné, že přístup k bezpečnosti v drážním odvětví není ještě zcela ustálen. Možnosti pro návrh přístupu k zabezpečení drážního systému se stalo velkou motivací k výběru tématu předložené diplomové práce. Na stanici metra lze výše uvedenou problematiku dostatečně demonstrovat, poukázat na nedostatky v legislativě a navrhnout řadu opatření.

Provoz metra musí plnit své provozní úkoly jak na trati, tak i ve stanici a to hlavně z pohledu veřejného zájmu. Provozní úkoly jsou obvykle řízeny z centralizovaných řídicích center s návazností na řídicí systémy jednotlivých stanic. Z uvedeného důvodu se práce zaměřuje hlavně na systémy řízení a nesleduje například stavbu vozidla, která je na rozdíl od řídicího systému evropskými standardy stanovena a důkladně provedena.

Předložená diplomová práce vychází z pojetí integrální bezpečnosti dle [1]. Stanici metra práce pojímá jako otevřený systém tj. uvažuje vzájemné propojení více (otevřených) systémů, jejich prvky (subsystémy, zařízení a komponenty), jejich vazby a toky (energií, informací, zboží) [1].

Jelikož předmětný koncept se dosud v praxi používá jen u vybraných objektů (jaderné elektrárny, přepravování vyhořelého paliva, objekty budované ve vesmíru apod.), je zřejmé, že existují jevy, které v ostatních objektech a zařízeních nejsou zváženy. Pro zajištění každého bezpečného systému s potenciálem rozvoje, je žádoucí bezpečnostní plán. Jeho srovnání s reálným stavem ukazuje aspekty, které na základě posouzení z hlediska bezpečnosti i hospodárnosti identifikují závažná rizika, která nejsou řešena, a proto se sestavuje plán řízení rizik.

Cílem práce je sestavení bezpečnostního plánu vybrané stanice metra pro dvě pohromy a identifikovat opatření a činnosti vedoucí k odstranění závažných nedostatků.

Metodika sestavení práce spočívá v:

- shromáždění a utřídění souboru poznatků o dané problematice,
- sběru dat a výběru vhodných metod pro řešení práce,
- zpracování podkladů řešení na bázi postupů rizikového inženýrství,
- vypracování bezpečnostního plánu,
- návrhu opatření na vylepšení současného stavu.

1 Bezpečnost technologií a infrastruktury

Kapitola „Bezpečnosti technologií a infrastruktury“ shrnuje základní poznatky o bezpečnosti a jejím řízením. Pojednává o pohromách, jejich dopadech a nakonec o řízení bezpečnosti v různých úrovních lidských systémů.

1.1 Práce s riziky a zajištění bezpečnosti

Management rizik v sobě zahrnuje procesy pro práci s riziky, jimiž jsou například identifikace rizik, jejich analýza, hodnocení, posouzení velikosti, rozhodnutí, řízení a vypořádání se s riziky. Dané procesy také v sobě zahrnují neustálou aktualizaci zdrojů nebezpečí a jejich vyhodnocení. V praxi se musí provádět mnoho různých opatření, aby bylo dosaženo přijatelného rizika.

Snižování jakéhokoliv rizika je spojeno se zvyšováním nákladů, s nedostatkem znalostí, s nedostatkem technických prostředků, apod. Proto se hledá hranice, na kterou je riziko možné snížit tak, aby vynaložené náklady byly ještě přijatelné [2].

Rizika ve vztahu k bezpečnosti jsou předmětem řízení bezpečnosti. Zdroji uvedených rizik jsou přírodní jevy, technologie používané člověkem, velké zásahy do životního prostředí, nežádoucí jevy a konflikty v lidské společnosti. Jedná se o rizika pro člověka, jeho majetek, životní prostředí, kritickou infrastrukturu a v neposlední řadě i pro stát.

Rizika se dle zdroje [3] liší podle toho, jaké jsou zvolená chráněná aktiva a zda je sledován jeden chráněný zájem (tj. dílčí riziko) či soubor chráněných zájmů (integrované) nebo soubor chráněných zájmů, 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.).

Pro zajištění bezpečného území, popřípadě větších technologických celků nebo zařízení, je nutné počítat s komplexním rizikem, tj. rizikem integrálním založeném na systémovém pojetí reality.

Integrální riziko zahrnuje více chráněných aktiv včetně života, zdraví a bezpečí lidí, majetku a veřejného blaha, životního prostředí i technologií a infrastruktur a zahrnuje i vliv propojení mezi uvedenými chráněnými aktivy (interdependences). Bezpečnost je chápana komplexně a činnosti a opatření pro ochranu jednoho aktiva nesmí výrazně ohrozit druhá aktiva [2].

Integrální riziko označené jako R je pro všechny pohromy v území dané vztahem [3]:

$$R = \sum_{k=1}^{m} R_k$$

R_k vyjadřuje riziko pro k-tou pohromu:

$$R_k = \sum_{i=1}^{n} P_k \cdot D_{i,k,}$$

P_k označuje pravděpodobnost výskytu k-té pohromy a $D_{i,k}$ dopad k-té pohromy na i-tý chráněný zájem. Podobné vztahy jsou aplikované i pro integrované riziko, ovšem s tím rozdílem, že dopady $D_{i,k}$ pro riziko integrální zahrnují mimo přímé dopady $DD_{i,k}$ i dopady nepřímé (sekundární, terciální a více) $DI_{i,k}$, jejichž vztahy jsou dle zdroje [3] následující:

$$DD_{i,k} = \int_S Z_{i,k} \cdot V_i \, dS \, ; DI_{i,k} = \int_S I_{i,k} \cdot V_i \, dS$$

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 [3]:

$$I_{i,k} = fu\left(VD_k, VP_{i,k}\right)$$

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 [3].

Cílem konkrétních programů pro řízení bezpečnosti je zajistit bezpečnost podniku či území. V systémovém pojetí jde o ochranu veřejných zájmů, a u podniků, také o konkurenceschopnost, zisk a dobrého jména (goodwill) podniku a jiného subjektu.

Řízení bezpečnosti dle zdroje [2]:

- zahrnuje princip předběžné opatrnosti,
- soustřeďuje se na prioritní pohromy,
- realizuje optimální opatření pro všechny relevantní pohromy možné v daném místě.

Nezbytné ***vstupní informace pro řízení bezpečnosti*** území ukazuje následující souhrn [2]:

1. Jaké živelné a jiné pohromy se na území spravovaném veřejnou správou mohou vyskytnout a jaké mají dopady?

2. Kde se živelné a jiné pohromy na území spravovaném veřejnou správou mohou vyskytnout, a jak jsou územně rozloženy jejich dopady?
3. Za jakých podmínek se živelné a jiné pohromy na území spravovaném veřejnou správou mohou vyskytnout, a jaké podmínky mohou způsobit eskalaci jejich dopadů?
4. Jak často se živelné a jiné pohromy na území spravovaném veřejnou správou mohou vyskytnout?
5. Od jaké velikosti mají živelné a jiné pohromy na území spravovaném veřejnou správou nežádoucí dopady, které působí škody na chráněných zájmech, tj. i na majetku?
6. Jaké škody na majetku může vyvolat maximální možná živelná a jiná pohroma určená na specifikované hladině věrohodnosti na území spravovaném veřejnou správou a jaké jsou její dopady na majetek?
7. Co se proti nežádoucím dopadům živelných a jiných pohrom dá dělat na území spravovaném veřejnou správou na úseku územního plánování, projektování, výstavby a provozu občanských i technologických objektů a infrastruktury a popř. v dalších oblastech jako jsou monitoring, inspekce, vzdělání aj., aby se zabránilo výskytu pohrom, kterým lze zabránit nebo, aby se zabránilo nežádoucím dopadům nebo alespoň, aby se nežádoucí dopady zmírnily preventivními opatřeními, připraveností, vhodnou odezvou na pohromu a obnovou, při níž bude respektována prevence ztrát a cíle udržitelného rozvoje?
8. Jaká opatření vůči konkrétním živelným a jiným pohromám na území spravovaném veřejnou správou jsou žádoucí v oblasti technické, organizační, finanční, sociální, právní, vzdělání a výchovy?
9. Jaká nepřijatelná a zbytková rizika (tj. nežádoucí dopady s pravděpodobností výskytu vyšší než stanovená mez) s ohledem na možné živelné a jiné pohromy na území spravovaném veřejnou správou zůstanou, když se provedou racionální opatření, která může veřejná správa zajistit v oblasti technické, organizační, finanční, sociální, právní, vzdělání a výchovy?
10. Jak provádět obnovu majetku po živelné a jiné pohromě na území spravovaném veřejnou správou, aby se racionálně využily zdroje, síly a prostředky, aby se zamezilo dalším ztrátám, aby se zvýšila odolnost proti živelným a jiným pohromám a aby se nastartoval další rozvoj území a lidské společnosti se všemi položkami (životním prostředím, majetkem, infrastrukturou, službami apod.), na

nichž je závislá?

11. Jaká forma řízení a provádění obnovy majetku po živelné a jiné pohromě na území spravovaném veřejnou správou je vhodná a jak ji lze realizovat?
12. Jak vytvořit finanční rezervu veřejné správy na racionální obnovu majetku po živelné a jiné pohromě na území spravovaném veřejnou správou?

Obdobný souhrn platí i pro jiné organizační celky, tj. podniky.

Pro řízení integrální bezpečnosti je charakteristický systémový koncept a specifický přístup All-Hazard-Aproach [4], tj. přístup zvažování všech možných ohrožení, který tvoří podklad pro zvládnutí dopadů od všech relevantních pohrom.

Vyjednávání s riziky je proces ke zjištění aspektů pro zvládnutí rizik, tj. procesů prevence před nejhoršími dopady poškozujících lidi, zmírnění dopadů, zvládnutí dopadů, obnovení a zajištění dalšího rozvoje. V praxi se zohledňuje, že člověk nemá veškeré znalosti a schopnosti k eliminaci všech pohrom, a proto se používá přístup ALARA a ALARP, který specifikuje, že existující rizika se požadují snížit na míru, která je technicky dosažitelná. U závažných rizik, která mohou přesáhnout přijatelnou míru, sestavujeme plán řízení rizik, protože dopady sníží rychlá a včasná odezva [5].

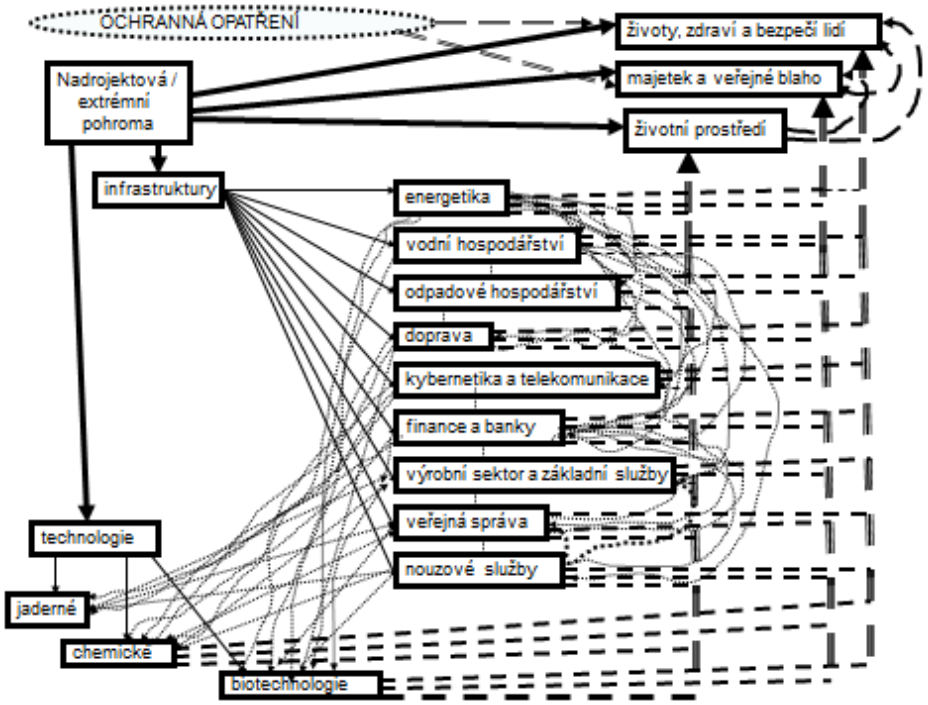
1.2 Pohromy a jejich dopady

Kapitola se zabývá kategorizací pohrom na základě jejich četností a dopadů. Druhá část kapitoly popisuje pohromy z hlediska jejich vlastností, člení je do několika základních skupin a v závěru uvádí seznam relevantních pohrom pro účely bezpečnostního plánu předložené práce.

1.2.1 Pohromy, jejich dopady a kategorizace

Příčinou rizik jsou pohromy (všeho druhu) a v případě rizik u technologických systémů se jedná také o poruchové stavy v důsledku náhodných či systematických chyb systému. Každé riziko lze ohodnotit jeho četnosti resp. pravděpodobnosti výskytu a velikosti jeho dopadů, jak je patrné ze vzorců uvedených v předchozím odstavci. Z výše uvedeného je patrné, že vznik jedné extrémní pohromy může vyvolat řetězec dalších pohrom, tj. sekundární efekty, i celou kaskádu dopadů. Sekundární, terciální a další dopady jsou označovány jako nepřímé dopady $DI_{i,k}$ zmíněné ve vzorcích v předchozím odstavci. 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.



Obr. 1: Účinky extrémních pohrom na veřejná aktiva [5].

Podle velikosti škod a ztrát na veřejných aktivech a pravděpodobnosti výskytu lze dle zdroje rizik pohromy v řízení bezpečnosti kategorizovat ***do tří kategorií*** [2]:

1. Živelné a jiné pohromy, jejichž dopady ve sledovaném období mohou být vysoké až velmi vysoké a pravděpodobnost jejich výskytu bude malá až velmi vysoká (tj. cca jedenkrát za 100 let či za 10 let či za 1 rok apod. u pohrom, které žijí v jiných časových měřítcích), které mohou vyvolat kritickou situaci, při níž se musí nebo bude muset vyhlásit krizová situace, a tudíž bude potřeba provádět obnovu majetku po krizové situaci.

2. Živelné a jiné pohromy, jejichž dopady ve sledovaném období mohou být malé až vysoké a pravděpodobnost jejich výskytu bude zanedbatelná až vysoká, u kterých není předpoklad pro vyvolání kritické situace, při níž může být vyhlášena krizová situace, a tudíž nebude potřeba provádět obnovu majetku po krizové situaci. Vůči těmto pohromám však musí být prováděna opatření v územním plánování, projektování, výstavbě a provozu objektů.

3. Živelné a jiné pohromy, jejichž dopady a pravděpodobnosti výskytu nepatří do kategorií vyšších, tj. 1 a 2. V tomto případě se provádí interpretace pohromy pomocí matice rizik.

Matice rizik skóruje pravděpodobnost výskytu rizika a velikost jeho dopadu. Do předmětné matice se rizika začlení podle jejich četnosti výskytů a rozsahu dopadů. Z tohoto zařazení se v klasické analýze rizik stanoví přijatelnost rizika, tj. riziko je přijatelné, podmíněně přijatelné,

nepřijatelné. Pro nepřijatelné a podmíněné přijatelné pohromy se provádí snížení rizika například pomocí přístupu ALARP / ALARA uvedených v předchozím odstavci.

V oblasti řízení bezpečnosti se stejné matice rizik využije pro kategorizaci pohromy a to pro každou pohromu a sledovanou entitu zvlášť. Matice rizik má podobu zachycenou na následujícím obrázku 2.

Velmi vysoké	Pravděpodobnost výskytu		G				
Vysoké		H			C	A	
Střední							
Malé				E			B
Velmi malé		F				D	
Zanedbatelné							
	Dopady	zanedbatelné	velmi malé	malé	střední	vysoké	velmi vysoké

Obr. 2: Kategorie pohrom ve sledovaném území [2].

Na obrázku 2 jsou pohromy kategorie 3 označeny písmeny A až H.

Pohromy kategorie 3. A, B jsou kritické, tj. 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.

Pohromy kategorie 3. C, D jsou specifické, tj. 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.

Pohromy kategorie 3. G, E, H jsou relevantní a měly by být zvládnuty běžnými standardními prostředky odezvy. 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.

Pohroma kategorie 3. F je relevantní a měly by ji zvládnout občané bez výkonných složek na základě své výchovy a zkušeností. Zde je výchova a vzdělání hlavním nástrojem pro zajištění bezpečnost.

1.2.2 Členění pohrom dle jejich vlastností

Pohromy se dle svých vlastností člení do následujících skupin [3]:

- výsledky procesů probíhající vně i uvnitř Země (živelné pohromy, nemoci rostlin, zvířat, eroze krajiny, rozšiřování pouští (desertifikace), ztekucení podloží, rozšiřování oceánů apod.),
- výsledky procesů v lidském těle, v chování lidí a procesů v lidské společnosti (neúmyslné: nemoci a lidské chyby, úmyslné jevy vyvolané lidmi: neoprávněné přivlastňování majetku, usmrcení lidského jedince, šikana, náboženská a jiná nesnášenlivost, kriminální činy, teroristické útoky, lokální a další ozbrojené konflikty),
- výsledky procesů a činností instalovaných lidmi (nehody, havárie, selhání infrastruktur, selhání technologií, ztráty obslužnosti apod.),
- interakce planety Země a životního prostředí na činnosti lidí (indukovaná zemětřesení, narušení ozónové vrstvy, skleníkový efekt, rychlé variace klimatu, kontaminace ovzduší, vody půdy i horninového prostředí, rozšiřování pouští v důsledku nepromyšlené regulace vodních toků, pokles diverzity živočišných a rostlinných druhů, neřízení populační exploze lidí – migrace velkých skupin lidí, postupné vyčerpávání neobnovitelných zdrojů, eroze půdy a horninových masivů, uniformita krajiny),
- vnitřní závislosti v lidském systému přirozené nebo lidmi vytvořené (přirozené: napjatost a pohyb desek, koloběhy vody v životním prostředí, koloběhy látek v životním prostředí, koloběhy látek v potravinovém řetězci člověka, planetární procesy, interakce solárních a galaktických procesů; lidmi vytvořené: řízení lidské společnosti, toky surovin a výrobků, toky energií, toky peněz, toky informací).

Na základě srovnání seznamu pohrom [5], analýzy archivních dokumentech hl. m. Prahy [6] a kritérií pro třídění [7] byly pro účely předložené diplomové práci odvozeny následující relevantní pohromy:

1. Výsledky procesů probíhající vně i uvnitř Země:

- povodeň,
- vichřice,
- zemětřesení,
- ztekucení podloží,
- výstup plynu na zemský povrch.

2. 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.

3. 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.

4. 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.

5. Vnitřní závislosti v lidském systému přirození nebo lidmi vytvoření:

- organizační havárie,
- porucha toků surovin a výrobků,
- porucha v toku energií,
- porucha v toku informací.

1.3 Řízení bezpečnosti

Relevantní pohromy mají nepříznivé dopady na lidskou společnost, a proto je nutné je patřičným způsobem řídit a předcházet jim. Následující odstavce popisují způsoby řízení bezpečnosti sestupně v různých vrstvách řízení. Pro každou vrstvu řízení bezpečnosti platí společné metody pro práci s riziky.

Pro pohromy zařazené v odstavci 1.2.1 do kategorie 1. a 3. A, B podle obrázku 2, tj. kritické pohromy, se provádí prevence, odezva (nouzové plány, tj. havarijní plány, povodňové plány, plány kontinuity atd..) a krizový plán, který využívá kromě standardních zdrojů i zdroje nadstandardní určené jen pro krizové situace.

Pro pohromy zařazené v odstavci 1.2.1 do kategorie 2. a 3. C, D podle obrázku 2, tj. specifické pohromy, se provádí prevence a odezva (nouzové plány, tj. havarijní plány, povodňové plány, plány kontinuity atd..)

Pro pohromy zařazené v odstavci 1.2.1 do kategorie 3. F podle obrázku 2, se provádí prevence, především ve formě výchovy a vzdělání, očkování.

1.3.1 Vrcholové řízení bezpečnosti

Vrcholové řízení bezpečnosti je základním kamenem řízení 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. Výstup řízení bezpečnosti vyšší vrstvy musí sloužit jako vstup pro řízení bezpečnosti na nižších úrovních, tj. konkrétního území, kritické infrastruktury a vybrané kritické objekty [9].

Vrcholové řízení bezpečnosti dle zdroje [2] zahrnuje následující postupy.

1. Určit seznam relevantních živelných a jiných pohrom.
2. Provést analýzu poznatků a zkušeností, spojených s každou relevantní živelnou či jinou pohromou s cílem:

- v daném konkrétním místě a pro stanovené časové intervaly určit ohrožení od dané živelné či jiné pohromy, tj. maximální velikost živelné či jiné pohromy a jejich dopadů v daném místě, četnost výskytu včetně pravděpodobnosti výskytu této velikosti v určených časových intervalech (očekávanou velikost pro 100 let tzv. projektová pohroma),
- pochopit rizika od dané živelné či jiné pohromy v širokých souvislostech a určit cíle z pohledu bezpečnosti,

- projednat všechny aspekty rizik a aspekty řízení bezpečnosti z pohledu integrálního systému (společnosti),
- identifikovat zdroje všech rizik, zranitelnosti, utrpení a možné ztráty spojené s danou živelnou či jinou pohromou v daném místě,
- vyjasnit možné problémy, spouštěcí mechanismy a podmínky při vzniku živelné či jiné pohromy,
- vytvořit možné scénáře živelné či jiné pohromy,
- zhodnotit dopady všech možných scénářů živelné či jiné pohromy, zvláště z pohledu bezpečnostních aspektů,
- odděleně zvážit újmy a škody na životech, majetku a životním prostředí,
- zvážit záznamy, empirické důkazy, zkušenosti a expertní posudky.

3. Provést hodnocení dopadů každé sledované živelné či jiné pohromy s ohledem na:

- objektivní kvantifikaci všech parametrů a jejich neurčitostí,
- výsledky citlivostní analýzy pro dynamickou situaci,
- existující fyzikální omezení a špatně určitelné hranice některých charakteristických parametrů,
- definovaný charakter dopadů živelné či jiné pohromy i velikost možných dopadů,
- četnost výskytu živelné či jiné pohromy,
- výsledky aplikace pravděpodobnostního přístupu.

4. Provést ocenění sledované živelné či jiné pohromy s ohledem na:

- věrohodnost odhadnutého ohrožení (v absolutní i relativní míře),
- přijatelnost ohrožení (z hlediska jednotlivce i společnosti),
- ekonomický dopad na společnost a existující fondy pro obnovu ve společnosti,
- náklady a zisky při regulaci nejzávažnějších dopadů živelné či jiné pohromy,
- analýzu nákladů a užitků s ohledem na velikost rizik od dané živelné či jiné pohromy,
- přijatelnost, snížení nebo přenos rizik od dané živelné či jiné pohromy.

5. Regulovat činnosti v dané oblasti s cílem:

- minimalizovat, zmírňovat a zvládat dopady živelné či jiné pohromy, tj. aplikovat opatření, aby se: změnila pravděpodobnost výskytu živelné či jiné pohromy /nebo jejich dopadů; snížila velikost dopadů; opatřily zdroje na odezvu na (zásah proti) dopady živelné či jiné pohromy a na následnou obnovu,

- zvážit všechny možnosti na snížení velikosti dopadů živelné či jiné pohromy, tj.: zavedení bezpečnostních opatření v projektu z pohledu prevence, ochrany a omezení škod; snížení neurčitosti v informacích o dopadech živelné či jiné pohromy,

soustavný monitoring klíčových částí technologie z hlediska velkých dopadů v případě živelných či jiných pohrom, oprava a vylepšování systému řízení; zavedení norem a aplikování kontroly kvality na všech stupních; vytvoření hloubkové obrany (Defence-In-Depth) na paralyzování malých selhání; redukce pravděpodobnosti výskytu lidských chyb nebo zvrhlostí (výcvik a kultura bezpečnosti).

6. Soustavně ověřovat přijatou metodiku vrcholového řízení bezpečnosti s cílem:

- testovat účinnost strategií na snížení dopadů živelných a jiných pohrom,
- získávat nezávislý bezpečnostní audit a inspekci dopadů živelných a jiných pohrom,
- ustanovit metodu na hlášení událostí, která zahrnuje odezvy společnosti na dopady živelných a jiných pohrom,
- sledovat mechanismy zpětné vazby s cílem poučit se ze zkušeností a případně změnit priority ve vrcholovém řízení,
- vytvořit programy, které zahrnují způsoby řízení, výcvik a postupy v případě dopadů dané živelné či jiné pohromy,
- zhodnotit celkové narušení systému (společnosti) ve všech fázích (včetně všech narušení systému, která jsou vyvolána zásahem proti dopadům živelné či jiné pohromy),
- zavést mechanismus kontroly jakosti tak, aby všechny části byly optimálně vyváženy,
- spojitě monitorovat, posuzovat a vylepšovat systém vrcholového řízení.

1.3.2 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 dané území [1]. Určí se dopady jednotlivých pohrom na aktiva entity, například pomocí metody What/IF. Dále se určí četnosti a provede se klasifikace pohrom [2]. Získáme rozdělení pohrom na relevantní pro konkrétní území, z relevantních pohrom určujeme pohromy specifické a kritické.

Pro veškeré ***relevantní pohromy*** se vytváří společné opatření a plány ke snížení četností a zmírnění dopadů relevantních pohrom dle All-Hazard-Approach.

Pro ***specifické či kritické pohromy*** se provádí kromě prevence specifická opatření na zmírnění dopadů i na provedení odezvy, tj. nouzové plány a u kritických pohrom pak plány kontinuity (pro podniky) a plány krizové (pro území). Aby bylo možné dopady zmírňovat, je zapotřebí znát jejich rozsah a velikost a podrobnější popis. Proto se vytváří ***scénáře dopadů***, kterými jsou například: plány záplavového území, plán rozletu úlomků, plán šíření požáru, mapa seismických zón, mapa srážek a podobně. Odezva na specifické pohromy se provádí

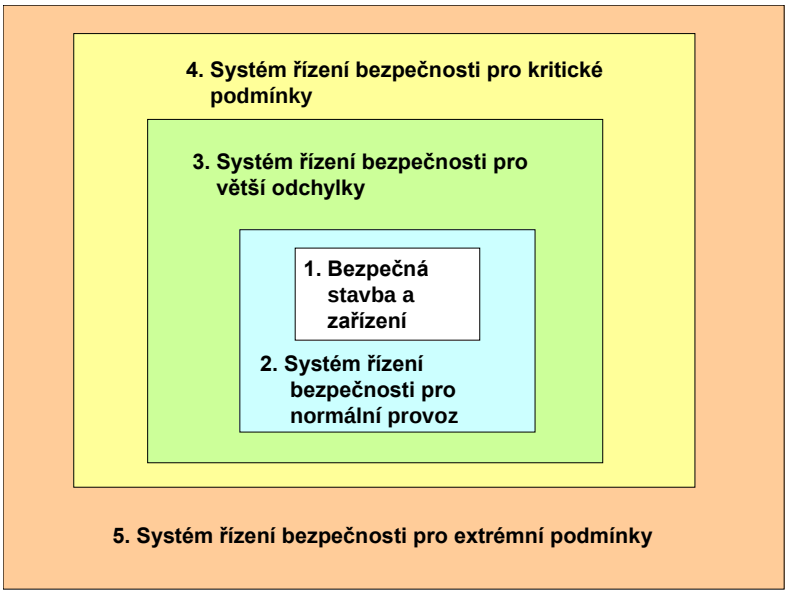
s využitím standardních finančních i lidských zdrojů, sil a prostředků dle povodňových plánů, havarijních plánů, plánů kontinuity a podobně.

Pro případ výskytu ***kritické pohromy*** je nutné vytvořit adekvátní schopnost zvládnout dopady. Jedním z bodů připravenosti je mimo jiné zpracování ***scénářů odezvy*** (zásahů), s ohledem na specifické 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.

1.3.3 Systém řízení bezpečnosti (SMS) pro systémy systémů (SoS)

Objekt kritické infrastruktury, kterým je každá stanice metra, lze popsat modelem systému systémů (dále jen SoS), který je součást i velkého systému systémů, kterým je systém dopravy v Praze atd. SoS označuje soubor otevřených prolínajících se systémů. Skládá se z několika systémů různé povahy a různého umístění, které jsou vzájemně provázané k tomu, aby zajistily jisté operace a činnosti. Provázanost mezi systémy (interdependence) si vynucuje přístup řízení integrálního rizika s respektováním i průřezových dílčích rizik způsobenými vazbami a toky mezi různými prvky a systémy SoS a okolím. Řízení bezpečnosti SoS je vyšší úrovní řízení, než je řízení bezpečnosti podle známých norem, které se zaměřují na bezpečnost pouze vybraného systému (například dle normy EN 61511 [10], EN 62508 [11] nebo drážní norma EN 50126 [12]). Řízení bezpečnosti SoS se snaží hledat řešení jak pro bezpečný systém, tak i pro bezpečné okolí včetně ostatních veřejných aktiv, tj. jde o integrální bezpečnost [1].

V moderním pojetí řízení bezpečnosti se pro složité technologické objekty, tedy SoS, používá dvou principů, a to All-Hazards-Approach [13] a zobecněná „obrana do hloubky“ (Defence-In-Depth) [15], která vychází z principů používaných pro zajištění bezpečnosti jaderných elektráren [14]. Stejný pojem Defence-In-Depth se používá taktéž i v jiných oblastech, ale v rozdílných pojetích (dva nebo tři stupně). Základní principy a cíle obrany do hloubky jsou vždy stejné. Obecný koncept obrany do hloubky pro technologické systémy (objekty, infrastruktury) byl definován v práci „Ochrana lidí před dopady nebezpečných látek implementovaná v konceptu řízení integrální bezpečnosti technologických objektů a infrastruktur“ [15]. Jedním z výsledků výše uvedené práce je definice pětistupňového modelu řízení bezpečnosti technologického objektu (viz obrázek 3).



Obr. 3: Pětistupňový model řízení bezpečnosti technologického objektu [15].

Při rozlišení míry bezpečnosti objektů a infrastruktur se dle zdroje [15] používá bezpečnostní charakteristika, dle které má objekt jednostupňovou nebo až pětistupňovou ochranu do hloubky, viz obrázek 3. 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 [15].

Zdroj [15] uvádí principy možných opatření pro jednotlivé vrstvy následovně:

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 pod-

mínek (tj. při abnormálních podmínkách) a zabraňují vzniku nežádoucích jevů, což znamená, že má dobrou resilienci. Předmětné systémy udržují bezpečný provoz i za změny podmínek nebo mají schopnost zajistit normální provoz po aplikaci nápravných opatření (vyčištění, oprava…).

4. 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 technologického objektu, musí mít technologický systém opatření i pro vnější odezvu, zmírňující opatření pro prevenci ztrát v objektu; a kapacitu pro překonání obtíží.

1.3.4 Řízení bezpečnosti drážních systémů v praxi

Řízení bezpečnosti na drahách je zakotveno v evropské směrnici 2004/49/ES ze dne 29. dubna 2004 o bezpečnosti železnic [16], nařízení Komise (ES) č. 352/2009 ze dne 24. dubna 2009 [17] a normy EN 50126 [12] pro prokázání bezporuchovosti (spolehlivosti), dostupnosti, udržovatelnosti a bezpečnosti drážního zařízení (dále jen RAMS - Reliability, Availability, Maintainability and Safety). Uvedené evropské směrnice upřesňují mimo jiné systém řízení rizik na drahách v čase, a to od detekce hrozeb, jejich analýzy, zmírnění a průběžného monitoringu. Norma EN 50126 [12] zase definuje životní cyklus železničního systému od návrhu, analýzy rizik, vývoj, výrobu, provoz až po likvidaci systému se zavedením jednotlivých úkolů pro prokázání RAMS. V drážním průmyslu se dále uplatňuje předpis IRIS [18], který doplňuje systém řízení kvality dle ISO 9001 [19] a je v něm uveden odkaz na povinnost splnění požadavků na RAMS dle uvedené normy EN 50126 [12].

Metodika normy EN 50 126 [12] zavádí pojem integrita (celistvost) bezpečnosti a stupeň integrity bezpečnosti (dále jen SIL – Safety Integrity Level) pro bezpečnostně relevantní systémy. Uvedené pojmy vychází z obecnějších norem pro širokou oblast průmyslového řízení EN 61511 [10] a EN 61508 [11], které jsou taktéž na drahách respektovány. Požadavky na prokázání bezpečnosti drážních systémů stanovuje norma EN 50 129 [20] a definuje strukturu dokumentu zvaného Průkaz bezpečnosti (Safety Case). Uvedenou normou se musí řídit vývoj a implementace systému, jež plní bezpečnostně relevantní funkce hodnocené daným SIL [9].

SIL pro dané funkce či určité systémy plnící předmětné funkce přiřazuje provozovatel dráhy na základě analýzy nebo vlastním posouzením. Metody a opatření definované v uvedené normě jsou určené k identifikaci a vypořádání se s náhodnými a systematickými chybami elektronického systému. Příkladem jedné z metod pro zvýšení bezpečnosti (kupříkladu zabezpečovacího zařízení) je jednoduchá architektura s vlastní bezpečností (tzv. inherentní bezpečnost), kdy při neschopnosti systému vykonat bezpečnostní funkci, systém selže bezpečně (návěstní hodnota „stůj“ apod.). Bezpečnou architekturu vytváří také zálohovaný (redundantní) systém s porovnáním výsledků (systémy 2 z 3, porovnávání výsledků tří systémů, kde se musí alespoň dva shodovat apod.) [9].

Pro software bezpečnostně relevantního drážního systému je dle drážních předpisů známá pouze systematická chyba způsobená zavedením chyby v návrhu softwaru, chyby programátora či zvolených metod programování. Pro eliminaci systémové chyby při vývoji softwaru jsou v normě EN 50128 [21] definované požadavky pro vývoj softwaru pro bezpečnostně relevantní drážní systémy s příslušnou integritou bezpečnosti (SIL 0 až 4) [9]. Jinými slovy jde o předcházení vzniku organizačních havárií [15].

Komunikace mezi bezpečnostně relevantními systémy je řízena normou EN 50159 [22]. Komunikace se může uskutečňovat skrze uzavřené nebo otevřené komunikační prostředí (radiová komunikace, Wi-Fi, různé technologické sítě). Uzavřené přenosové prostředí je přístupné pouze tvůrci systému popřípadě autorizovaným osobám. Do otevřeného komunikačního prostředí mají přístup i neoprávněné a neautorizované subjekty. Bezpečnostně relevantní data v otevřeném prostředí mohou být zachycena útočníkem, který má možnost provést chybné operace a způsobit tak nehodu nebo i destrukci systému [9].

1.4 Úmyslné útoky na dopravní systém

Speciálním odvětvím pro zajištění bezpečnosti je obrana proti úmyslným násilným útokům, které lze zařadit do kategorie ***teroristické útoky***. V drážním průmyslu se s danými druhy útoků dosud téměř nepočítá. Jediným náznakem řízení předmětných hrozeb je znění normy EN 50 159 [22], která se zabývá komunikací mezi elektronickými systémy zajišťující bezpečnostně relevantní funkce. Předmětná norma definuje několik hrozeb, které v komunikaci vznikají v důsledku různých poruch a pohrom. Hrozbou úmyslných útoků je takzvané maskování zpráv, proti kterým se lze bránit v normě zmíněnými technikami. V daném ohledu je norma nedostatečná, protože klade požadavek pouze na integritu a autenticitu přenášených dat a nezvažuje jiné sofistikovanější kybernetické útoky (úmyslné zachytávání zpráv, opakování zpráv, čtení zpráv, využití chyb v designu komunikačních protokolů, ve správě klíčů a jiné), proto se běžně v praxi přebírají normy pro IT bezpečnost (common criteria IEC 15408) [23]

a návrh normy řady ISA 99 / IEC 62443 [24] (Security Technologies for Industrial Automation and Control Systems, tj. bezpečnostní technologie pro průmyslovou automatizaci a řídicí systémy), která ještě oficiálně nevyšla, ale certifikační autority již podle ní hodnotí a certifikují.

Z výše uvedeného lze konstatovat, že jakékoliv úmyslné útoky, tedy i kybernetické útoky, jsou prozatím nevyřešenou záležitostí a je zapotřebí vnímat předmětné útoky minimálně jako specifickou pohromu pro drážní systém.

Diplomová práce obsahuje bezpečnostní plán, který zpracovává pro vybrané specifické pohromy, konkrétně pro výpadek elektrické energie (tzv. blackout) a útok na tok informací.

1.5 Řízení rizik projektů

Řízení rizik se v mnoha případech nezabývá pouze řízení bezpečnostních rizik, ale také řízením i jiných projektových rizik. Pro konkrétní plán řízení rizik projektu výstavby nebo modernizace objektů kritické infrastruktury lze vycházek z tabulky dle zdroje [25], která se běžně používá pro řízení rizik evropských projektů. Příklad obsahu zmíněné tabulky je uveden níže.

Tabulka 1: Plán řízení rizik projektu [25].

Oblast rizika	Popis rizika	Pravděpodobnost výskytu a dopady rizika	Opatření na zmírnění rizika
Řízení	Nedostatek zdrojů nebo kvalitního personálu nebo ztráta člena týmu	Pravděpodobnost: malá Dopady: Kvalita výsledků by mohla poklesnout, protože závisí na kvalifikaci zdrojů.	1. Zajistit seminář vedoucích pracovníků projektu s cílem stanovit konsensuální řešení daného problému. 2. V konzultaci se zadavatelem projednat možnost náhrady partnera.
	Jeden člen týmu opustí řešitelský tým před ukončením projektu	Pravděpodobnost: malá Dopady: Rozsah projektu a výsledky by mohly být menší.	1. Přenést úkoly na koordinátora projektu. 2. Redukovat zdroje u jiných úkolů tak, aby výsledky všech úkolů byly na přijatelné úrovni.
	Spletité problémy (metodologie, sběr dat, problémy se strukturováním úkolů).	Pravděpodobnost: malá Dopady: Rozsah a výsledky projektu by se mohly redukovat.	1. Koordinátor projektu navrhne řešení. 2. Zajistit seminář s cílem stanovit konsensuální řešení daného problému.
	Nezávislost - prokázaný konflikt zájmů např. v důsledku využití experta pracujícího na tématu pro provozovatele	Pravděpodobnost: vysoká Dopady: neobjektivní a popř. odborně nesprávné řešení	1. Nastaveny interní procesy zadávání práce externím expertům nebo expertům s částečným úvazkem 2. Komunikace s významnými inženýrskými organizacemi a to i v zahraničí

			3. Předběžně podepsané smlouvy s významnými zahraničními TSO
Personální	Fluktuace kádrů - ztráta zkušených pracovníků odchodem do zahraničí nebo do důchodu	Pravděpodobnost: malá Dopady: nekompetentní výsledky	1. Nabídka perspektivního a stabilního zaměstnání 2. Motivační finanční ohodnocení 3. Firemní benefity
Technická	Nedostatečná kvalita dat a výsledků od některého člena týmu.	Pravděpodobnost: malá Dopady: Výsledky projektu by nemusely být spolehlivé.	1. Přenést úkoly a povinnosti na koordinátora projektu. 2. Přerozdělit úkoly, povinnosti a peníze mezi zbývající partnery.
	Některý úkol nebude splněn včas.	Pravděpodobnost: střední Dopady: Mohlo by dojít k narušení všech úkolů, celých podprojektů či celého projektu.	1. Přesunout další zdroje z jiných projektů. 2. Použít simulace výsledků nesplněného úkolu pro další úkoly. 3. Pomoc od koordinátora projektu.
	Kvalita výstupu nemá odpovídající úroveň.	Pravděpodobnost: střední Dopady: Mohlo by to ovlivnit kvalitu celého výstupu z projektu.	1. Přidělit další zdroje na příbuzné práce a zajistit vyšší kvalitu. 2. Pomoc od koordinátora projektu.
	Člen týmu odpovídající za DSS (systém pro podporu rozhodování) není schopen dodat kvalitní výsledek.	Pravděpodobnost: malá Dopady: Je ohrožen kvalitní výsledek celého projektu.	Řeší koordinátor projektu, popř. s řídícím orgánem konsorcia.
Distribuce výsledků projektu	Nedostatečný počet výstupů	Pravděpodobnost: malá Dopady: Narušen plán distribuce výsledků projektu	1. Koordinátor projektu bude po celou dobu projektu speciálně sledovat tuto oblast. 2. V řízení kvality (QA) projektu bude speciální postup zaměřený na tuto oblast.
	Příručky a návrh metodiky nebudou včas.	Pravděpodobnost: malá Dopady: Narušen plán distribuce výsledků projektu.	1. Koordinátor projektu bude po celou dobu projektu speciálně sledovat tuto oblast. 2. V řízení kvality (QA) projektu bude speciální postup zaměřený na tuto oblast.
Vnější	Změna prostředí v ČR	Pravděpodobnost: malá Dopady: Řešení projektu by ztratilo podporu zadavatele.	Koordinátor projektu bude hledat řešení jednáním se zadavatelem.
	Válka či závažná změna mezinárodní situace.	Pravděpodobnost: malá Dopady: Neschopnost dokončit úkoly. Případně hrozba náhlého ukončení projektu.	Koordinátor projektu bude hledat řešení jednáním se zadavatelem.

Výsledkem tabulky 1 je přehled rizik projektu a opatření pro jejich zmírnění. Rizika projektu následují projektový troj imperativ, tj. kvalita, čas, cena. Cílem projektového řízení je získat produkt (systém) v definované kvalitě (včetně bezpečnosti) při použití omezených zdrojů a v omezeném čase. Systémy mají ve svém životním cyklu i další fáze, které jsou kontinuálními procesy a neodpovídají projektové struktuře. Jedná se především o fáze provozu systému, monitoringu, údržby. Proto se v praxi zavádí pojem náklady na životní cyklus (LCC – Life Cycle Cost). LCC se počítá již v návrhu systému a hledá se kompromis s parametry RAMS pro zajištění celkové hospodárnosti systému. Stejně tak lze do těchto propočtů započíst i požadavky plynoucí ze SMS pomocí pětistupňového modelu. Dále je nutní v celém životním cyklu systému plány řízení rizik aktualizovat, náklady na životní cyklus a parametry RAMS přepočítávat a kontrolovat efektivitu požadovaných opatření [12].

2 Data o pražském metru a jeho řídicím systému

Každý složitější systém se skládá z několika subsystémů, vazeb a toků mezi nimi. Subsystémy lze dělit z hlediska řízení na řízené a řídicí. Vedlejší 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.

Pražské metro je velký komplexní systém. Následující kapitola obsahuje popis řízených, řídicích a zabezpečovacích subsystémů komplexního systému pražského metra. Předmětný popis je výsledkem analýzy, porovnání a syntézy poznatků z textů [26], [27], [28],[29].

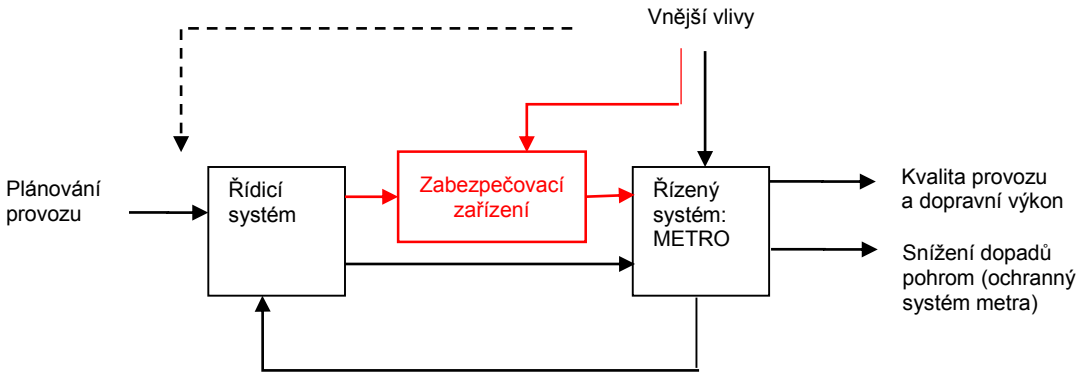
2.1 Obecný popis systému metra

Metro, 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.

Systém pražského metra plní dvě základní funkce – dopravní a ochranný. Dopravní systém je řízen ze střediska plánování městské dopravy, ze kterého vychází požadavky v podobě jízdních řádů a požadavků na kvalitu provozu dle ČSN EN 13816 [30]. Uvedené požadavky jsou vstupem do dopravního systému metra, který je určen chováním vlastních subsystémů a také různými vnějšími vlivy. Pomocí řídících a zabezpečovacích systémů dostáváme na výstupu jistou kvalitu provozu a produkt v podobě dopravního výkonu. V případě režimu ochranného systému metra, na výstupu systému dostáváme funkce snižující dopady pohrom.

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 4 ukazuje zobecněný pohled na řízený a řídicí systém.



Obr. 4: Schema řízení systému pražského metra.

Obrázek 4 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 negativní poruchy systému či negativní vnější vlivy a vykonají svojí funkci tak, aby řízený systém uvedli do bezpečného stavu, tj. stavu v které neohrozí sebe ani své okolí.

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

- stacionárních systémů – traťové, staniční a dispečerské,
- mobilních systémů – vlaky a jejich zařízení (on-board).

2.2 Pražské metro jako řízený systém

Síť metra tvoří páteř celého systému MHD v Praze. Cestující mohou využívat 57 stanic na třech linkách A, B, a C, jejichž délka činí cca 65 km [26]. Nyní jsou na trase A zprovozněny další 4 nové stanice. 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 [26] 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 a B, nese označení 81-71M a jedná se o vozy vzniklé rekonstrukcí starších sovětských vozů typu 81-71 [26].

Rozložení tras metra je znázorněno v mapě na obrázku 5.

Obr. 5: Metro Praha - mapa linek [28].

Z obrázku 5 jsou patrné barevně oddělené trasy metra A, B, C a šedou linkou je znázorněny prodloužená trasa A o nové navazující stanice, které jsou již v provozu.

2.2.1 Provozní režimy řízeného systému

Pražské metro se provozuje ve dvou základních režimech:

- dopravní systém metra (DSM),
- ochranný systém metra (OSM).

V obou režimech provozu jsou řídicí systémy v nepřetržité pohotovosti.

Režim DSM je základním režimem metra, režim OSM je použit pouze v kritických situacích, při kterých je primátorkou hl. m. Prahy vyhlášen stav nebezpečí dle zákona č 240/2000 Sb.

Jednotlivé subsystémy a zařízení pražského metra se mohou dle daných situací nacházet v různých stavech a režimů provozu. Obecně lze předpokládat, že se jedná o režimy provozu zabezpečovacích zařízení, režimy provozu sdělovacích zařízení, režimy provozu vlaku a jeho řízení, režimy při závadách na zařízení a při mimořádných událostech řízených dle metodiky Drážního úřadu a vyhlášky 376/2006 Sb. [31], která stanovuje systém bezpečnosti provozování dráhy a drážní dopravy a postupy při vzniku mimořádných událostí na dráhách. V oblasti řízení bezpečnosti je nutné uvedené režimy detailně znát a musí být popsané v interních předpisech provozovatele dráhy, které nejsou veřejně dostupné.

2.2.2 Mimořádné události v systému pražského metra

Mimořádné události jsou důsledky škodlivých jevů (pohrom), které narušují kvalitu nebo bezpečnost provozu metra. Mimořádné události v systému metra se řeší metodikou stanovenou speciálními předpisy provozu metra, vycházející z drážních předpisů a požadavků Drážního úřadu, jakožto orgánu zodpovědného za bezpečnost na drahách. Pro zvládnutí mimořádné události jsou definované postupy a metody pro jejich identifikaci, ohlášení, zmírnění dopadů, šetření, dokumentování, likvidace a uzavření mimořádné události včetně zavedení opatření k předcházení mimořádných událostí [31].

Mimořádnou událostí můžou být obecně nehody drážních vozidel v různých kategorií dle rozsahu škod, události ohrožující bezpečnost, události ohrožující plynulost provozu, dále speciální události, při kterých je nutné zavést postupy pro jejich zvládnutí [31].

Postupy pro zvládnutí mimořádných událostí jsou součástí interních předpisů provozovatele dráhy dle metodiky Drážního úřadu v souladu s vyhláškou 376/2006 Sb. [31]. Předpisy provozovatele dráhy obecně zahrnují evakuační plány, činnosti zodpovědných osob tj. dozorčí stanic, dispečeři, činnosti při požáru, činnosti při poruše zabezpečovacích zařízení, činnosti při ztrátě kontroly nad řídicím systémem, činnosti při poruše sdělovacích zařízení apod.

2.2.3 Technologie řízeného systému

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 odděleny do zvláštních kategorií.

Zdroj [27] uvádí následující technologické systémy:

- energetická zařízení,
- měnírny a distribuční transformovny (pozn. Trasy stanice metra jsou napájeny několika napájecími zdroji 22 kV, každá stanice má navíc svůj záložní zdroj UPS v případě výpadku el. energie, zabezpečovací a řídicí systémy mají navíce vlastní nezávislé zdroje.),
- sdělovací zařízení,
- sdělovací kabely, VKV spojení s vlaky, Automatické odbavování cestujících,
- zařízení průmyslové televise, Telefonní zřízení, Rozhlasové zařízení,

- hodinové zařízení, Elektrická požární signalizace,
- elektrická zabezpečovací signalizace,
- strojní zařízení:
  - pohyblivé schody ve stanicích,
  - čerpací stanice ve stanicích a mezistaničních úsecích,
  - výtahy ve stanicích,
  - dílny a sklady údržby ve stanicích,
- vzduchotechnická zařízení:
  - hlavní větrání,
  - staniční vzduchotechnika,
- mobilní stroje a zařízení (vozový park),
- zařízení a prostředky pro čištění odpadu zahrnují mycí a zametací vozíky, kontejnery na odpad a soustavu žebříků a lešení pro čištění osvětlovací techniky;
- prostředky požární ochrany umístěné ve stanicích, které umožňují rychlý zásah při požáru v podzemních prostorách.

2.2.4 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:

- 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 (viz následující odstavec 2.2.5) 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 interlocking.

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.

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). 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 vedením vlaku. Záleží, na jaký režim jízdy je vlak 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. V pražském metru se provozují tři systémy VZZ, tj. zařízení LZA, ARS a zařízení MATRA.

Ve vybrané modelové stanici metra je instalován francouzský systém vlakového zabezpečovače MATRA s kontrolou rychlosti jízdy vlaků, kontrolou sledu vlaků a se zařízením pro automatické vedení vlaku.

2.2.5 Řídicí systém pražského metra

Řídicí systémy pražského metra nesou název ASDŘ, což znamená automatizovaný systém dopravního řízení. Z hlediska evropských norem ani z hlediska provozu se nejedná o zcela přesný název, ale je již řadu let zaveden.

Dispečerská pracoviště jsou umístěna na následujících stanovištích pro každou trasu metra (A, B, C) zvlášť:

- 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 diplomové práce jsou důležité systémy 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.

Další funkcí ASDŘ-D jsou vzdálená ovládání technologií a zabezpečovacích zařízení, zde se už může jednat o bezpečnostně relevantní příkazy, které plní určité bezpečnostní funkce a jejich chybné provedení může zapříčinit nehodu. Například špatně zvolený rychlostní stupeň 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 též 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 [32], popsaného dále.

2.2.6 Systémy UGTMS dle EN 62290

Systémy pro řízení městské a příměstské dráhy (UGTMS – Urban Guided Transport Management and command/control System) jsou definovány normou EN 62290 [32]. Norma je rozdělena do tří částí. První část definuje stupně automatizace řízení, takzvané GOA (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 má obsahovat bezpečnostní požadavky na systém, tato část dosud nevyšla, je v připomínkovém řízení.

V případě plně automatizovaného provozu, bez strojvedoucího nebo bez obsluhy, jsou specifikované bezpečnostní požadavky na systém v normě EN 62267 [33].

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

Tabulka 2: Stupně automatizace [32].

Základní funkce provozu vlaku		Provoz vlaku podle rozhledu	Neautomatizo-vaný provoz vlaku	Poloautomatizo-vaný 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 2 rozděluje základní funkce systému podle dané stupně automatizace. Jeslitliže pražské metro definujeme jako systém režimu GOA2 dle [32], 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 rozhaní se subsystémy uvedenými v předmětné normě, pokud jsou použity. Tabulka 3 rozhraní, prostředí a systémové hranice popisuje v souladu se zmiňovanou normou [32] a srovnává je s reálným stavem provozu Pražského metra.

Tabulka 3 Požadavky na rozhraní systému.

Legenda tabulky:

Tučně vyznačené položky jsou v řízeném systému využívány a jsou součástí řídícího systému.

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, počátače 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 nechtáněného 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 mezivozidlové propojky)*
	Rozhraní s personálem obsluhy vlaku
	Zařízení pro detekci překážek, vykolejení, ohně/kouře
	Detekce nechráněného prostoru, zařízení pro uzavření nechráněného prostoru
	Rukojeť pro nouzové zastaveníPuvolnění dveří/nouzové tlačítko
	Rozhraní s jinými zařízeními (např. s osvětlením, vytápěním, větráním, klimatizaccí (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 uvažované, nicméně v případě dalšího rozvoje bude nutné funkce instalovat.

3 Metody zpracování dat

Pro účely předložené diplomové práce je využita řada metod. Předmětné metody slouží k získání informací o entitě, identifikaci relevantních pohrom, určení jejích četností a dopadů na entitu pro určení jejich kritičnosti (tj. pohroma relevantní, specifická a kritická), vypracování bezpečnostního plánu a také provedení porovnání získaných výsledků práce s reálným stavem a informacemi uvedenými v předchozích kapitolách.

3.1 Standardní metody zpracování dat

Metody sběru dat jsou dle [8] techniky získávání dat, které dělíme na přímé či nepřímé pozorování, které jsou zaměřené na plánované vnímání vybraných jevů a jsou pak systematicky zaznamenávány. Pro účely předložené diplomové práce bylo dále pro sběr dat využito strukturovaného rozhovoru a analýze dokumentů. Strukturovaný rozhovor získává vyžadované informace v přímé interakci s respondentem. Rozhovor může být prováděn „face-to-face (z očí do očí)“, nebo přes nějaké komunikační medium (telefon, mail apod.). Analýza dokumentů je analýza jakýchkoliv dokumentů, které nebyly vytvořeny za účelem předmětného výzkumu.

Analýza je dle [8] myšlenkový (logický) postup poznávání okolního světa a v něm vymezených objektů, jevů procesů a problémů (reálných i abstraktních).

Syntéza je dle [8] logickým doplňkem analýzy; je procesem sjednocení částí, vlastností a vztahů vydělených analýzou v jeden celek. Je to postup poznávání nebo konstrukce systémů, jehož podstatou je myšlenkové nebo praktické spojování známých prvků do jednoho celku.

Hodnocení je dle [8] metoda stanovení hodnoty sledované entity v dané hodnotové stupnici.

Srovnání (komparace) dle [8] je technika porovnávání objektů či předmětů sledování s poznávacím, určujícím a rozlišujícím znakem s cílem stanovit jejich shodné a rozdílné znaky, tj. ***metoda shody*** dle příslušné ČSN [3] . Má významnou roli v úsudcích založených na analogii. Metoda porovnání podobností je založena na tvůrčím myšlenkovém procesu, jehož cílem je vyhledávání objektů, které jsou tvarem, složením, rozměry, hmotností apod. podobné výrobku nebo procesu, jenž je předmětem racionalizace [8].

Procesní model dle [8] slouží k detailní identifikaci a specifikací procesů, jejich struktury, vstupů, výstupů, omezení apod. Modelování je technika, kterou vytváříme analogicky (potřebně zjednodušený) obraz reálného procesu/systému a na něm sledujeme zkoumané souvislosti.

3.2 Procesní model

Výsledky předložené práce byly získány na základě aplikace tří procesních modelů. Procesní model je zobrazení logického postupu výstavby výsledků [8]. První je proces vytvoření Bezpečnostního plánu, druhý je k porovnání výsledků s reálným stavem a třetí navrhuje plán řízení rizik. Procesy v sobě zahrnují skupinu úkolů uvedených v následujícím seznamu.

1. Bezpečnostní plán obsahuje položky:
    - získání informací o entitě,
    - hledání relevantních pohrom příslušných vybrané entitě,
    - stanovení ohrožení a identifikace četností,
    - určení dopadů na chráněná aktiva (metoda What, If),
    - matice odpovědnosti pro jednotlivé pohromy,
    - sestavení bezpečnostního plánu pro jednotlivé pohromy (prevence, ochrana-zmírnění, scénáře odezvy, scénáře obnovy, vzdělávací systém, cvičení).
2. Porovnání výsledků s reálným stavem obsahuje položky:
    - porovnání údajů v bezpečnostním plánu s aktuálními opatřeními řízení bezpečnosti,
    - nalezení slabých míst,
3. Plán řízení rizik:
    - návrh opatření ke zvýšení bezpečnosti,
    - návrh obecného plánu řízení bezpečnostní a plánu vybraný objekt.

Následující odstavce popisují některé specifické metody pro splnění uvedených úkolů.

3.2.1 Získání informací o entitě (chráněná aktiva, specifické zranitelnosti)

Pro získání dat pro vypracování práce jsou využity veřejně dostupné zdroje a znalosti uvedené v kapitole 2. Při práci s riziky je nezbytné pracovat s datovými soubory, které jsou reprezentativní, tj.: úplné; obsahují správná data; mají dostatečný počet dat; data musí být rozprostřena homogenně v celém sledovaném intervalu a musí být validovaná [3].

3.2.2 Hledání relevantních pohrom náležících vybrané entitě

All-Hazard-Approach bere v potaz všechny relevantní pohromy pro danou oblast. Výpis relevantních pohrom pro řešenou entitu je uveden v odstavci 1.2. Pro relevantní pohromy se identifikují četnosti výskytu a dopady na entitu, klasifikují se a provádí příslušná opatření (prevence, plány odezvy, obnovy a monitoring).

3.2.3 Stanovení ohrožení a identifikace četností dle zdroje

Stanovení ohrožení znamená určení velikosti jevu, který se opakuje za určitý časový interval, a proti kterému se dělají opatření [3]. Četnost opakovaných událostí lze popsat metodou doby návratu a roční pravděpodobností překročení. Ohrožení souvisí s pohromou a nikoliv s místem chráněného aktiva, které sledujeme.

Stanovení ohrožení se prování například metodou založenou na teorii extrémních hodnot, pomocí teorie mezních odhadů na základě scénářů minulých pohrom, pomocí obalové křivky všech možných scénářů, měřením nejméně příznivého scénáře a nejméně příznivého scénáře pro největší očekávanou pohromu [2].

Pro klasifikaci pohromy je zapotřebí stanovit četnost dané pohromy dle tabulky 4.

Tabulka 4: Tabulka četností a pravděpodobnosti výskytu pohrom dle zdroje [7].

Četnost:	Pravděpodobnost výskytu:
menší než 10^{-6} / rok,	pravděpodobnost zanedbatelná,
v rozmezí 10^{-5} / rok až 10^{-6} / rok,	pravděpodobnost velmi malá,
v rozmezí 10^{-4} / rok až 10^{-5} / rok,	pravděpodobnost malá,
v rozmezí 10^{-3} / rok až 10^{-4} / rok,	pravděpodobnost střední,
v rozmezí 10^{-2} / rok až 10^{-3} / rok,	pravděpodobnost vysoká,
větší než 10^{-2} / rok.	pravděpodobnost velmi vysoká.

3.2.4 Metoda What, IF pro určení dopadů na chráněná aktiva

Dle zdroje [7] je What, IF - analýza toho, co se stane když, je postup na hledání možných dopadů vybraných provozních situací. V podstatě je to spontánní diskuse a hledání nápadů, ve které skupina zkušených lidí dobře obeznámených s procesem klade otázky nebo vyslovuje úvahy o možných nehodách. Není to vnitřně strukturovaná technika jako některé jiné (např. HAZOP a FMEA). Namísto toho po analytikovi požaduje, aby přizpůsobil základní koncept šetření určitému účelu.

Prvním bodem analýzy je definování oblasti zájmu a cílových zájmů (finanční rizika, životní prostředí, majetek a zdraví lidí, chráněná aktiva). Dále se vytvoří tabulka se dvěma až třemi sloupci popisující možné dopady při různých pohromách:

- možné dopady na životy a zdraví lidí,
- možné dopady na bezpečí lidí,
- možné dopady na majetek,
- možné dopady na veřejné blaho,
- možné dopady na životní prostředí,
- možné dopady na infrastruktury a technologie.

Možné dopady na infrastruktury a technologie se dále člení na:

- možné dopady na dodávky energií (elektřina, teplo, plyn),
- možné dopady na systém dodávky vody,
- možné dopady na kanalizační systém,
- možné dopady na přepravní síť,
- možné dopady kybernetickou infrastrukturu (komunikační a informační sítě),
- možné dopady na bankovní a finanční sektor,
- možné dopady na nouzové služby (policie, hasiči, zdravotníci),
- možné dopady na základní služby v území (zásobování potravinami, likvidace odpadů, sociální služby, pohřební služby), průmysl a zemědělství,
- možné dopady na státní správu a samosprávu.

Pro zohlednění veřejného zájmu se používá metoda ve formě tabulky [3].

Tabulka 5: Příklad tabulky What, If.

If (Když?)	Možné dopady:	What (co se stane?):
Pohroma	život a zdraví lidí, Majetek.	možné poranění osob, možné ztráty na majetku.

Rozsah dopadů – používá se verbální stupnice dle zdroje [2]:

0 - dopady zanedbatelné,
1 - dopady velmi malé,
2 - dopady malé,
3 - dopady střední,
4 - dopady vysoké,
5 - dopady velmi vysoké.

Pro účely bezpečnostního plánu je hodnotová stupnice pro uvedení dopady následující:

0 – dopady, které nemají vliv na bezpečnost,
1 – dopady, které mají značný vliv na kvalitu dopravy, mohou ovlivnit bezpečnost při kombinaci s jinou pohromou či poruchou některých zařízení, může dojít ke zranění lidí,
2 – může dojít ke ztrátě kontroly k některým zařízením, výpadku či poškození některých zařízení, větší ztráty na majetku, možné zranění více lidí, možné úmrtí 1 – 2 lidí,
3 – ztráta kontroly nad vzniklou situací, velké ztráty na majetku lití i provozovatele dráhy, dopady na chráněná aktiva, možná úmrtí a zranění více lidí (do 10),
4 – stupeň 3 + velké dopady na veřejná aktiva území, ve kterém se objekt nachází, velké ztráty na majetku lidí i provozovatele dráhy, možná úmrtí a zranění velkého počtu lidí (nad 10),
5 – stupeň 4 + může vést k destabilizaci území a případně i státu, vliv na chráněná aktiva státu, vnější projevy pohromy, obrovské ztráty na životech a majetku.
Klasifikace pohrom se provádí za využití četností a rozsahu dopadů dle metodiky popsané v odstavci 1.2 a dle obrázku 2.

3.2.5 Matice odpovědnosti

Na zvládnutí kritických pohrom se musí podílet všechny orgány státní správy, právnické a fyzické osoby a také občané. Proto se soustřeďuje pozornost na základní funkce území (kritickou infrastrukturu), které zajišťují život společnosti.

Zabezpečení každé základní funkce území koordinuje resort, který je určen zákonem č. 2/1969 Sb. [34] nebo vládou. Předmětný resort má primární odpovědnost za zvládnutí situace a ke splnění dané povinnosti mu pomáhají resorty spolupracující. K zajištění přehlednosti se sestavují matice odpovědnosti. Ve sloupcích matice jsou uvedeny názvy resortů, právnických a fyzických osob a v řádcích matice jsou uvedeny základní funkce území či jednotlivé činnosti, o jejichž zajištění jde.

Odpovědnosti resortů jsou stanoveny bez ohledu na pohromu, a to proto, že jde o zajištění stability území, existence státu a jeho funkcí za každých podmínek. Teprve na úrovni resortů se stanovují způsoby, jak resort zajistí svou odpovědnost při různých kritických pohromách s ohledem na jejich specifika. Pro jednotlivé kritické pohromy se matice odpovědnosti sestavují pro monitorování, hodnocení, preventivní opatření, zmírňující opatření, odezvu a obnovu.

Matice odpovědnosti je tabulka, ve které jsou ve sloupcích názvy rezortů a v řádcích základní funkce, resp. činnosti. Ve výsledné matici se pro určitý úkol přiřazuje primární odpovědnost daného resortu písmenem P, sekundární odpovědnost spolupracujících rezortů se značí S [5].

3.2.6 Bezpečnostní plán

Bezpečnostní plán je koncepční dokument, který určuje strategii pro zajištění bezpečnosti s ohledem na konkrétní pohromu [3]. Bezpečnostní plán se dle zdroje [3] skládá z:

- stručného popis entity (místopis, chráněná aktiva, specifické zranitelnosti chráněných aktiv),
- seznamu pohrom, které mohou entitu postihnout, a jejich rozdělení na relevantní, specifické a kritické,
- sestavení reprezentativních scénářů dopadů specifických a kritických pohrom (simulace provedené metodou What, If),
- popisu systematických preventivní opatření v územním plánování, výstavbě a provozu entit (součástí bezpečnostního plánu modelové pohromy),
- scénářů odezvy na specifické pohromy (součástí bezpečnostního plánu modelové specifické pohromy),
- scénářů odezvy na kritické pohromy (součástí bezpečnostního plánu modelové kritické pohromy),
- plánů konkrétních činností, které jsou potřebné při odezvě (součástí bezpečnostního plánu modelové pohromy)
- plánů obnovy po pohromách většího rozsahu.

3.2.7 Plán řízení rizik

Plán řízení rizik aplikuje v práci navržená opatření a je navržen ve struktuře, která je v souladu s kapitolou 1, tabulka 1.

4 Bezpečnostní plán

Předložený bezpečnostní plán obsahuje následující body odvozené z obecného plánu dle odstavce 3.2.7:

- stručný popis entity, místopis a její chráněná aktiva,
- seznam pohrom a jejich rozdělení,
- scénáře dopadů specifických a kritických pohrom a jejich klasifikace,
- bezpečnostní plán pro zvládnutí jednotlivých pohrom, tj. prevence, ochrana a scénáře odezvy,
- plán obnovy.

Bezpečnostní plán je metodickým návrhem a obsahuje pouze dva plány pro dvě vybrané pohromy: selhání technologií (výpadek elektřiny), teroristický útok (na tok informací). Pro řízení bezpečnosti v reálném prostředí je nutné vypracovat plány pro všechny relevantní pohromy dle All-Hazard-Approach.

Jelikož jednotlivé stanice metra se liší ve svých parametrech i bezpečnostních prvcích, byla sestavena modelová stanice, zachycující zásadní prvky, vazby a spřažení vytvořená toky, aby byly získané obecné závěry. Pro řešení odlišných rysů je třeba použít důkladnější charakteristiky, jejichž publikace ve veřejné diplomové práci není možná.

4.1 Stručný popis entity

Odstavec obsahuje stručný popis entity dle [26] a [27] s místopisem a identifikací chráněných aktiv.

4.1.1 Obecné informace

Předmět: stanice pražského metra.

Vlastník: hl. město Praha.

Provozovatel: Dopravní podnik hlavního města Prahy, akciová společnost.

Umístění: severovýchodní okraj Prahy,

jihovýchodně od křižovatky ulic (T x B).

Konstrukce: uzavřený monolitický železobetonový rám se zalomenou základovou deskou; délka 592 m vč 250 odstavné koleje.

Vzdálenost k následující stanici: 1836 m tunelem po trase dráhy.

Režimy provozu: dopravní; (tato stanice neplní ochranné funkce OSM).

Prostory: úroveň vestibulů, úroveň nástupiště, úroveň pod nástupištěm, prostor obratových a odstavných kolejí, dispečink PID.

Přístup do objektu: severní vestibul (5 východů; obsluha MHD, PID, PVA. R+P)

jižní vestibul (3 východy; nezpřístupněn veřejnosti)

únikové schodiště u obratových a odstavných kolejí

1. a 2. kolej – příjezdy resp. odjezdy ve směru sousední stanice.

Počet cestujících: průměr v období ranní špičky celkem 11 800 lidí (5 900 / hod.)

průměrný počet na nástupišti ve špičce cca 200 lidí.

Minimální interval mezi vlaky: následné jízdy 90 s.

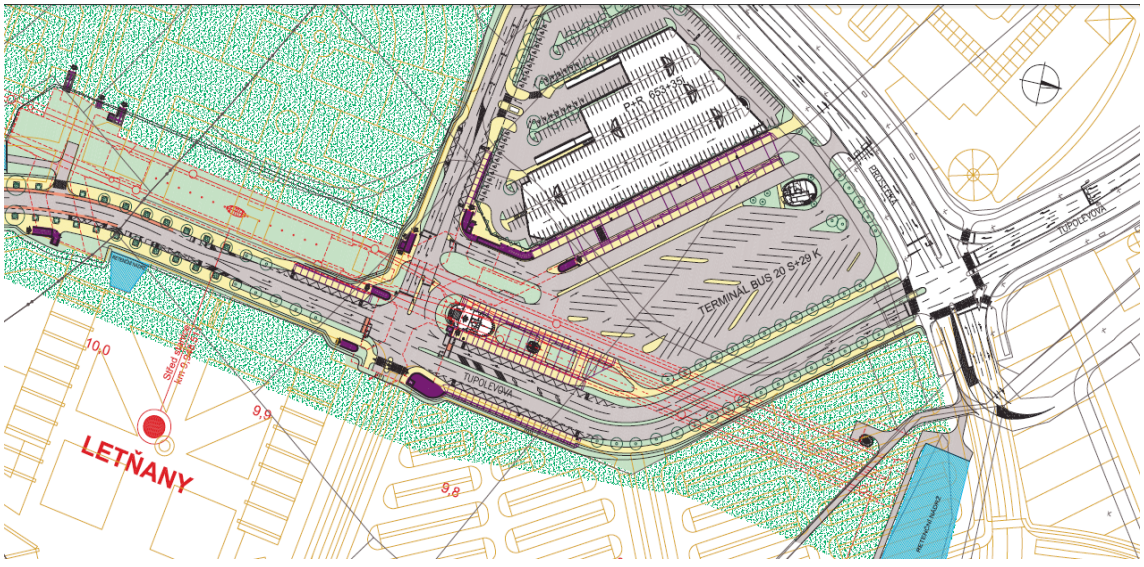
Provozní interval jízdy: 110 s.

Maximální povolená rychlost: 80 km/h.

Kapacita vlaku: 545 cest/vlak (pro standard kvality 2,6 lidí stojící/m^2).

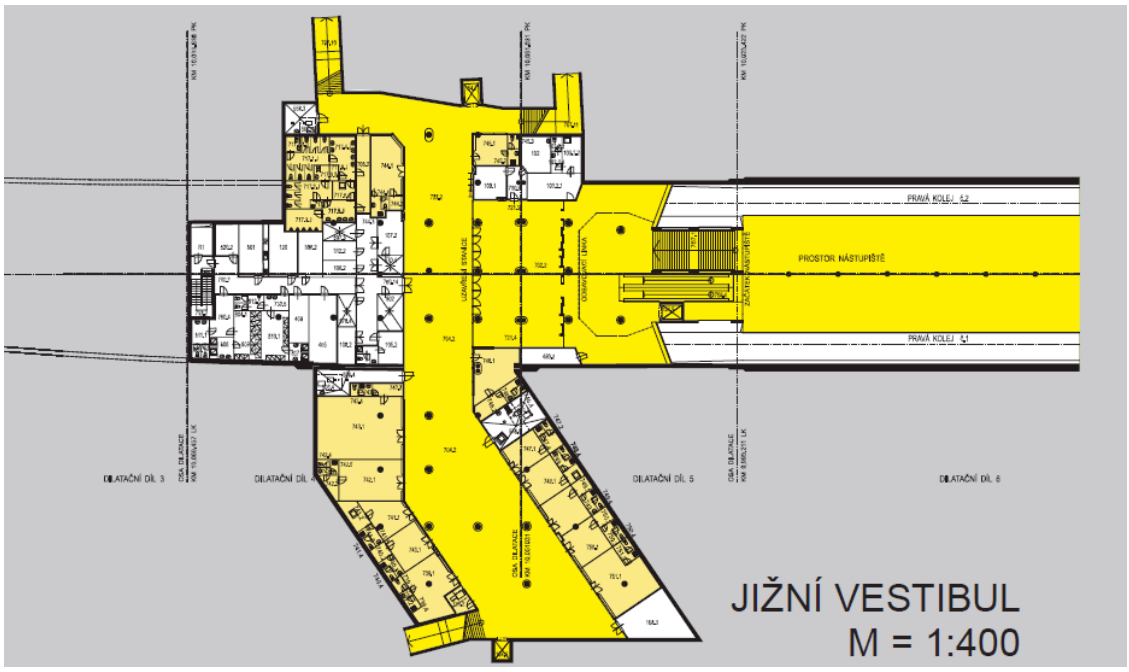
Počet vlaků ve stanici: ve stanici je možné deponovat až 6 vlakových souprav složených z 5 vozů.

Následující obrázky 6-9 znázorňují reálné prostředí vybrané stanice metra.



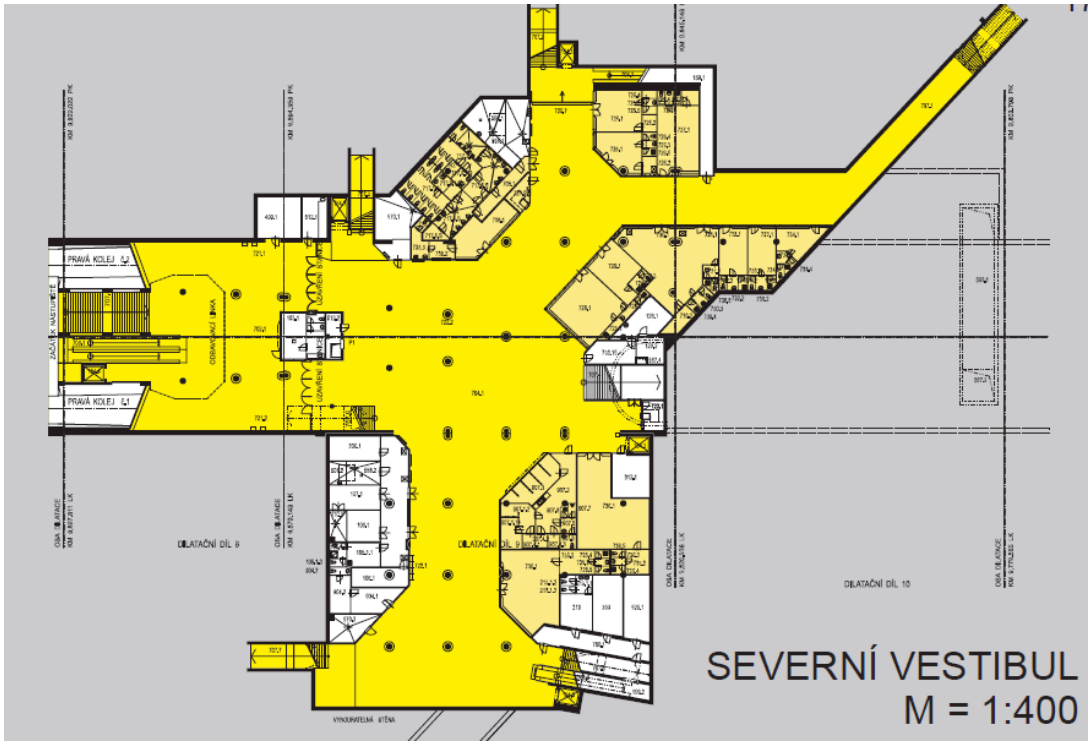
Obr. 6: Vnější prostory vybrané stanice [27].

Na obrázku 6 je červenými čarami znázorněná stanice metra zobrazená na vnější ploše parkoviště P+R a okolí.



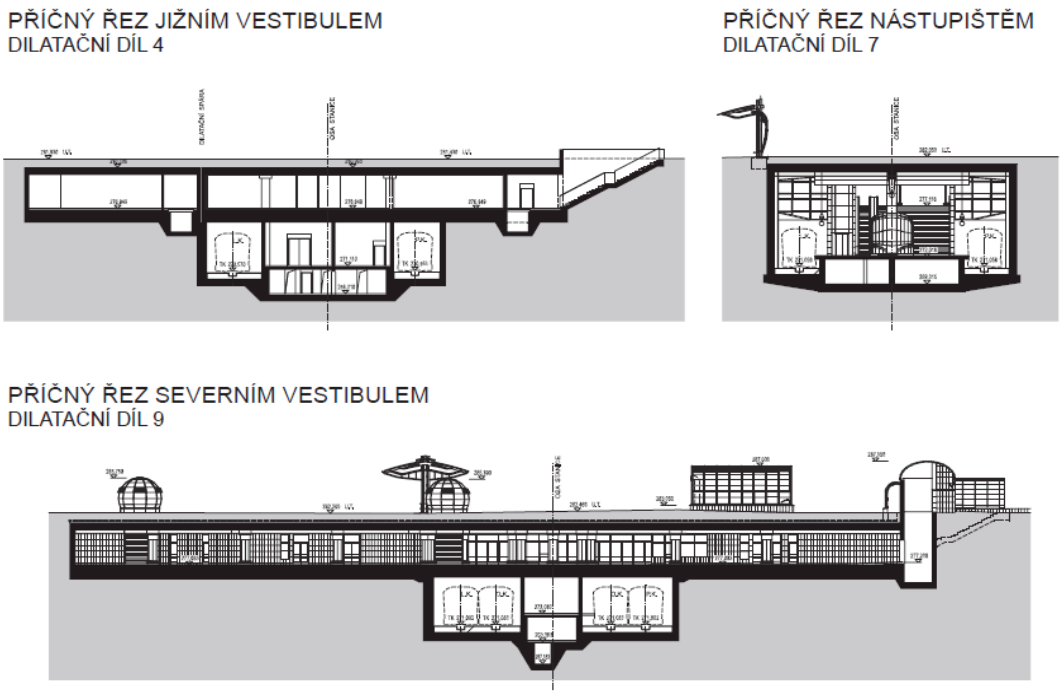
Obr. 7: Jižní vestibul vybrané stanice [27].

Obrázek 7 zachycuje půdorys jižního veřejně nepřístupného vestibulu.



Obr. 8: Severní vestibul vybrané stanice [27].

Obrázek 8 zachycuje půdorys severního vestibulu.



Obr. 9: Příčné řezy stanice [27].

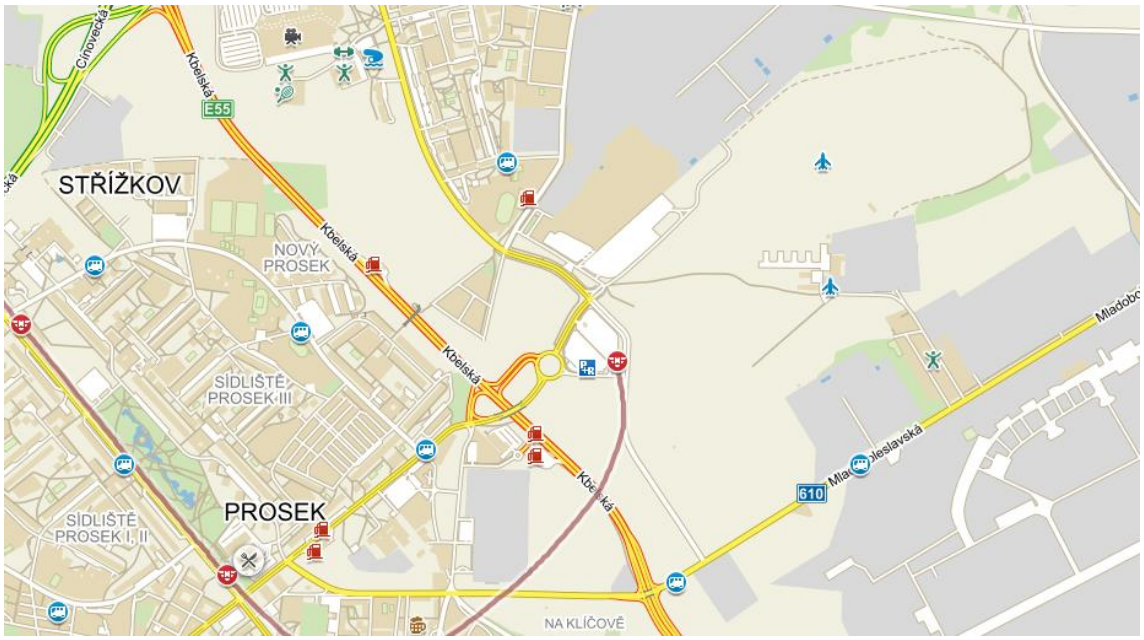
Obrázek 9 zachycuje vybrané příčné řezy stanicí metra.

4.1.2 Místopis

V těsné blízkosti vybrané stanice se vyskytuje silnice E v ulici K, která křižuje dopravně důležité ulice M, P a C. Ulice C dále navazuje na rychlostí silnici a následně na dálnici.

Stanice díky své situaci navazuje na autobusovou dopravu obsluhující okolní oblasti. Spojuje také dálkovou dopravu a navazuje na IAD z mimopražských oblastí ukončenou parkovištěm typu P+R.

Důležitými objekty v řešené lokalitě jsou především blízká obchodní střediska, obytné zóny, parkoviště, školy a areál výstaviště nebo letiště, jak je znázorněno na následující mapce.



Obr. 10: Mapa [35].

Obrázek 10 zachycuje mapu vnějšího okolí modelové stanice metra, stanice metra je znázorněna uprostřed obrázku červeným symbolem „M“.

4.1.3 Chráněná aktiva veřejná (okolí)

Analyzovaná chráněná aktiva okolí jsou znázorněna na obrázku 11, přičemž oblast x je oblastí řešené stanice včetně parkoviště a návazných nástupišť na navazující dopravní obsluhu. Písmeny jsou označena jednotlivá chráněná aktiva, která podrobněji popisuje tabulka pod obrázkem.

Obr. 11: Mapa obecných chráněných aktiv.

Obrázek 11 na mapě okolí stanice metra znázorňuje veřejná chráněná aktiva v okolí stanice s jejich písemným označením a směrem.

Popis označených veřejných chráněných aktiv obsahuje tabulka 6.

Tabulka 6: Veřejná chráněná aktiva okolí

Chráněná aktiva:		Dosah [m]:	Předmět ohrožení:	Hrozby:
X	parkoviště P+R,	0	lidi, majetek lidí (auta),	výbuch, požár, únik chemických látek,
	autobusové zastávky,	0	lidi, majetek PID (autobusy),	výbuch, požár, únik chemických látek,
	PID dispečink,	0	??	??
A.	křižovatka K – P,	350	lidi, infrastruktura, auta,	výbuch, požár, únik chemických látek,
B.	obytná zóna,	420	lidi, majetek lidí,	požár, nemoci, nákaza,
C.	čerpací stanice,	330	lidi, majetek, auta, pohonné hmoty,	výbuch, požár, únik chemických látek,
D.	výstaviště,	350	lidi, majetek lidí a vystavovatelů, auta,	výbuch, požár, nemoci, nákaza, únik chemických látek,
E.	nákupní centrum, autoservis a STK, parkoviště,	400	lidi, majetek, auta,	výbuch, požár, nemoci, nákaza, únik chemických látek,
F.	čerpací stanice,	570	lidi, majetek, auta, pohonné hmoty,	výbuch, požár, únik chemických látek,
G.	škola, sídliště,	510	lidi, majetek,	požár, nemoci, nákaza,
H.	civilní letiště,	630	lidi, majetek, letadla,	výbuch, požár, únik chemických látek, pád letadla,
I.	mateřská škola, sídliště,	650	lidi, majetek,	požár, nemoci, nákaza,
J.	křižovatka K – M,	760	lidi, infrastruktura, auta,	výbuch, požár, únik chemických látek,
K.	vojenské letiště,	1000	lidi, vojenský prostor, letadla,	výbuch, požár, únik chemických látek, pád letadla, jiné,
L.	parkoviště autobusů,	500	lidi, majetek, autobusy,	výbuch, požár, únik chemických látek,
M.	akademie věd.	900	lidi, majetek.	požár, nemoci, nákaza, jiné.

Z tabulky 6 jsou patrné důležité informace o veřejných aktiv v okolí stanice metra, které mohou být ohroženy, mohou způsobit zřetězení událostí a mohou být původcem nepříznivých událostí. Tabulka 6 uvádí předmět ohrožení obecného aktiva a možné hrozby.

4.1.4 Chráněná aktiva stanice

Z údajů v předchozích kapitolách a z relevantních zdrojů [26],[27],[29] byla identifikována následující chráněná aktiva stanice.

Životy a zdraví:

- životy a zdraví cestujících,
- životy a zdraví zaměstnanců,
- pracovní prostředí.

Majetek (technologie, infrastruktura, objekty, zařízení,…)

Místa:

- veřejné prostory (severní vestibul, nástupiště, soupravy metra),
- shromažďovací místo,
- technologické místnosti (stavědlo, reléová místnost),
- stanoviště dozorčího.

Energetická zařízení:

- měnírny a distribuční transformovny.

Sdělovací zařízení:

- sdělovací kabely, VKV spojení s vlaky,
- automatické odbavování cestujících,
- zařízení průmyslové televise, telefonní zřízení, rozhlasové zařízení,
- hodinové zařízení, elektrická požární signalizace,
- elektrická zabezpečovací signalizace.

Strojní zařízení:

- pohyblivé schody ve stanicích,
- čerpací stanice ve stanicích a mezistaničních úsecích,
- výtahy ve stanicích,
- dílny a sklady údržby ve stanicích.

Vzduchotechnická zařízení:

- hlavní větrání, staniční vzduchotechnika.

Mobilní stroje a zařízení:

- vozový park,
- zařízení a prostředky pro čištění odpadu zahrnují mycí a zametací vozíky,

kontejnery na odpad a soustavu žebříků a lešení pro čištění osvětlovací techniky,

- prostředky požární ochrany umístěné ve stanicích, které umožňují rychlý zásah při požáru v podzemních prostorách.

Ostatní důležitá zařízení:

- bezpečnostní a poplachová tlačítka,
- zařízení pro vyhlášení požárního poplachu,
- trakční zařízení a osvětlení,
- traťová zařízení, hlavní uzávěr vody,
- pohyblivé schody, plošiny, signální panel strojního zařízení,
- uzavírací zařízení (el. rolety).

Staniční jednotky řídicího systému ASDŘ:

- staniční uzel ASDŘ-D,
- staniční jednotka automatického stavění jízdních cest,
- staniční uzly s návazností na energetický a technologický dispečink,
- staniční uzly systému centrálního ovládání osvětlení,
- staniční uzly s návazností na dispečink sdělovací, zabezpečovací a dispečink hasičů.

Zabezpečovací zařízení:

- staniční zabezpečovací zařízení (ESA 11 M),
- traťová zabezpečovací zařízení (AŽD 71, ESA 11 M),
- vlaková zabezpečovací zařízení (MATRA a vozové jednotky).

Toky:

energetické toky,

informační toky:

- centrální dispečink – staniční uzly ASDŘ,
- centrální dispečink – staniční sdělovací zařízení,
- staniční uzly ASDŘ – zabezpečovací zařízení,
- staniční uzly ASDŘ – sdělovací zařízení,
- zabezpečovací zařízení – technologie (traťové, vlak),
- telefonní spojení mezi centrálním dispečinkem a stanicí,
- telefonní spojení mezi centrálním dispečinkem a vlakem.

4.2 Seznam pohrom, které mohou entitu postihnout

All-Hazard-Approach [4] požaduje zvažovat všechna možná ohrožení (pohromy), vychází z konceptu integrální bezpečnosti stanoveného v OSN roku 1994 [36] a přijatém EU v roce 2000 [37]. V daném případě jde o zvážení všech pohrom definovaných pro dané území uvedených v odstavci 1.2.2.

Metodou srovnání a bližší analýzy textů zdrojů [5],[6] a první kapitoly diplomové práce, byla provedena kategorizace relevantních pohrom, viz bulka 7.

Tabulka 7 Rozdělení 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

Z tabulky 7 vyplývá celkem 33 relevantních pohrom, 21 specifických pohrom a z toho 14 pohrom kritických. Pro každou identifikovanou pohromu je zapotřebí provádět příslušná opatření dle stanovené metodiky.

4.3 Scénáře dopadů dvou vybraných pohrom

Scénáře dopadů jsou z důvodu rozumného rozsahu diplomové práce vypracované pouze pro dvě vybrané pohromy, kterými jsou selhání technologií, konkrétně výpadek elektřiny (black out), a teroristický útok na tok informací. V praxi je ovšem nutné pro zajištění bezpečnosti vypracovat scénáře dopadů pro každou relevantní pohromu.

4.3.1 Výpadek elektřiny (black out)

Výpadkem elektřiny je míněn úplný výpadek vnějších zdrojů energie (tzv. „black out“) nebo selhání více zařízení zdroje energie. Scénáře dopadů pro úplný a dlouhodobý výpadek elektrické energie je analyzován níže metodou WHAT, IF. Analýza je rozdělena do dvou tabulek, první zachycuje dopady na veřejná (resp. vnější) aktiva a druhá na konkrétní (resp. vnitřní) aktiva stanice. Určení četností je velmi složité, avšak lze předpokládat, že výpadek elektrické energie eliminujeme zavedením náhradních zdrojů a velmi zde záleží na době obnovy. Velikost dopadů je odvozena z tabulek WHAT, IF níže a metodami uvedenými v kapitole 3.

Tabulka 8: Analýza WHAT, IF pro výpadek elektřiny a vliv na okolní aktiva.

If (Když?)	Možné dopady na veřejná aktiva:		What (co se stane?)
Když dojde k výpadku elektřiny ve stanici metra	Možné dopady na životy a zdraví lidí.		ušlapání, vážné či smrtelné úrazy z důvodu paniky v těsné blízkosti okolí entity
	Možné dopady na bezpečí lidí.		vznik paniky
	Možné dopady na majetek.		rabování, krádeže v okolí entity
	Možné dopady na veřejné blaho.		omezení dopravní obslužnosti
	Možné dopady na životní prostředí.		znečištění, kontaminace technickými kapalinami a odpadem
	Možné dopady na infrastruktury a technologie:	možné dopady na dodávky energií (elektřina, teplo, plyn)	výpadek elektřiny pro další 3 stanice metra, výpadek vzduchotechniky, větrání
		možné dopady na systém dodávky vody	Vytopení a zaplavení pokud dojde k poruše vodovodního řádu
		možné dopady na kanalizační systém	porucha čerpadel, znečištění, zaplavení stanice
		možné dopady na přepravní síť	výpadek dopravního spojení; nutné zavést náhradní autobusovou dopravu
		možné dopady na kybernetickou infrastrukturu (komunikační a informační sítě)	výpadek spojení s centrálním dispečinkem a okolními stanicemi, výpadek komunikačních sítí v metru
		možné dopady na bankovní a finanční sektor	nutné odškodnění poškozených, obnova majetku, velké finanční dopady
		možné dopady na nouzové služby (policie, hasiči, zdravotníci)	obsazení zdrojů
		možné dopady na základní služby v území (zásobování potravinami, likvidace odpadů, sociální služby, pohřební služby), průmysl a zemědělství	Narušení dopravní obslužnosti, lidé se nedostanou do práce, nemocnic aj.
		možné dopady na státní správu a samosprávu.	zatížení finančních a lidských zdrojů, nedůvěra občanů ke službám státu

Tabulka 9: Analýza WHAT/IF pro výpadek elektřiny a vliv na aktiva stanice.

If (Když?)	Možné dopady na aktiva stanice:		What (co se stane?)
Když dojde k výpadku elektřiny ve stanici metra	Životy a zdraví lidí:		-
	životy a zdraví cestujících		možné úmrtí více lidí, možné zranění více lidí, možné trvalé následky
	životy a zdraví zaměstnanců		možné úmrtí více lidí, možné zranění více lidí, možné trvalé následky
	pracovní prostředí		nedostatek světla, zatopení a znečištění prostorů,
	Majetek:		-
	Místa:	veřejné prostory (severní vestibul, nástupiště, soupravy metra)	výskyt velkého množství lidí, ***panika, možnost ušlapání***
		shromažďovací místo	výskyt velkého množství lidí, ***panika, možnost ušlapání***
		technologické místnosti (stavědlo, reléová místnost)	výpadek zařízení, znemožnění stavění jízdních cest a řízení dopravy
		stanoviště dozorčího	znemožnění dohledu a řízení

Energetická zařízení	Měnírny a distribuční transformovny	výpadek zařízení; výpadek napájení ostatních technologií – toky
Sdělovací zařízení	sdělovací kabely, VKV spojení s vlaky, automatické odbavování cestujících	výpadek zařízení; znemožněné komunikace s centrálou a vlakem
	zařízení průmyslové televise, telefonní zřízení, rozhlasové zařízení;	výpadek zařízení; znemožnění komunikace
	hodinové zařízení, elektrická požární signalizace;	výpadek zařízení; ztížení hašení v případě požárů
	elektrická zabezpečovací signalizace	výpadek zařízení znemožnění dohledu
Strojní zařízení	pohyblivé schody ve stanicích	výpadek zařízení; ztížení pohybu cestujících; možné ohrožení distribuce elektrické energie
	čerpací stanice ve stanicích a mezistaničních úsecích	možné ohrožení distribuce elektrické energie
	výtahy ve stanicích	výpadek zařízení; ztížení pohybu cestujících; možné ohrožení distribuce elektrické energie
	dílny a sklady údržby ve stanicích	možné ohrožení distribuce elektrické energie
Vzduchotechnická zařízení	hlavní větrání, staniční vzduchotechnika	výpadek zařízení, možnost otravy, udušení lidí
Mobilní stroje a zařízení	vozový park	znehybnění veškerých souprav; možná překážka při evakuaci
	zařízení a prostředky pro čištění odpadu zahrnují mycí a zametací vozíky, kontejnery na odpad a soustavu žebříků a lešení pro čištění osvětlovací techniky	narušení pracovních činností
	prostředky požární ochrany umístěné ve stanicích, které umožňují rychlý zásah při požáru v podzemních prostorách	ztížení přístupu k prostředkům; pomalejší reakce při zásahu
Ostatní důležitá zařízení	bezpečnostní a poplachová tlačítka	výpadek zařízení, pomalejší reakce při odezvě; možné ohrožení distribuce elektrické energie
	zařízení pro vyhlášení požárního poplachu	výpadek zařízení pomalejší reakce při odezvě
	trakční zařízení a osvětlení	výpadek zařízení eskalace paniky, ztížení prací personálu a záchranných složek
	traťová zařízení, hlavní uzávěr vody	výpadek zařízení; zatopení, nedostatek vody
	pohyblivé schody, plošiny, signální panel strojního zařízení	výpadek zařízení; ztížení řízení odezvy; možné ohrožení distribuce elektrické energie
	uzavírací zařízení (el. Rolety)	výpadek zařízení; znemožnění přístupu; vnik neoprávněných osob do neveřejných částí; možné ohrožení distribuce elektrické energie
Staniční jednotky řídicího systému ASDŘ	staniční uzel ASDŘ-D	výpadek zařízení; znemožnění vzdáleného řízení dopravy, rozhlasů a kamer

		staniční jednotka automatického stavění jízdních cest	výpadek zařízení; nutnost nouzového stavění cest
		staniční uzly s návazností na energetický a technologický dispečink	výpadek zařízení; znemožnění centrálního dohledu a řízení technologií; možné ohrožení distribuce elektrické energie
		staniční uzly systému centrálního ovládání osvětlení	výpadek zařízení; znemožnění centrálního ovládání osvětlení
		staniční uzly s návazností na dispečink sdělovací, zabezpečovací a dispečink hasičů	výpadek zařízení; znemožnění vzdáleného dohledu a řízení odezvy
	Zabezpečovací zařízení	staniční zabezpečovací zařízení (ESA 11 M)	výpadek zařízení; znemožnění jízdy vlaku
		traťová zabezpečovací zařízení (AŽD 71, ESA 11 M)	výpadek zařízení; znemožnění jízdy vlaku
		vlaková zabezpečovací zařízení (MATRA a vozové jednotky).	výpadek zařízení; znemožnění jízdy vlaku
	Toky energetické		výpadek všech systémů bez záloh
	Toky informační	centrální dispečink – staniční uzly ASDŘ	výpadek komunikace; znemožnění vzdáleného řízení dopravy, rozhlasů a kamer
		centrální dispečink – staniční sdělovací zařízení	při výpadku síťových prvků znemožnění centrálního dohledu a řízení technologií
		staniční uzly ASDŘ – zabezpečovací zařízení	znemožnění řízení dopravy
		staniční uzly ASDŘ – sdělovací zařízení	znemožnění řízení odezvy
		zabezpečovací zařízení – technologie (traťové, vlak)	znemožnění řízení dopravy
		telefonní spojení mezi centrálním dispečinkem, stanicí a vlakem	výpadek spojení; znemožnění přímé komunikace s okolím, panika

Z tabulek 8 a 9 jsou patrné dopady vybrané pohromy na chráněná aktiva. Na základě diskuze s experty, tj. ústního sdělení [38],[39] a expertního posouzení na základě zkušeností v souladu se standardními metodami zpracování dat uvedenými v odstavci 3.1, lze pohromu ohodnotit a následně kategorizovat.

Ohodnocení pohromy s použitím stupnic uvedených v odstavcích 3.2.3 a 3.2.4 (odhad):

- intenzita výskytu – malá (v rozmezí 10^{-4} / rok až 10^{-5} / rok),
- dopady pohromy – velké (velké dopady na veřejná aktiva území, ve kterém se objekt nachází, velké ztráty na majetku lidí i provozovatele dráhy, možná úmrtí a zranění velkého počtu lidí - nad 10).

Předmětná pohroma dle metodiky uvedené v odstavci 1.2.1 spadá do kategorie 3 D, tj. ***pohroma specifická.***

Řízení bezpečnosti zahrnuje prevenci dle bezpečnostního plánu níže, odezvu v případě vzniku pohromy dle nouzových plánů.

4.3.2 Teroristický útok (na tok informací)

Teroristický útok představuje velké nebezpečí v mnoha oblastech, protože se s ním při výstavbě metra nepočítalo a navíc se špatně předvídá. Útočník může provést bombový či chemický útok, ozbrojený útok ve stanici nebo může ovlivnit jakákoliv zařízení (na zdroje energie, vyřazení zabezpečovacích zařízení, úmyslný kybernetický útok vedoucí k poruše řízení či přímé nehodě vlaků a podobně). Diplomová práce předkládá analýzu teroristického útoku na informační tok, který může bez zpětné znalosti uživatele vyřadit předmětné technologie nebo zapříčinit provedení nepříznivé funkce.

Analyzovaný útok na tok informací může napomoct k další sérii promyšlených přímých útoků na chráněná aktiva, například může ovlivnit pohyb lidí a vlaků na útočníkem určená místa a podobně.

Četnost výskytu předmětné pohromy se stanoví velmi těžko, avšak ve světě k podobným útokům dochází často [40], záleží na motivu útočníků, na společenské stability území a mnoha jiných aspektech. Podrobná analýza motivu útoků a možných pravděpodobností není předmětem této práce. Velikost dopadů je odvozen z tabulek WHAT, IF níže a metodami uvedenými v kapitole 3.

Tabulka 10: Analýza WHAT, IF pro útok na tok informací a vliv na veřejná aktiva.

If (Když?)	Možné dopady:		What (co se stane?)
Teroristický útok na tok informací	Možné dopady na životy a zdraví lidí.		ušlapání, vážné či smrtelné úrazy většího počtu lidí z důvodu paniky,
	Možné dopady na bezpečí lidí.		vznik paniky většího rozsahu
	Možné dopady na majetek.		možné poškození celého systému stanice
	Možné dopady na veřejné blaho.		panika, vliv na společnost, omezení dopravní obslužnosti hl. m. Prahy
	Možné dopady na životní prostředí.		znečištění, kontaminace neznámou látkou
	Možné dopady na infrastruktury a technologie	možné dopady na dodávky energií (elektřina, teplo, plyn),	výpadek elektřiny, výpadek zdroje světla, vzduchotechniky
		možné dopady na systém dodávky vody,	odstavení přívodu vody
		možné dopady na kanalizační systém,	odstavení čerpadel
		možné dopady na přepravní síť,	kolaps dopravy v oblasti pohromy, tj. hl. m. Prahy, dopravní kongesce na území hl. m. Prahy.
		možné dopady kybernetickou infrastrukturu (komunikační a informační sítě)	možnost odstavení či ovlivnění celé technologické sítě Dopravního podniku hl. města Prahy.
		možné dopady na bankovní a finanční sektor,	velké finanční ztráty hl. města Prahy
		možné dopady na nouzové služby (policie, hasiči, zdravotníci),	čerpání rezervních finančních i lidských zdrojů
		možné dopady na základní služby v území (zásobování potravinami,	vliv na zásobování okolí

		likvidace odpadů, sociální služby, pohřební služby), průmysl a zemědělství,	
		možné dopady na státní správu a samosprávu.	čerpání rezervních finančních i lidských zdrojů

Tabulka 11: Analýza WHAT/IF pro útok na tok informací a vliv na aktiva stanice.

If (Když?)	Možné dopady na aktiva stanice:		What (co se stane?)
Teroristický útok na tok informací	Životy a zdraví lidí:		-
	životy a zdraví cestujících		možné úmrtí více lidí, možné zranění více lidí, možné trvalé následky
	životy a zdraví zaměstnanců		možné úmrtí více lidí, možné zranění více lidí, možné trvalé následky
	pracovní prostředí		neznámé
	Majetek:		
	Místa	veřejné prostory (severní vestibul, nástupiště, soupravy metra)	při ovládnutí řídicích počítačů vlaku; ***možné úmrtí velkého počtu lidí***
		shromažďovací místo	-
		technologické místnosti (stavědlo, reléová místnost)	převzetí kontroly nad řízením; nepřímý vliv na bezpečnost
		stanoviště dozorčího	chybné zobrazování informací; nepřímí vliv na bezpečnost; špatné rozhodnutí
	Energetická zařízení	Měnírny a distribuční transformovny	možné ohrožení distribuce elektrické energie; ohrožení zdraví lidí
	Sdělovací zařízení	sdělovací kabely, VKV spojení s vlaky, automatické odbavování cestujících	výpadek systému nebo chybné provedení funkcí; možná zranění a úmrtí několika lidí
		zařízení průmyslové televise, telefonní zřízení, rozhlasové zařízení;	chybné zobrazování informací; špatné rozhodnutí; možné úmrtí velkého počtu lidí (při chybném nouzovém hlášení)
		hodinové zařízení, elektrická požární signalizace;	chybné zobrazování informací; špatné rozhodnutí; možné úmrtí velkého počtu lidí (při chybném nouzovém hlášení)
		elektrická zabezpečovací signalizace	nepřímý vliv na bezpečnost
	Strojní zařízení	pohyblivé schody ve stanicích	ohrožení zdraví lidí
		čerpací stanice ve stanicích a mezistaničních úsecích	ohrožení zdraví lidí
		výtahy ve stanicích	ohrožení zdraví lidí
		dílny a sklady údržby ve stanicích	ohrožení zdraví lidí
	Vzduchotechnická zařízení	hlavní větrání, staniční vzduchotechnika	vyřazení nebo provedení chybné funkce - ***možnost otravy, udušení lidí***
	Mobilní stroje a zařízení	vozový park	vyřazení nebo částečné převzetí kontroly nad řízením; ***možné úmrtí velkého počtu lidí***
		zařízení a prostředky pro čištění odpadu zahrnují mycí a zametací vozíky, kontejnery na odpad a soustavu žebříků a lešení pro čištění osvětlovací techniky	nepřímý vliv na bezpečnost
		prostředky požární ochrany umístěné ve stanicích, které umožňují rychlý zásah při požáru v podzemních prostorách	nepřímý vliv na bezpečnost
	Ostatní důležitá zařízení	bezpečnostní a poplachová tlačítka	nepřímý vliv na bezpečnost
		zařízení pro vyhlášení požárního poplachu	ohrožení zdraví a životy lidí

		trakční zařízení a osvětlení	dočasné vyřazení osvětlení; eskalace paniky, ztížení prací personálu a záchranných složek
		traťová zařízení, hlavní uzávěr vody	nepřímý vliv na bezpečnost
		pohyblivé schody, plošiny, signální panel strojního zařízení	ohrožení zdraví lidí
		uzavírací zařízení (el. Rolety)	ohrožení zdraví lidí
	Staniční jednotky řídicího systému ASDŘ	staniční uzel ASDŘ-D	vyřazení nebo převzetí řízení dopravy a některých technologií;
		staniční jednotka automatického stavění jízdních cest	Možnost vyřazení nebo „bezpečné“ přestavení jízdních cest; ***ovládnutí jízdy vlaků***.
		staniční uzly s návazností na energetický a technologický dispečink	znemožnění dálkového ovládání
		staniční uzly systému centrálního ovládání osvětlení	dočasné vyřazení osvětlení; eskalace paniky, ztížení prací personálu a záchranných složek
		staniční uzly s návazností na dispečink sdělovací, zabezpečovací a dispečink hasičů	znemožnění vzdáleného dohledu a řízení odezvy
	Zabezpečovací zařízení	staniční zabezpečovací zařízení (ESA 11 M)	Postavení protisměrných jízdních cest; ***úmrtí velkého počtu lidí***
		traťová zabezpečovací zařízení (AŽD 71, ESA 11 M)	povolení vjezdu do obsazených traťových úseků; ***úmrtí velkého počtu lidí***
		vlaková zabezpečovací zařízení (MATRA a vozové jednotky).	vyřazení rychlostních omezení, nastavení vyšší povolené rychlosti nebo úmyslné zastavení vlaku; ***úmrtí velkého počtu lidí***
	Toky energetické		Vyřazení nebo ovládnutí; eskalace paniky, ztížení prací personálu a záchranných složek
	Toky informační	centrální dispečink – staniční uzly ASDŘ	vyřazení nebo ovládnutí; úmrtí velkého počtu lidí
		centrální dispečink – staniční sdělovací zařízení	vyřazení nebo ovládnutí; úmrtí velkého počtu lidí
		staniční uzly ASDŘ – zabezpečovací zařízení	vyřazení nebo ovládnutí; úmrtí velkého počtu lidí
		staniční uzly ASDŘ – sdělovací zařízení	vyřazení nebo ovládnutí; úmrtí velkého počtu lidí
		zabezpečovací zařízení – technologie (traťové, vlak)	vyřazení nebo ovládnutí; úmrtí velkého počtu lidí
		telefonní spojení mezi centrálním dispečinkem, stanicí a vlakem	vyřazení nebo ovládnutí; úmrtí velkého počtu lidí

Z tabulek 10 a 11 jsou patrné dopady vybrané pohromy na chráněná aktiva. Na základě diskuze s experty, tj. ústního sdělení [38],[39] a expertního posouzení na základě zkušeností v souladu se standardními metodami zpracování dat uvedenými v odstavci 3.1, lze pohromu ohodnotit a následně kategorizovat.

Ohodnocení pohromy s použitím stupnic uvedených v odstavcích 3.2.3 a 3.2.4 (odhad):

- intenzita výskytu – vysoká (v rozmezí 10^{-2} / rok až 10^{-3} / rok),
- dopady pohromy – velké (velké dopady na veřejná aktiva území, ve kterém se objekt nachází, velké ztráty na majetku lidí i provozovatele dráhy, možná úmrtí a zranění velkého počtu lidí - nad 10).

Předmětná pohroma dle metodiky uvedené v odstavci 1.2.1 spadá do kategorie 3 A, tj. ***pohroma kritická.***

Řízení bezpečnosti zahrnuje:

- prevenci dle bezpečnostního plánu níže,
- odezvu v případě vzniku pohromy dle nouzových plánů,
- obnova v případě vzniku pohromy s využitím nadstandardních zdrojů.

4.4 Bezpečnostní plán pro případ velkého výpadku elektřiny

V souladu se současným poznáním bereme stanici metra jako technologický objekt, pro který zpracováváme bezpečnostní plány s cílem chránit veřejná aktiva stanice před výskytem a dopady sledované pohromy. Výpadek elektřiny je klasifikován jako specifická pohroma, a proto je nutné provádět patřičná preventivní opatření, vypracovat plány odezvy a obnovy se standardními zdroji. Následující odstavce obsahují bezpečnostní plán pro pohromu velký výpadek elektrické energie. Předmětný bezpečnostní plán obsahuje konkrétní návrhy k zajištění bezpečnosti resp. snížení dopadů výše uvedenými metodami (plány prevence, ochranné opatření, scénáře odezvy, evakuační plány, varovací systém, cvičení a výcvik, plány odezvy, plány obnovy).

4.4.1 Prevence

V rámci prevence jsou zavedena technická, organizační, právní a výchovná preventivní opatření, jak je popsáno ve zdroji [5]. Technická preventivní opatření jsou prováděna v souladu se stavebním zákonem 0, zákonem o drahách [41] a dalšími zvláštními právními předpisy [42],[43] a zajišťují bezpečnost stavby a zařízení. Organizační, právní a výchovná opatření [3] zvyšují bezpečnost z hlediska správnosti procesů, kvality služeb, připravenosti zaměstnanců, průmyslu i obyvatel.

Technická opatření:

- územním plánováním je zajištěné vhodné umístění entity, tak aby neohrozila okolí a měla zajištěné vazby na okolní infrastrukturu,
- stavba poblíž rozvoden poskytovatele energií a energetické propojení jednotlivých stanic metra umožňuje distribuci elektrické energie z více nezávislých zdrojů,
- zavedené stavební úpravy, aby i po výpadku elektrické energie byl zajištěn dostatek vzduchu v tunelech, odvod spodní vody a splašků, dostatečný přísun vzduchu, světla (možné využití světlovodů apod.) a jiných stavebních prvků k zajištění bezpečnosti,

- provozování zařízení a objektů dle profesionálně vypracovaných provozních řádů pro udržení dlouhé životnosti a správné funkci kritických zařízení a objektů,
- více stupňů řízení technologií, především energetických zařízení pro normální nouzové a krizové řízení.

Organizační opatření:

zavedení řízení kvality a vnitřních předpisů pro řízení bezpečnosti; profesionálně proškolený technologický a energetický dispečink ne jen v otázkách bezpečnosti.

Právní opatření:

respektování státní, územní a drážní legislativy.

Výchovná opatření:

školení a přezkoušení ostatních zaměstnanců a dodavatelů, veřejně dostupné informace pro cestující a informování obyvatel v okolí sledované entity o možných dopadech pohromy a možných způsobů ochrany pro jejich zmírnění.

4.4.2 Ochrana - zmírnění

Pro zmírnění rizika dopadů sledované pohromy se zavádí technologické ochrany. Při výpadku elektrické energie uvedené technologické ochrany představují například dieselové elektrocentrály, staniční bateriové zálohy či prověřené a udržované UPS na jednotlivých kritických zařízeních (technologických, řídicích i bezpečnostních). Předmětná ochranná zařízení podléhají pravidelným kontrolám a obsluhující personál je řádně a opakovaně proškolován na jejich ovládání a údržbu.

Předmětné ochrany zajišťují bezpečí chráněných aktiv, a jsou schopné aktivovat příslušné nouzové režimy. V přídě ochrany lidí se jedná o zajištění nouzového osvětlení a označení nouzových východů či zajištění nouzových hlášení. V případě technologií se jedná o dostatek náhradní elektrické energie pro uvedení zařízení do nouzových režimů, pro jejich bezpečné odpojování, respektive pro zachování jejich zabezpečovacích funkcí.

Pro zmírnění dopadů pohromy se dále vytváří zásoby a to materiální, finanční i lidské, včetně zajištění paliva pro vytvoření náhradní elektrické energie.

4.4.3 Scénáře odezvy - nouzové plány

Plán odezvy pro pohromu výpadku elektrické energie osahuje činnosti pro zmírnění dopadů pohromy, tj. v první řadě chránit aktiva stanice a okolí. Činnosti jsou dle priority rozdělené

následovně:

1. Vyvedení lidí, tj. realizace plánů evakuace, varovacího systému, zajištění shromažďovacích míst, zajištění zdrojů a ochrana zařízení potřebných k realizaci odezvy.
2. Monitoring a zajištění informačních toků, aktivace vnějších nouzových plánů, pokud je potřeba.
3. Zajištění zboží, materiálu a náhradních zdrojů elektrické energie.
4. Realizace plánu kontinuity jako akce pro ochranu majetku.

Činnosti jsou prováděné dle konkrétních plánů s jasně definovanými kroky a odpovědnosti rezortů a řešitelů.

Nedílnou součástí plánu odezvy je plán kontinuity zabývající se vztahy mezi systémy v rámci entity a jejich kritičností. Plán kontinuity vychází z procesní analýzy se vzájemnými vztahy mezi funkcemi objektu KI (vybrané entity) a službami systému systémů, jak je uvedeno v následujícím seznamu [5]:

- v první fázi je uvedena metodika procesní analýzy,
- dále je analyzována kritičnost vybrané entity, kritičnost její hlavní funkce a funkcí subsystémů na základě analýzy nebezpečných poruch a selhání, vlivů vnějších pohrom, analýze ztrát a škod na základě neprovedení dané funkce a podobně,
- v analýze jsou zahrnuty vazy mezi vrstvami řízení bezpečnosti, vztahy mezi funkcemi systému systémů (vybrané entity) a výkonosti provozu; funkce jsou analyzovány zvlášť podle provozních režimů, tj. běžný provoz metra nebo ochranný systém metra, podle stavu ve kterém se systém nachází, tj. normální, abnormální, kritický; zvlášť jsou posuzovány bezpečnostní úkoly k zabránění zřetězení pohrom,
- analýza služeb systému v čase, tj. funkce systému v bezprostřední odezvě na pohromu do dvou hodin od výskytu pohromy, od dvou do šesti hodin výskytu pohromy, od šesti do dvanácti hodin a odezvu systému na vyžádání.

Plánu kontinuity obsahuje:

1. Soupis hlavních funkcí a režimů dané entity při odezvě na pohromu.
2. Definování, kdy se jedná o stav normální, abnormální a kritický.
3. Definování jednotlivých zařízení, které provádí analyzované kritické funkce.
4. Stanovení popisu přepínání stavů systémů do dalších režimů a postupné odpojování nepotřebných zařízení pro úsporu energie.
5. Stanovení rolí a zodpovědností při realizaci odezvy na pohromu a jednotlivé dílčí kroky.

4.4.4 Evakuační plány

Paralelně s plánem odezvy se při daných režimech a stavech systému definují postupy pro evakuaci lidí a to cestujících i zaměstnanců, kteří se nepodílí na činnostech odezvy. Evakuační plán obsahuje vypsané odpovědnosti pro evakuaci, popis shromažďovacích míst, postupy kdy, kde a za jakých podmínek bude evakuace probíhat, a popis postupů při kontrole prostoru po evakuaci.

4.4.5 Varovací systém

Komunikace mezi jednotlivými zaměstnanci, cestujícími a členy záchranných složek probíhá pomocí dostupných sdělovacích zařízení. Jedním z těchto zařízení je veřejný rozhlas a nouzové požární hlášení, které je možné ovládat ze vzdáleného pracoviště centrálního dispečinku pomocí řídicího systému ASDŘ-D nebo přímo ze staničních rozhlasových zařízení.

Pro případ odezvy na pohromu jsou definované základní a výstižné věty, určené pro informování, varování nebo podávání nouzových pokynů cestujícím. Tyto hlášení obsahují jednoznačné povely, aby nedošlo k nepochopení a aby se podle nich lidé efektivně řídili. Při odezvě je důležité volit takové povely, aby nedošlo ke zbytečné panice a vzniku jiných sekundárních pohrom. Pro realizaci nouzových hlášení je nutné rozdělit jasnou pravomoc a odpovědnosti pracovníků, kdo v jakou chvíli hlášení vybírá, spouští a v jakých chvílích je hlášení spouštěno automaticky. Při vzdáleném ovládání pomocí systému ASDŘ je zajištěna zpětná kontrola (odposlech) hlášených zpráv, aby nedošlo k hlášení nevyžádané zprávy, což může zapříčinit jiná sekundární rizika.

Správné provedení varování je závislé na dostupnosti varovných systémů a informovanosti personálu. Uvedené aspekty jsou zahrnuté ve funkční analýze plánu kontinuity pro zajištění dostupnosti, spolehlivosti a bezpečnosti varovacích systémů.

4.4.6 Cvičení a výcvik

Bezpečnostní plán zavádí pravidelná cvičení, jež umožňují odkrýt nové hrozby, případně rizika spojená s danou pohromou a zároveň ověřují správnost definovaných kroků odezvy. Na základě výsledků cvičení a zjištěných nedostatků se předmětné plány odezvy upravují, zavádí se nová opatření a doplňují se preventivní opatření ve formě výcviku a přeškolování personálu.

4.4.7 Konkrétní plány a postupy při odezvě

Vedle plánu kontinuity, evakuace a hlášení jsou vypracovány další konkrétní postupy při odezvě. Konkrétní postupy jsou popsány ve formě procesu pro každou dotčenou roli, uvedenou v matici odpovědnosti. Uvedený proces obsahuje popis úkolů, které jsou v případě pohromy provedeny resp. průběžně prováděny. Předmětné plány jsou jednoduché, výstižné, věcné a mají formu krizového plánu dle zdroje [5].

4.5 Bezpečnostní plán pro případ velkého teroristického útoku (útok na tok dat)

V souladu se současným poznáním bereme stanici metra jako technologický objekt, pro který zpracováváme bezpečnostní plány s cílem chránit veřejná aktiva stanice před výskytem a dopady relevantních pohrom. Teroristický útok na tok dat je klasifikován jako kritická pohroma, je tedy nutné provádět patřičná preventivní opatření, vypracovat plány odezvy a obnovy s nadstandardními zdroji. Následující odstavce obsahují konkrétní návrhy k zajištění bezpečnosti resp. snížení dopadů výše uvedenými metodami (plány prevence, ochranné opatření, scénáře odezvy, evakuační plány, varovací systém, cvičení a výcvik, plány odezvy, plány obnovy).

4.5.1 Prevence

Podobně jako u jiných pohrom jsou pro případy velkého teroristického útoku prováděna preventivní opatření dle [5] a to v první řadě technická, dále pak organizační, právní a výchovná.

Technická opatření

U informačních technologií jsou technická opatření prováděna samotnou architekturou sítě, kde je jasně definovaná kritičnosti jednotlivých zařízení. Dle kritičnosti se technologické sítě dělí do různých skupin (úrovní) s předem definovanými vlastnostmi dle standardu ISA99 [24].

Norma EN 50159 [22] rozlišuje 3 kategorie přenosových prostředí dle možného přístupu cizích uživatelů. Kategorie 1 je zcela uzavřený přenosový systém, kde mají přístup pouze předem známí a důvěrní uživatelé, riziko narušení tohoto prostředí se zanedbává. Uvedeného prostředí lze dosáhnout úplným fyzickým oddělením systému od jiné technologické sítě. Kategorie 2 předpokládá větší množství uživatelů (vedle lidských uživatelů to mohou být i jiné okolní systémy), kteří nejsou dopředu známí, ale jedná se o důvěrné, autorizované uživatele. Riziko spojené s narušením sítě útočníkem se v předmětné kategorii uvažuje jako relevantní. Kategorie 3 je zcela otevřené prostředí i neautorizovaným uživatelům. Výše uvedené rozdělení

je určené primárně pro komunikaci mezi více bezpečnostně relevantními systémy, ale předmětná norma definuje možné hrozby příslušící danému prostředí a navrhuje možná opatření. Proto se 3 kategorie dle EN 50159 [22] používá pro jakékoliv jiné systémy.

V rámci technických opatření se systémy různých kritičností umisťují do příslušných kategorií přenosového prostředí. Provádí se opatření pro oddělení jednotlivých kategorií, například uzavřené technologické místnosti, nebo že na otevřenou komunikační síť budou připojena pouze informační zařízení, která nemají při své poruše kritické dopady. Dále se omezuje počet otevřených přístupových bodů a jiných síťových prvků, používají se optické kabely při přechodu mezi kategoriemi přenosových prostředí. Různě kritické systémy se dále dle jejich stupně kritičnosti oddělují i z hlediska kybernetické bezpečnosti pomocí ochranných prvků.

Organizační opatření

Společně s technickým řešením datových sítí je spojena správa uživatelů a oprávnění přístupů do místností a virtuálních přístupů do technologických sítí. Uvedená otázka spadá do organizačních opatření, která jasně určují kompetence, odpovědnosti a důvěrnosti osob pracujících v oblasti zabezpečení nebo vývoje zařízení, která mají být z hlediska přenosu dat zabezpečená. Pro zmíněné účely se vychází z návrhu normy ISA 99 [24], která definuje vzájemný vztah mezi lidmi, procesy a technologiemi. Každá z uvedených složek má definované požadavky pro zajištění maximálního zabezpečení řídicích systémů, včetně definice požadavků na jejich zabezpečený vývoj, tj. aby procesy vývoje předmětného systému neohrozili jeho zabezpečení (například požadavky na výměnu informací mezi zaměstnanci, jejich kontrolu, omezení možnosti vzniku úmyslných bezpečnostních mezer tzv. backdoors a jiné).

Systém nebo systém systémů, navržený a provozovaný uvedeným přístupem řízení, s definovanými bezpečnostními procesy (v provozních předpisech), se zabezpečenými přístupy proti vniknutí neautorizovaných subjektů (správa přístupových klíčů, definované způsoby autentizace), se zabezpečenou technologií a vývoje, může výrazným způsobem redukovat riziko útoku na tok dat. Riziko je sníženo především tím, že by potencionální útočník musel ke svému činu vynaložit neúměrně vysoké úsilí.

Právní opatření:

V rámci prevence je respektován zákon o kybernetické bezpečnosti [36] [45], který provozovateli sítě nebo informačních systémů KI stanovuje následující povinnosti:

- nahlášení kontaktních údajů,
- detekovat kybernetické bezpečnostní události,
- hlásit kybernetické bezpečnostní incidenty,

- zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření,
- provádět opatření vydaná Národním bezpečnostním úřadem.

Výchovná opatření

V rámci organizace se zavádí školení kybernetické bezpečnosti, pro zajištění správných návyků, jelikož nejvíce bezpečnostních slabin v kybernetice pochází především ze špatně proškoleného personálu. Pro zajištění školení nebo jiných služeb týkající se prevence lze využít služeb Národního bezpečnostního úřadu nebo příslušných bezpečnostních organizací (CSIRT) [46].

Mezi výchovná opatření patří také školení a přezkoušení dodavatelů, patří zde i veřejně dostupné informace pro cestující a informování obyvatel v okolí sledované entity o možných dopadech pohromy a možných způsobů ochrany pro jejich zmírnění.

4.5.2 Ochrana - zmírnění

Definovaná architektura technologické sítě je chráněna různými zařízeními pro oddělování sítí, firewally, jednotkami pro vytvoření bezpečného a zabezpečeného kanálu v rámci komunikace bod - bod mezi dvěma autorizovanými účastníky komunikace, antiviry, systémy pro sledování podezřelých aktivit na síti (IDS) a podobně. Předmětné systémy plní důležité zabezpečovací funkce, které jsou jasně definovány a ověřovány v různých stupních dle jejich kritičnosti.

Pro výše uvedené účely se používá evropská norma EN 15408 [23] v praxi známá jako CC (Common Criteria). Předmětem této normy je definice hodnoceného systému (TOE – Target Of Evaluation), množiny jeho bezpečnostních funkcí tzv. profil ochrany (PP - Protection Profile), stupeň jejich hodnocení (EAL – Evaluation Assurance Level) a prokázání splnění definovaných cílů (ST – Security Target), tj. množina jednoho nebo více profilů ochrany (PPs). Správce informační struktury volí množinu bezpečnostních opatření (PP) a podle kritičnosti zařízení volí stupeň jejich hodnocení (EAL od 0 do 7). Podle EAL se provádí hodnocení různými metodami zahrnující prověření dokumentace vývoje, testování až po formální (matematické) modely a formální prokázání bezpečnosti. Čím vyšší stupeň EAL, tím jsou kladeny vyšší nároky na prokázání splnění bezpečnostních cílů (ST).

Pro drážní systémy a tedy i v předmětné stanici metra se přenáší informace a povely mezi různými kritickými zařízeními. Uvedená zařízení se většinou nachází v uzavřeném komunikačním prostředí, ale samotná komunikace často probíhá na dlouhé vzdálenosti skrze otevřené prostředí (rádio, WiFi, různé technologické sítě). Zmíněným způsobem se uzavřená přenosová prostředí otevírají. Potenciální útočník má v tomto případě možnost tzv. penetrovat (proniknout) do uzavřeného prostředí a může tak ovlivnit vnitřní datový

tok, popřípadě může mezi kritickými zařízeními zachycovat a měnit jimi přenášená data.

Z výše uvedeného důvodu se instalují speciální zařízení, která zabezpečují uzavřená komunikační prostředí. Vytváří bránu mezi uzavřeným a otevřeným prostředím a navíc chrání přenášená data proti úmyslné manipulaci.

Hlavním úkolem kritických systémů je plnit bezpečnostně relevantní funkce, jsou na ně kladeny vysoké požadavky na bezpečnost (tj. neohrozí sebe ani okolí). Funkce zabezpečení mohou předmětné systémy pozitivně, ale i negativně ovlivňovat. Vyšší požadavek na zabezpečení přenosu dat může například zpomalit přenos informací a v kritických situacích to může vést až k fatálním selháním. Proto procesy bezpečnosti a zabezpečení probíhají současně v celém životním cyklu systému. V předem stanovených milnících života systému, včetně jeho vývoje a provozu, se provádí sloučení posuzování výsledků jednotlivých analýz bezpečnosti a zabezpečení, jak bylo definováno v evropském projektu SESAMO [44].

Předmětná drážní zařízení dále splňují požadavky všech drážních norem především EN 50126 [12], EN 50159 [22], požadavky na vývoj dle ISA 99 [24], a zabezpečovací techniky jsou volené a hodnocené dle normy EN 15408 [23]. Pro správnou aplikaci těchto požadavků se využívá znalostí evropského projektu SESAMO (Safety and Secuirity Modelling), kde byl definován proces pro vývoj bezpečného a zabezpečeného systému [44].

4.5.3 Scénáře odezvy - nouzové plány

Scénáře odezvy zavádí postupy pro nalezení útočníka a pro ochranu veřejných aktiv, tj.:

1. Zahájení monitoringu a analýzy místa průniku do sítě. Útok na datové toky může představovat jeden z kroků sofistikovanějšího útoku, proto je nutné dohledat útočníka v co nejkratší době. K vyhledání útočníka mohou posloužit již zmíněné monitorovací systémy IDS a podobně.
2. Hledání vhodných cest a příprava lidských zdrojů pro aktivaci plánu evakuace za pomocí ozbrojených sil bez využití elektronických systémů.
3. Provedení evakuace.
4. Provedení plánu kontinuity, bezpečné odpojování kritických systémů.
5. Zajištění zdrojů pro poskytování bezpečných informací a pro koordinaci činností. Činnost zahrnuje navázání spolupráce s vládním, respektive národním, CERT orgánem definovaným Zákonem o kybernetické bezpečnosti [45], tj. především nahlášení kybernetického incident a jeho dokumentace. V rámci odezvy je možné požádat spolupráci CSIRT týmu [46].

Obdobně jako u jiných pohrom je pro případ útoku na datové toky vypracován plán kontinuity. Plán kontinuity obsahuje podobné kroky, jak bylo zmíněno výše u výpadku elektrické energie s tím rozdílem, že je zaměřen na odpojování síťových zařízení a omezuje funkčnost některých řídicích systémů.

V případě jízdy vlaků jsou stanoveny vhodné režimy provozu (jízda v plné moci strojvedoucího nebo příkaz pro zastavení vlaku v bezpečném místě aj.).

4.5.4 Evakuační plány

Paralelně s nouzovým plánem a plánem kontinuity se při daných režimech a stavech systému jsou definované postupy pro evakuaci lidí a to cestujících i zaměstnanců, který se nepodílí na činnostech odezvy. Evakuační plán obsahuje vypsané odpovědnosti pro evakuaci, popis shromažďovacích míst, postupy kdy, kde a za jakých podmínek bude evakuace probíhat, a popis postupů při kontrole prostoru po evakuaci.

Při teroristickém útoku na datový tok lze předpokládat, že se jedná o sofistikovaný proces s cílem zmást oběť a navíc může představovat pouze počátek dalších násilných kroků. Proto se pro evakuaci v tomto případě používají ozbrojené síly pro zajištění maximálního bezpečí lidí a omezuje se využití elektronických systémů pro podporu zvládnutí odezvy.

4.5.5 Varovací systém

Varovací systémy realizují stejné funkce, jak bylo popsáno výše u výpadku elektrické energie. Při útoku na datový tok je nutné počítat s možností úmyslného znehodnocení varovacích resp. sdělovacích zařízení. Tímto se zvyšuje požadavek na zpětné ověřování hlášených zpráv, pokud je nutné tyto systémy využít. V některých případech je nutné rozhodnou o provádění hlášení přímo odpovědným pracovníkem bez použití elektronických rozhlasových zařízení.

4.5.6 Cvičení a výcvik

Bezpečnostní plán zavádí pravidelná cvičení, jež umožňují odkrýt nové hrozby, případně rizika spojená s danou pohromou a zároveň ověřují správnost definovaných kroků odezvy. Na základě výsledků cvičení a zjištěných nedostatků se předmětné plány odezvy upravují, zavádí se nová opatření a doplňují se preventivní opatření ve formě výcviku a přeškolování.

V oblasti kybernetické infrastruktury se zavádí speciální oddělení s odpovědným a kompetentním personálem, pravidelně školeným a přezkoušeným v oblasti kybernetické bezpečnosti (cyber security).

4.5.7 Konkrétní plány a postupy při odezvě

Vedle plánu kontinuity, evakuace a hlášení jsou vypracovány další konkrétní postupy při odezvě. Konkrétní postupy jsou popsány ve formě procesu pro každou dotčenou roli, uvedenou v matici odpovědnosti. Uvedený proces obsahuje popis úkolů, které jsou v případě pohromy provedeny resp. průběžně prováděny. Předmětné plány jsou jednoduché, výstižné, věcné a mají formu krizového plánu dle zdroje [5].

4.6 Plány obnovy po pohromách většího rozsahu

V případě výskytu pohromy s velkými dopady se prování obnova v předem definovaných krocích. Obnova provozu je nejdříve zavedena pomocí omezeného zkušebního provozu, zavádí se monitoring a teprve poté návrat k původnímu režimu. Obnova po kritické pohromě znamená likvidaci velkého množství škod a je nutné vytvářet rezervu pro čerpání nadstandardních prostředků. Stejně tak je důležité vyčlenit také lidské zdroje pro realizaci odezvy na pohromu a následně obnovy.

5 Srovnání výsledků práce se současným stavem

Základními požadavky na řízení bezpečnosti, tedy i řízení bezpečnosti vybrané stanice, je, aby byla stanice metra:

- z hlediska pohrom zabezpečená,
- bezpečná v případě selhání nebo poruchy, tj. stanice neohrozí sebe ani okolí.

Pro zajištění výše uvedených cílů bezpečnosti je pro technologické objekty, tedy systémy systémů (SoS), nutné zavést strukturované řízení bezpečnosti (SMS) pomocí pětistupňového modelu uvedeného v odstavci 1.3.3.

Obecné bezpečnostní plány založené na současném poznání a integrální bezpečnosti, naznačené v předchozí kapitole, nerespektují strukturovaný systém řízení bezpečnosti. Z výše uvedených důvodů je nezbytné provádět srovnání výsledků bezpečnostních plánů s jednotlivými vrstvami pětistupňového modelu a bezpečnostní plán doplňovat nebo dle pětistupňového modelu strukturovat. Zmíněný proces lze v praxi provádět v několika iteracích vzájemného porovnávání.

Cílem kapitoly je ukázat položky (mechanismy, opatření a metody), jež jsou dle bezpečnostního plánu a dle strukturovaného systému řízení bezpečnosti nutné pro zajištění bezpečnosti objektu i okolí. Navíc práce poukazuje na položky v praxi buď nezavedené, nebo mají z hlediska bezpečnosti nižší úroveň.

Podle metody shody (viz kapitola 3) bylo provedeno srovnání bezpečnostního plánu a pětistupňového modelu se současným stavem, tj. současné legislativy a technických možností.

Hledání shody a vzájemných propojeních mezi bezpečnostními plány, systémy řízení bezpečnosti a opatřeními v jednotlivých vrstvách SMS budou předmětem dalšího výzkumu.

5.1 Současný stav bezpečnosti stanic metra

Z veřejně dostupných zdrojů je zřejmé, že v systému Pražského metra je prevence zajištěna při výstavbě a konstrukcí dle stavebního zákona. Existuje zde připravenost ve smyslu cvičení mimořádných událostí, například při pohromě chemického nebo požární cvičení. Existují zde také ochranné prvky pro snížení rizik různých pohrom v podobě náhradních zdrojů elektrické energie, zabezpečovacích systémů provozu metra nebo elektronických bezpečnostních systémy omezující přístup do neveřejných prostor, prostor kolejiště a podobné. Jsou zde tedy

důkazy o zavedeném řízení bezpečnosti.

I přes výše zmíněné skutečnosti, česká legislativa a ani jiné autority (například drážní úřad), nevyžadují vícestupňové řízení bezpečnosti popsané v kapitole 1. Proto Dopravní podnik hlavního města Prahy a. s. uvedené přístupy pravděpodobně nezavádí, tedy nezohledňuje veškeré relevantní, specifické a kritické pohromy, stejně tak jako nejsou zaváděny u většiny jiných staveb a projektů stejné úrovně bezpečnosti.

Prvního požadavku na bezpečnost, tj. aby byla stanice metra zabezpečená z hlediska pohrom, lze v praxi docílit integrálním řízením bezpečnosti založeným na přístupu All-Hazard-Approach, uvedeným v odstavci 1.3.1 a 1.3.2.

Druhý požadavek, na bezpečnost stanice v případě selhání nebo poruchy (tj. stanice neohrozí sebe ani okolí), může být naplněn současnými zákonnými ustanoveními a drážními standardy, avšak pouze za normálních podmínek. V případě výskytu pohromy, a uvedení zařízení do abnormálních a kritických stavů, nelze bez řádné připravenosti zajistit bezpečí samotné stanice ani okolí. Pro zvýšení potřebné ochrany prvku KI je nutné zavést pětistupňový model uvedený v odstavci 1.3.3.

5.2 Porovnání nároků pětistupňového modelu SMS s platnou legislativou

Cílem odstavce je porovnat nároky na zajištění bezpečnosti pětistupňového modelu s platnou legislativou, tj. českými zákony, vyhláškami a evropskými směrnicemi nebo normami v oblasti drážního prostředí.

V tabulce 12 jsou uvedené nároky systému zajištění bezpečnosti dle pětistupňového modelu popisovaného v předchozích kapitolách a jsou porovnány s reálnými legislativními opatřeními v ČR (resp. v Evropě).

Tabulka 12: Srovnání nároků pětistupňového modelu na zajištění bezpečnosti s reálným stavem.

Vrstva	Nárok	Realita a její nedostatky
1.	V návrhu, výstavbě a konstrukci inherentně používat principy bezpečného projektu (přístupy: - 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, - monitoring, ve kterém jsou zabudovány korekční opatření a činnosti).	Vrstva je v současnosti zajištěna: - stavebním zákonem 0 a drážní legislativou [41], - řízením rizik definované normou EN 50 126 [12] a evropskou směrnicí [17], - kvalitou drážního zařízení dle standardu IRIS [18] založeném na systému řízení kvality ISO 9001 [19], - zákonem o kybernetické bezpečnosti [36]. Slabiny: - absence All-Hazard-Approach, není zavedena povinnost zvážit všechna ohrožení; - zabezpečení je prováděno jen do výše projektové pohromy, tj. stoleté pohromy [13],[51] - proto u řady ohrožení chybí proaktivní přístup; - chybí vazba na vyšší vrstvy řízení bezpečnosti;

		- požadavky na bezpečnost a zabezpečení jsou řešené odděleně (mohou mít negativní dopady, protože nejsou zohledněny vazby a spřažení, ke kterým může dojít při větších odchylkách od normálního stavu).
2.	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.	Vrstva je v současnosti zajištěna: - požadavky na systém řízení dle EN 62290 [32] pro městskou a příměstskou dráhu, - bezpečnostními požadavky pro systémy provozu UGTMS bez obsluhy EN 62267 [33], - rozhraním na nouzové zvukové zařízení a požární signalizaci podléhající normám EN 54 [49] a EN 60849 [50], - životním cyklem systému UGTMS dle EN 50126 (zajištění a prokázání RAMS) [12], - technikami pro informační systém a komunikaci dle zákona č. 181/2014 o kybernetické bezpečnosti [45]. Slabiny: - požadavky na systém řízení jsou definované pouze pro systémy UGTMS, tj. městskou a příměstskou dráhu, - bezpečnostní požadavky pouze na provoz vozidla bez obsluhy, - chybí požadavky na signalizaci, upozornění v případě abnormálních událostí dle All-Hazard-Approach, - požadavky na bezpečnost a zabezpečení řídicího systému jsou řešeny odděleně, tj. mohou se navzájem negativně ovlivňovat (zvláště za podmínek hodně odchýlených od normálního stavu).
3.	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 resilienci. Předmětné systémy udržují bezpečný provoz i za změny podmínek nebo mají schopnost zajistit normální provoz po aplikaci nápravných opatření (vyčištění, oprava…).	Vrstva je v současnosti zajištěna: - identifikací bezpečnostně relevantních funkcí a zařízení dle EN 50 126 [12], - vývojem bezpečnostně relevantních zařízení dle EN 50129 [20] a EN 61511 [10], - vývojem bezpečnostně relevantního SW dle EN 50128 [21], - komunikace mezi bezpečnostními systémy dle EN 50159 [22]. Slabiny: - chybí koncept zabezpečení bezpečnostně relevantních zařízení a to jak z hlediska fyzických i SW opatření, - koncept zajištění komunikace je z hlediska drážních norem nedostatečná, - chybí definice vstupních ovlivňujících činitelů, tj. relevantní události dle All-Hazard-Approach, - požadavky na bezpečnost a zabezpečení řídicího systému jsou řešeny odděleně, tj. mohou se navzájem negativně ovlivňovat (zvláště za podmínek hodně odchýlených od normálního stavu).
4.	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).	Pro některé pohromy je pro metro připraven „Katalog typových činností IZS“. Dopravní podnik hl. m. Prahy zpracovává „Plán krizové připravenosti subjektu KI“ dle krizového zákona [47] a jeho doplnění ve změně [48], Slabiny: - typové činnosti a krizová připravenost respektuje pouze některé pohromy, - nejsou zavedené přístupy All-Hazard-Approach,

		- pohromy a chráněná aktiva nejsou identifikovány metodami respektující integrální riziko, - mimo krizový zákon [47], nejsou zavedené speciální legislativní požadavky, - není plán kontinuity, - není vnitřní havarijní plán na ochranu zaměstnanců a cestujících; - není plán kontinuity.
5.	Systém řízení bezpečnosti pro extrémní podmínky by mělo být stanoveno přímo vyššími orgány zodpovědnými za vrcholové řízení bezpečnosti.	Nejsou speciální legislativní požadavky, tj. neřeší se předem.

Z tabulky 12 je patrné, že se v praxi na drahách používá převážně pouze třístupňový, částečně čtyřstupňový model, navíc jsou v prvních třech až čtyřech vrstvách znatelné mezery, protože největším problémem je skutečnost, že se netestuje odolnost řídicích a řízených systémů a jejich prvků na pohromy větší než jsou projektové [51].

Identifikované nedostatky lze obecně začlenit do následujících bodů [9]:

- není řádně zavedeno vrcholové řízení založené na proaktivním přístupu a na integrálním riziku,
- chybí mezioborová komunikace a vazba mezi jednotlivými vrstvami řízení bezpečnosti,
- požadavky na bezpečnost nejsou řešeny komplexně; nemusí být identifikována všechna rizika,
- neřeší se otázka selhání lidského faktoru,
- ve všech vrstvách řízení bezpečnosti chybí aplikace konceptu All-Hazard-Approach,
- absence konceptu Defence-In-Depth pro kritické položky v potřebné síti,
- přístup k bezpečnosti a zabezpečení je v české i evropské legislativě pojat odděleně a neřeší vzájemné závislosti, které mohou ovlivnit bezpečnost,
- drážní předpisy a normy dosud dostatečně neřeší zabezpečení všech drážních zařízení,
- neuvažují se vazby a toky přes hranice systému a za hranicemi systému.

V důsledku uvedených mezer v zabezpečení, může provoz sledovaného prvku KI ohrozit chráněná aktiva.

5.3 Prvky pro zajištění bezpečnosti chráněných aktiv

Z výše uvedených informací a dalších veřejně dostupných zdrojů [26],[27], [29] lze srovnávací metodou odvodit prvky pro zabezpečení jednotlivých chráněných aktiv předmětné stanice metra. Nalezené metody, techniky a opatření jsou v různých podmínkách provozu buď dostatečné, nebo nedostatečné. Tabulka 13 zachycuje známé ochranné mechanismy a pro vybrané pohromy stanovuje, zda jsou dostatečné či nikoliv. Výsledky srovnání mají pouze informativní charakter, mohou existovat i další ochranné mechanismy zavedené dopravním

podnikem, které zajišťují bezpečnost chráněných aktiv v různých provozních podmínkách. Tabulka 13 zachycuje příslušná opatření pouze pro 3 vrstvy, tj. pro bezpečnou stavbu a zařízení, normální provoz a větší odchylky.

Tabulka 13: Návrh ochranných mechanizmů.

Legenda: ☑ - zajištěné příslušnými opatřeními, ☒ - částečné opatření, ☒ - nepodchycené

		výpadek elektřiny		útok na tok informací	
Lidé	1.	Stavební zákon, ISO 9001.	☑	neřeší se	-
	2.	Dispečerský a dozorčí dohled, systémy nouzového hlášení.	☑	neřeší se	-
	3.	Dieselové a bateriové zálohy	☒	neřeší se	-
Objekty	1.	Stavební zákon, ISO 9001.	☑	Zákon o kybernetické bezpečnosti; fyzické zabezpečení.	☑
	2.	Dispečerský a dozorčí dohled, systémy nouzového hlášení.	☑	Zákon o kybernetické bezpečnosti; systémy IDS	☒
	3.	Dieselové a bateriové zálohy.	☑	neřeší se	☒
Energetická zařízení	1.	Příslušné ČSN a drážní legislativa.	☑	Zákon o kybernetické bezpečnosti; autorizace vstupu do místností; fyzické zabezpečení.	☑
	2.	Dispečerský, staniční dohled.	☑	Zákon o kybernetické bezpečnosti; systémy IDS	☒
	3.	Dieselové a bateriové zálohy.	☑	neřeší se	☒
Sdělovací zařízení	1.	Příslušné ČSN.	☑	Zákon o kybernetické bezpečnosti; autorizace vstupu do místností; fyzické zabezpečení.	☑
	2.	Signalizace dle ČSN.	☑	Zákon o kybernetické bezpečnosti; systémy IDS	☒
	3.	UPS, bateriové zálohy.	☑	neřeší se	☒
Strojní zařízení	1.	Příslušné ČSN.	☑	Zákon o kybernetické bezpečnosti; autorizace vstupu do místností; fyzické zabezpečení.	☑
	2.	*neznámé*	☒	Zákon o kybernetické bezpečnosti; systémy IDS	☒
	3.	Bateriové zálohy.	☒	neřeší se	☒
Vzduchotechnická zařízení	1.	Příslušné ČSN a drážní legislativa.	☑	Zákon o kybernetické bezpečnosti; autorizace vstupu do místností; fyzické zabezpečení.	☑
	2.	Dispečerský, staniční dohled.	☑	Zákon o kybernetické bezpečnosti; systémy IDS	☒
	3.	Dieselové a bateriové zálohy.	☒	neřeší se	☒
Mobilní stroje a zařízení	1.	Příslušné ČSN a drážní legislativa.	☑	Příslušné ČSN - TCN komunikace; EN 50159 fyzické zabezpečení.	☑
	2.	Proškolený strojvedoucí.	☒	neřeší se	☒
	3.	Proškolený strojvedoucí.	☒	neřeší se	☒
Ostatní důležitá zařízení	1.	Příslušné ČSN a drážní legislativa.	☑	Zákon o kybernetické bezpečnosti; autorizace vstupu do místností; fyzické zabezpečení.	☑
	2.	Dispečerský, staniční dohled.	☑	Zákon o kybernetické bezpečnosti; systémy IDS	☒
	3.	Dieselové a bateriové zálohy.	☒	neřeší se	☒
Staniční jednotky	1.	Příslušné ČSN a drážní legislativa.	☑	Zákon o kybernetické bezpečnosti; autorizace vstupu do místností; ČSN EN 50159;	☑

řídicího systému				fyzické zabezpečené (optické kabely, omezené množství AP)	
	2.	Dispečerský, staniční dohled.	☑	Zákon o kybernetické bezpečnosti; systémy IDS.	☑
	3.	Dieselové a bateriové zálohy, redundantní systém.	☑	CSIRT	☒
Zabezpečovací zařízení	1.	Příslušné ČSN a drážní legislativa.	☑	Zákon o kybernetické bezpečnosti; ČSN EN 50159; autorizace vstupu do místností.	☑
	2.	Dispečerský, staniční dohled.	☑	Zákon o kybernetické bezpečnosti; systémy IDS.	☒
	3.	Dieselové a bateriové zálohy, redundantní systém, ČSN EN 50128,9, ČSN EN 50159	☑	neřeší se	☒
Toky	1.	Příslušné ČSN a drážní legislativa.	☑	Zákon o kybernetické bezpečnosti; autorizace vstupu do místností; fyzické zabezpečené (optické kabely, omezené množství AP)	☑
	2.	Dispečerský, staniční dohled.	☑	Zákon o kybernetické bezpečnosti; systémy IDS	☑
	3.	Dieselové a bateriové zálohy, redundantní systém.	☑	CSIRT [46]	☒

V tabulce 13 bylo identifikováno 25 nepokrytých požadavků vrstev, hledání vhodných opatření pro pokrytí zjištěných mezer bude předmětem dalšího výzkumu.

Obdobným způsobem jako v tabulce 13 lze pokračovat pro každou další relevantní pohromu. Předmětem příslušného hodnocení shody mezi normativem založeným na integrální bezpečnosti a reálným stavem je zjistit, které vrstvy jsou nebo nejsou dostatečně pokryty ochrannými mechanizmy. Dostatečnost pokrytí pro veškeré relevantní pohromy vybrané stanice a chráněná aktiva znázorňuje tabulka, kde jsou uvedené pohromy, chráněná aktiva a první tři vrstvy ochrany.

Tabulka 14: Pokrytí vrstev ochrannými mechanizmy.

Legenda: ☑ - podchycené příslušnými opatřeními, ☒ - částečné opatření, ☒ - nepodchycené

	Pokrytí vrstvy	Povodeň	Zemětřesení	Ztekucení podloží	Výstup plynu na zem.	Epidemie	Pandemie	Stabilita lid. Spol.	Kriminalita	Útok	Teroristický útok	Útok CNRB	Ozbrojený konflikt	Válka	Průmyslová havárie	Havárie – neb. látky	Havárie při dopravě	Pohroma v oblasti KI	Pohroma v ekonomice
Lidé	1.	☑	☑	☑	☑	☒	☒	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	-
	2.	☑	☑	☑	☒	☒	☒	☑	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	-
	3.	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	-
Objekty	1.	☑	☑	☑	☑	☒	☒	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	-
	2.	☑	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑	☒	☒	☒	☒	-
	3.	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	-
Energetická zařízení	1.	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	-	☑	☑	-
	2.	☑	☑	☑	-	-	-	☑	☑	☑	☒	☑	☑	☒	☑	-	☑	☑	-
	3.	☒	☑	☑	-	-	-	☒	☑	☑	☒	☒	☑	☒	☑	-	☑	☑	-
Sdělovací zařízení	1.	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	-	☑	☑	-
	2.	☑	☑	☑	-	-	-	☒	☑	☑	☒	☑	☑	☒	☑	-	☑	☑	-
	3.	☒	☑	☑	-	-	-	☒	☑	☑	☒	☒	☑	☒	☑	-	☑	☑	-
Strojní zařízení	1.	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	-	☑	☑	-
	2.	☒	☒	☒	-	-	-	☒	☒	☒	☒	☒	☒	☒	☒	-	☒	☒	-
	3.	☒	☒	☒	-	-	-	☒	☒	☒	☒	☒	☒	☒	☒	-	☒	☒	-
Vzduchotechnická zařízení	1.	☑	☑	☑	☑	-	-	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	-
	2.	☑	☑	☑	☒	-	-	☒	☑	☑	☒	☑	☑	☒	☑	☒	☑	☑	-
	3.	☒	☒	☒	☒	-	-	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	-
Mobilní stroje a zařízení	1.	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	-	☑	☑	-
	2.	☑	☒	☒	-	-	-	☒	☒	☒	☒	☑	☒	☒	☒	-	☒	☒	-
	3.	☒	☒	☒	-	-	-	☒	☒	☒	☒	☒	☒	☒	☒	-	☒	☒	-
Ostatní důležitá zařízení	1.	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	-	☑	☑	-
	2.	☑	☑	☑	-	-	-	☒	☑	☑	☒	☑	☑	☒	☑	-	☑	☑	-
	3.	☒	☒	☒	-	-	-	☒	☒	☒	☒	☒	☒	☒	☒	-	☒	☒	-
Staniční jednotky řídicího systému	1.	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	-	☑	☑	-
	2.	☑	☑	☑	-	-	-	☒	☑	☑	☒	☑	☑	☒	☑	-	☑	☑	-
	3.	☒	☑	☑	-	-	-	☒	☑	☑	☒	☒	☑	☒	☑	-	☑	☑	-
Zabezpečovací zařízení	1.	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	-	☑	☑	-
	2.	☑	☑	☑	-	-	-	☒	☑	☑	☑	☑	☑	☒	☑	-	☑	☑	-
	3.	☑	☑	☑	-	-	-	☒	☑	☑	☒	☑	☑	☒	☑	-	☑	☑	-
Toky	1.	☑	☑	☑	☑	-	-	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	2.	☑	☑	☑	☒	☒	☒	☒	☑	☑	☒	☑	☑	☒	☑	☒	☑	☑	☒
	3.	☒	☑	☒	☒	☒	☒	☒	☑	☑	☒	☑	☑	☒	☑	☒	☑	☑	-

Tabulka 15: Pokrytí vrstev ochrannými mechanizmy - pokračování

Legenda: ☑ - podchycené příslušnými opatřeními, ☒ - částečné opatření, ☒ - nepodchycené

	Pokrytí vrstvy	Poh. V územní inf.	Poh. V kybernetické i.	Služby, zás., spojení	Velká znečištění	Selhání technologií	Ztráty obslužnosti	Stabilita podloží, vib.	Kontaminace ovzduší	Kontaminace vody	Rychlé variace klimatu	Migrace vel. skup. lidí	Organizační havárie	Toky surovin a výrob.	Toky energií	Toky informací
Lidé	1.	-	-	-	☑	☑	-	☑	☑	☑	☑	☑	☑	-	☑	-
	2.	-	-	-	☒	☑	-	☑	☒	☒	☑	☑	☒	-	☑	-
	3.	-	-	-	☒	☒	-	☒	☒	☒	☒	☒	☒	-	☒	-
Objekty	1.	-	☑	-	☑	☑	-	☑	☑	☑	☑	☑	☑	-	☑	☑
	2.	-	☒	-	☒	☑	-	☒	☒	☒	☑	☒	☒	-	☑	☒
	3.	-	☒	-	☒	☑	-	☒	☒	☒	☑	☒	☒	-	☑	☒
Energetická zařízení	1.	-	☑	-	-	☑	-	☑	-	-	☑	☑	☑	-	☑	☑
	2.	-	☒	-	-	☑	-	☑	-	-	☑	☑	☒	-	☑	☒
	3.	-	☒	-	-	☑	-	☑	-	-	☑	☒	☒	-	☑	☒
Sdělovací zařízení	1.	-	☑	-	-	☑	-	☑	-	-	☑	☑	☑	-	☑	☑
	2.	-	☒	-	-	☑	-	☑	-	-	☑	☒	☒	-	☑	☒
	3.	-	☒	-	-	☑	-	☑	-	-	☑	☒	☒	-	☑	☒
Strojní zařízení	1.	-	☑	-	-	☑	-	☑	-	-	☑	☑	☑	-	☑	☑
	2.	-	☒	-	-	☒	-	☒	-	-	☒	☒	☒	-	☒	☒
	3.	-	☒	-	-	☒	-	☒	-	-	☒	☒	☒	-	☒	☒
Vzduchotechnická zařízení	1.	-	☑	-	☑	☑	-	☑	☑	-	☑	☑	☑	-	☑	☑
	2.	-	☒	-	☒	☑	-	☑	☒	-	☑	☒	☒	-	☑	☒
	3.	-	☒	-	☒	☒	-	☒	☒	-	☒	☒	☒	-	☒	☒
Mobilní stroje a zařízení	1.	-	☑	-	-	☑	-	☑	-	-	☑	☑	☑	-	☑	☑
	2.	-	☒	-	-	☒	-	☒	-	-	☒	☒	☒	-	☒	☒
	3.	-	☒	-	-	☒	-	☒	-	-	☒	☒	☒	-	☒	☒
Ostatní důležitá zařízení	1.	-	☑	-	-	☑	-	☑	-	-	☑	☑	☑	-	☑	☑
	2.	-	☒	-	-	☑	-	☑	-	-	☑	☒	☒	-	☑	☒
	3.	-	☒	-	-	☒	-	☒	-	-	☒	☒	☒	-	☒	☒
Staniční jednotky řídicího systému	1.	-	☑	-	-	☑	-	☑	-	-	☑	☑	☑	-	☑	☑
	2.	-	☑	-	-	☑	-	☑	-	-	☑	☒	☒	-	☑	☑
	3.	-	☒	-	-	☑	-	☑	-	-	☑	☒	☒	-	☑	☒
Zabezpečovací zařízení	1.	-	☑	-	-	☑	-	☑	-	-	☑	☑	☑	-	☑	☑
	2.	-	☒	-	-	☑	-	☑	-	-	☑	☒	☑	-	☑	☒
	3.	-	☒	-	-	☑	-	☑	-	-	☑	☒	☒	-	☑	☒
Toky	1.	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	2.	☒	☑	☒	☒	☑	☒	☑	☒	☒	☑	☒	☒	☒	☑	☑
	3.	-	☒	-	☒	☑	-	☑	☒	☒	☑	☒	☒	-	☑	☒

Výsledkem analýzy tabulek 14 a 15 je zjištění, že mnoho chráněných aktiv vybrané stanice metra není dostatečně chráněno při výskytu relevantních pohrom. Navíc zde nejsou zahrnuté další vrstvy v případě provozu v abnormálních a kritických podmínkách. V uvedené čtvrté a páté vrstvě lze v případě pražského metra najít několik dílčích plánů, ale uvedené plány nejsou postaveny na All-Hazard-Approach a také nezahrnují identifikaci chráněných aktiv a jejich ochranu.

6 Plán řízení rizik

Předchozí kapitola ukazuje, že je v současné koncepci bezpečnosti mnoho nedostatků z pohledu konceptu aplikace integrální bezpečnosti. Jak již bylo v předchozích kapitolách řečeno, v praxi se u nejvíce kritických technologických objektů používá obrana do hloubky pomocí pěti vrstev ochranných opatření. Zavedení veškerých opatření pro všech pět vrstev ochrany dle přístupu Defence-In-Depth je velmi finančně, časově i technicky náročné. V některých případech i znalostně, protože z důvodu architektury SoS, tj. otevřený systém vzájemně propojených a otevřených systémů, je nutno počítat s existencí konfliktů a s výsledkem realizace rizik. Pro snížení nákladů a složitosti výpočtů kritičnosti je pro méně kritické objekty možné počet vrstev zredukovat a hledat relevantní opatření jen pro nejkritičtější pohromy a nejzranitelnější chráněná aktiva. K účelům určení kritičnosti pohrom a zranitelnosti chráněných aktiv je zapotřebí bližší spolupráce se vyššími vrstvami řízení bezpečnosti (na úrovni obce, kraje až státu), dále je nutné zavést předběžná opatření, monitoring a mezioborovou komunikaci. Na rizika plynoucí z vnitřní struktury systému se musí pohlížet stejně tak jako na vnější rizika, tj. problematika bezpečnosti a zabezpečení, kde se jednotlivé aspekty mohou navzájem pozitivně, ale i negativně ovlivňovat.

Jinými slovy lze říct, že bezpečnost drážních objektu lze zvýšit a především proaktivně řídit zavedením několika známých technik řízení bezpečnosti dle [9] jako opatření ke zvýšení bezpečnosti objektu:

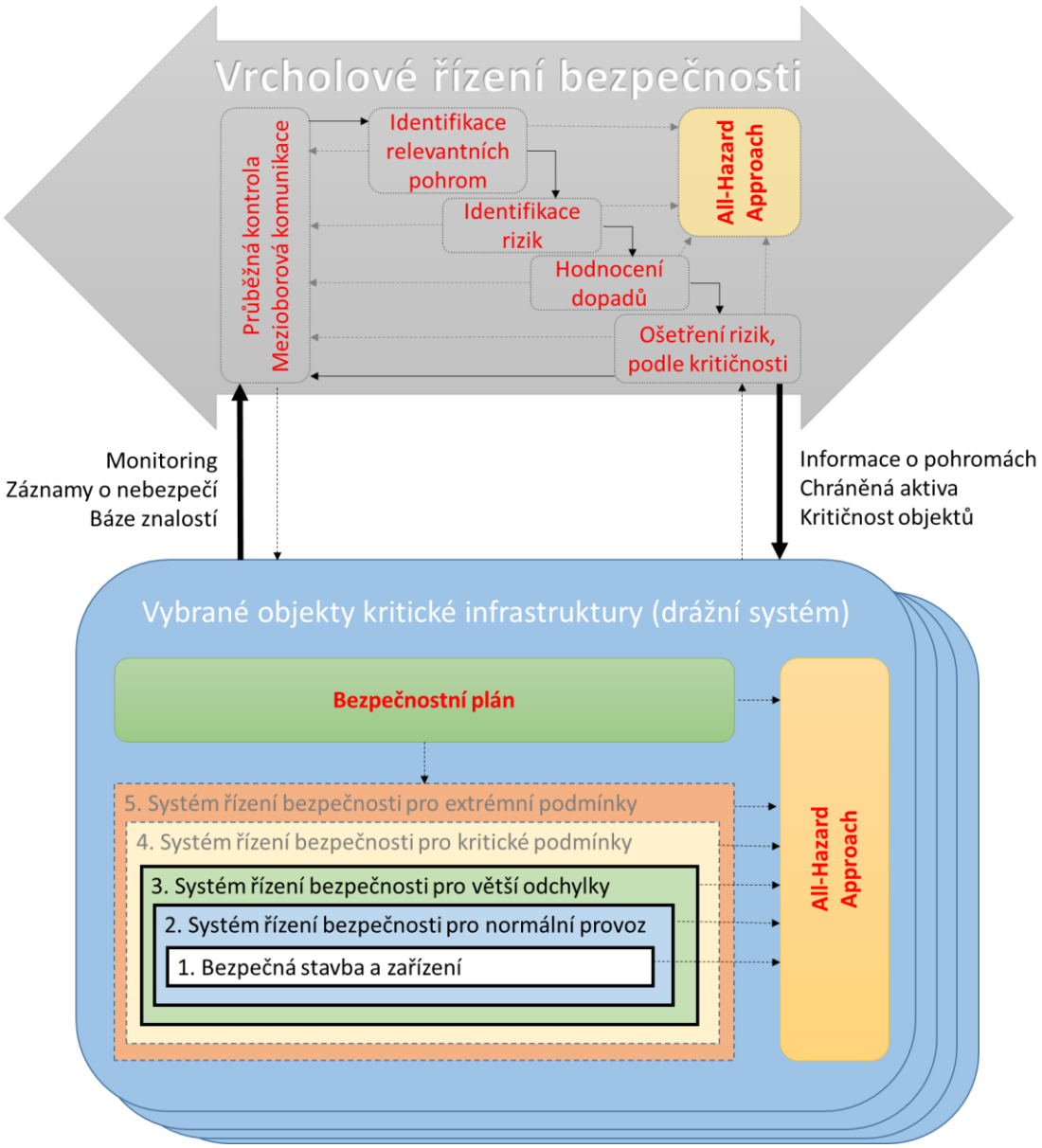
1. Zavedení návaznosti vývoje drážních systémů a objektů na vrcholové řízení bezpečnosti.
2. V rámci vrcholového řízení bezpečnosti a řízení bezpečnosti území určit chráněná aktiva a objekty kritické infrastruktury včetně objektů drah.
3. Určit kritičnost vybraných objektů kritické infrastruktury.
4. Dle míry kritičnosti zvolit třístupňový až pětistupňový model řízení bezpečnosti.
5. Aplikovat dosavadní metody na drážní systémy respektive objekty a přidat jednotlivé nároky příslušných vrstev řízení bezpečnosti.
6. Při návrhu drážního systému zavést metodiku pro zajištění zabezpečení (security) systému a jeho kybernetické infrastruktury s posouzením vlivu vzájemných vazeb na bezpečnost.

Kapitola v souladu se současnou odbornou praxí předkládá obecný plán řízení rizik a plán řízení rizik vybraného objektu kritické infrastruktury v drážním systému, jenž zachycuje různé relevantní oblasti bezpečnostních rizik.

6.1 Obecný plán řízení bezpečnostních rizik

Doplněním výsledků předložené práce a navrhovaných technik popsaných v úvodu kapitoly do známých modelů řízení bezpečnosti uvedených v kapitole 1., jsme sestavili obecný plán řízení bezpečnostních rizik.

Obecný plán řízení bezpečnostních rizik je znázorněn na obrázku 12.



Legenda:
- informační tok
- posloupnost procesů
- vazba závislostí (závisí na…)
- povinná opatření
- opatření volitelná dle kritičnosti objektu
- použité metody a techniky

Obr. 12: Obecný plán řízení bezpečnostních rizik.

Obrázek 12 popisuje propojení vrstev vrcholového řízení bezpečnosti s nižšími vrstvami řízení bezpečnosti konkrétních objektů kritické infrastruktury. Kritická infrastruktura musí být identifikována na základě hodnocení integrálního rizika a přístupu All-Hazard-Approach s využitím mezioborové komunikace, zkušeností z minulosti, tj. informací ze zavedeného monitoringu. Vybraný objekt KI využívá tří až pětistupňového modelu řízení bezpečnosti podle určené kritičnosti z vyšší vrstvy. Zajištění bezpečnosti objektu kritické infrastruktury, tedy i vybrané stanice metra, je zachyceno v bezpečnostním plánu. Bezpečnostní plán je přímo závislý na pětistupňovém modelu (Defence-In-Depth) a All-Hazard-Appoach.

Hledání ochranných opatření v jednotlivých vrstvách a jejich vzájemných vazeb i vazeb na okolní systémy bude předmětem dalšího výzkumu. I přesto jsou v drážním prostředí, pro vybranou stanici pražského metra, již zavedené některé metody pro práci s riziky.

Bezpečná stavba je zajištěna stavebním zákonem 0 a zákonem o drahách [41]. Bezpečné zařízení podléhá řadě drážních norem, avšak z hlediska systému je klíčová definice životního cyklu systému, ve kterém se dle EN 50126 [12] provádí úkoly pro stanovení a prokázání RAMS a to na základě identifikaci nebezpečí a řízení rizik ve vrstvě konkrétního drážního systému.

Jedním z prvních kroků pro stanovení RAMS je určení ovlivňujících činitelů, které mají vliv na RAMS. Bez návaznosti na vyšší vrstvy řízení bezpečnosti je provozovatel dráhy odkázán pouze na svůj subjektivní názor a popřípadě několik málo definovaných činitelů určených normou. Proto je nutné určit relevantní vnější činitele z vyšších vrstev řízení jako možné vnější vlivy na systém a uvést je v analýze rizik systému. Provozovatel dráhy či jiná drážní autorita z výsledků analýzy rizik zadává detailní požadavky na bezpečnost dodavatelům a ti dále pak svým subdodavatelům. Každý subjekt drážního průmyslu musí prokázat své kompetence, kvalitu služeb, prokázat bezpečnost produktů a splnit požadavky na zabezpečení zařízení. Uvedené kvality a bezpečnost se dokládají dokumentací zavedených procesů příslušných norem, především ISO 9001 [19], IRIS [18] a EN 50126 [12], z nižší úrovně pro vývoj jednotlivých bezpečnostně relevantních systémů pak EN 50129 [20], EN 50128 [21], EN 50159 [22].

V každé vrstvě drážního systému se provádí analýza rizik, jejíž výstupem jsou bezpečnostně relevantní funkce, tj. funkce, které jsou v analýze identifikované jako nejrizikovější anebo jsou zavedené jako ochrana ke snížení rizika. Předmětné funkce se přiřazují zabezpečovacím zařízením s definovanou integritou bezpečnosti (SIL), podle kritičnosti.

Bezpečnost produktu, resp. kritické komponenty, mající vliv na bezpečnost, se dokazuje průkazem bezpečnosti dle EN 50129 [20] a EN 50128 [21]. Průkaz bezpečnosti se musí v daném případě orientovat i na zabezpečení, což není v drážním průmyslu zvykem. Průkazy

bezpečnosti dodaných kritických produktů hodnotí nezávislí posuzovatelé. Předmětné průkazy se musí předkládat zpět do vyšších úrovní řízení k ověření a implementaci těchto zařízení či jejich změn do větších celků.

Samotný životní cyklus systému na drahách je koncipován jako V-model s fázemi, které mají své vstupy a výstupy. V jednotlivých fázích životního cyklu se provádí úkoly. Úkoly fází životního cyklu se dělí na projektové, kvalitativní a bezpečností [12]. Pro zajištění kybernetické bezpečnosti kritické infrastruktury je nutné respektovat kybernetický zákon [45], ale vzhledem k jeho obecnosti je dále zapotřebí zavést procesy a požadavky standardu ISA99 [24] a evropské normy EN 15408 [23]. Do drážního V-modelu a jeho jednotlivých fází lze implementovat nové úkoly plynoucí s výše uvedených norem, standardů a opatření. Řešení závislostí otázek bezpečnosti a zabezpečení je definováno vlastními úkoly prováděnými vždy na konci fáze životního cyklu a to podle evropského projektu SESAMO [44].

Velkou výhodou drážních procesů je povinnost zaznamenávat veškeré hrozby, které jsou v rámci celého životního cyklu identifikované. Práce s hrozbami vyžaduje opakovanou analýzu rizik a zavádění stále nových opatření, ať už se jedná o vlastní bezpečnost objektu / systému / zařízení či komponenty nebo IT bezpečnostní hrozby. Relevantní hrozby z vyšších vrstev drážního systému mohou sloužit jako vstup pro vrcholové řízení bezpečnosti k jejich analýze z ještě vyššího pohledu a z úrovně dané oblasti, k mezioborové diskuzi, hledání závislostí, či posuzování kvality zvolené metodiky řízení rizik. Jinými slovy, zaznamenávání hrozeb umožní identifikovat kritická místa systému relevantní k bezpečnosti a zavést patřičné bezpečnostně relevantní funkce nebo jiná opatření.

Životní cyklus drážního systému je dostatečně obecný a dokáže pokrýt první tři vrstvy řízení bezpečnosti dle přístupu Defence-In-Depth a to s jasně definovanými úkoly a odpovědnostmi. Poslední dvě vrstvy lze do uvedeného modelu doplnit, ovšem to vyžaduje mnohem větší znalosti ohledně vzájemných vazeb mezi systémy a jednotlivými vrstvami pro zajištění bezpečnosti včetně vrcholového řízení bezpečnosti pomocí SMS, které není v drážní praxi zavedeno a jde tedy o opatření, které je nutné pokrýt jinými legislativními opatřeními.

6.2 Plán řízení bezpečnostních rizik vybrané stanice metra

Plán řízení bezpečnostních rizik vybraného objektu na drahách 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.

Předmětný plán řízení rizik je vypracován formou tabulky v souladu s technikou uvedenou v odstavci 1.5, která uvádí relevantní oblasti rizik, popis rizik, jejich pravděpodobnost výskytu,

jejich dopady a návrh možných opatření na zmírnění rizika. Protože lidský faktor je významným činitelem, a to zvláště jako příčina organizačních havárií špatné rozhodnutí, špatné řízení) [52], soustředili jsme se dále na oblast řízení, tj. systém SMS. Tabulku 16 je nutné v rámci životního cyklu objektu pravidelně aktualizovat a bezpečnostní rizika vyhodnocovat, popřípadě doplňovat vhodná opatření na jejich zmírnění.

Tabulka 16: Plán řízení bezpečnostních rizik vybraného objektu na drahách.

Oblast rizika	**Popis rizika**	**Pravděpodobnost výskytu a dopady rizika**	**Opatření na zmírnění rizika**
Poruchy jednotlivých vrstvách SMS	Slabiny v zabezpečení vůči vnějším vlivům.	Pravděpodobnost: střední Dopady: mírné až vysoké	Bezpečnostní plán založený na integrálním riziku, All-Hazard-Approach a Defence-in-Depth.
	Výskyt vnitřních náhodných poruch systému.	Pravděpodobnost: nízká dle SIL Dopady: vysoké	Systém řízení kvality ISO 9001, IRIS, zavedení alespoň SIL 0 na všechny E/E/PE, nezávislá kontrola a audit.
	Výskyt vnitřních systémových poruch zařízení.	Pravděpodobnost: nízká dle SIL Dopady: vysoké	Systém řízení kvality ISO 9001, IRIS, zavedení alespoň SIL 0 na všechny E/E/PE, nezávislá kontrola a audit.
	Poruchy v procesech, lidská chyba.	Pravděpodobnost: velmi vysoká Dopady: vysoké	Systém řízení kvality ISO 9001, IRIS, školení, přezkoušení, cvičení, potvrzovací funkce E/E/PE, zavedení zpětných vazeb.
	Omezené zdroje	Pravděpodobnost: nízká Dopady: střední	Projektový management, systém řízení kvality ISO 9001, IRIS.
	Vzájemné vlivy požadavků na bezpečnost a zabezpečení	Pravděpodobnost: vysoká Dopady: střední	Analýza závislostí, hledání kompromisů dle projektu SESAMO.
	Chybná nebo nedostatečná identifikace ovlivňujících činitelů.	Pravděpodobnost: střední Dopady: vysoké	EN 50126, nezávislé posouzení, monitoring a mezioborová komunikace.
	Chybná práce s riziky, volba metody, definice stupnic, ohodnocení rizik.	Pravděpodobnost: nízká Dopady: vysoké	EN 50126, nezávislé posouzení, monitoring a mezioborová komunikace.
	Odpovědnosti, kompetence, nezávislost a důvěrnost řešitelských subjektů.	Pravděpodobnost: nízká Dopady: vysoké	EN 50126, jasná definice rolí, projektové řízení, systém řízení kvality ISO 9001, nezávislé hodnocení.

Tabulka 177: Plán řízení bezpečnostních rizik vybraného objektu na drahách - pokračování.

Vzájemné vazby a toky s vedlejšími a nadřazenými systémy	Přenos chybných a matoucích informací, tj. chyby na vstupu nebo na výstupu systémů.	Pravděpodobnost: střední Dopady: velmi vysoké	Monitoring a mezioborová komunikace, jednotná terminologie.
	Přerušení informačních a materiálových toků.	Pravděpodobnost: nízká Dopady: vysoké	Vytváření záloh a redundantních systémů
	Vykonávání navzájem se ovlivňujících funkcí.	Pravděpodobnost: vysoká Dopady: vysoké	Monitoring a mezioborová komunikace.
	Poruchy okolních systémů a realizace relevantních pohrom.	Pravděpodobnost: střední Dopady: velmi vysoké	Monitoring a mezioborová komunikace.
Vazby mezi jednotlivými vrstvami systému řízení bezpečnosti	Chybná metodika identifikace nebezpečí a analýzy rizik z vyšších úrovní SMS.	Pravděpodobnost: vysoká Dopady: velmi vysoké	Monitoring a mezioborová komunikace, jednotná terminologie.
	Neporozumění požadavkům a informacím z jiné vrstvy SMS.	Pravděpodobnost: vysoké Dopady: vysoké	Monitoring a mezioborová komunikace, jednotná terminologie, vzdělávání, kompetence.
	Přenos poruchových stavů v případě jejich výskytů z jedné vrstvy do druhé.	Pravděpodobnost: střední Dopady: střední	Přiměřená nezávislost vrstev, fyzické oddělení, diverzitní sběr informací.
	Chybějící vstupní informace.	Pravděpodobnost: vysoká Dopady: velmi vysoké	Vrcholové řízení bezpečnosti, vzdělávání, výzkum.
Jiné nepředvídatelné události a lidský faktor	Vnější faktory	Pravděpodobnost: vysoké Dopady: střední	Zabezpečení, monitoring, připravenost.
	Vnitřní faktory	Pravděpodobnost: střední Dopady: vysoké	Systém řízení kvality ISO 9001, IRIS, školení, přezkoušení, cvičení, kompetence, zabezpečení dle ISA 99, CC.
	Úmyslná poškození	Pravděpodobnost: nízká Dopady: velmi vysoké	Požadavky na zabezpečení ISA 99, CC, monitoring.

Tabulka 16 zachycuje několik základních skupin rizik, se kterými je v rámci SMS objektů kritické infrastruktury potřeba pracovat. Předmětem diplomové práce není popisovat a vyhodnocovat uvedená rizika, ale ukázat plán pro jejich zvládnutí, který tabulkou 16 reprezentován. Výzkum předmětné oblasti musí dále pokračovat, aby se zlepšilo řízení bezpečnosti po celou dobu životnosti technického díla.

Závěr

Cílem předložené diplomové práce bylo vypracování bezpečnostního plánu. Předmětný bezpečnostní plán byl vypracován na základě znalostí o pohromách, na základě získaných poznatků o pražském metru a jeho systému řízení a na základě informací relevantních k vybrané modelové stanici, která zahrnuje typické rysy všech stanic. Práce s daty a postupy pro vypracování bezpečnostního plánu jsou provedeny v souladu s požadavky na sběr dat, zapracování dat a s požadavky konceptu integrální bezpečnosti, který vychází ze systémového chápání sledované entity.

Sestavený bezpečnostní plán obsahuje popis vybrané modelové stanice s analýzou dopadů pohrom pomocí metody What, If, pomocí které byla určena kritičnost v případě dvou vybraných pohrom. Pro předmětné dvě pohromy byl sestaven bezpečnostní plán s návrhem na preventivní a ochranná opatření, která mají zajistit bezpečí analyzovaných chráněných aktiv stanice i veřejných aktiv. Preventivní a ochranná opatření jsou popsaná obecně, jelikož konečné řešení musí být výsledkem několikaleté inženýrské činnosti založené na ověřených relevantních místně specifických informacích a vhodně zvolených metod.

Bezpečnostní plány pro dvě vybrané pohromy popisují preventivní opatření, ochranné mechanismy pro zmírnění pohromy, scénáře odezvy, evakuační plány, varovací systém, cvičení a výcvik, plány odezvy, plány obnovy. První pohroma, výpadek elektrické energie, vyžaduje opatření především ve formě vytváření záloh elektrické energie, náhradní zdroje pro kritická zařízení, materiálové zásoby pro výrobu náhradní elektrické energie, plány kontinuity pro výpadek elektřiny a postupné odpojování méně potřebných systémů. Druhá pohroma, útok na tok dat, je mnohem hůře předvídatelná a vzhledem k úmyslnosti útoku může mít až fatální následky. Obranou proti danému typu útoků je dobře proškolený personál, zavedení zabezpečovacích procesů pro výrobu a provoz kritických zařízení, fyzická a kybernetická oddělení zařízení a technologických sítí dle kritičnosti, zajištění důvěryhodnosti personálu a relevantních rolí v systému, sledování procesů a sítí, řešení konfliktů mezi požadavky bezpečnosti a zabezpečení, plány pro odpojování sítí a jiné. Pro obě pohromy je nutné zavést procesní řízení, zajistit plány kontinuity a evakuace, systém hlášení, zajistit patřičné výcviky a školení a v neposlední řadě vytvořit přesné plány odezvy a obnovy, kde je cílem návrat systému do normálního stavu.

Bezpečnostního plán, který zohlednil způsob zajištění bezpečnosti přístupem Defence-In-Depth v pětistupňovém modelu, byl metodou shody porovnán se současnou praxí v drážním prostředí, která je určená drážní legislativou, normami a předpisy. Výsledkem bylo zjištění, že současná praxe nesplňuje nároky pro pokrytí všech vrstev pětistupňového modelu, který je produktem současného vrcholového odborného poznání. Proto lze předpokládat, že nebude

zajištěna bezpečnost všech chráněných aktiv stanice metra za podmínek abnormálních a kritických.

Koncept popsaný v kapitole 6 navrhuje několik technik, kterými lze identifikované nedostatky v bezpečnosti drážního systému, tj. vybrané stanice metra, výrazným způsobem eliminovat. Metody jsou zobrazené v obecném plánu řízení bezpečnostních rizik na obrázku 12. V předmětném odstavci je uveden návrh, jak dané techniky aplikovat a to s respektováním současné drážní legislativy, evropských vyhlášek a norem.

Plán řízení bezpečnostních rizik vybraného objektu na drahách v tabulce 16 rozděluje bezpečnostní rizika do skupin podle oblasti, kde se daná rizika vyskytují. Předmětná rizika jsou spojena se systémem řízení bezpečnosti stanice metra a zavedenou metodou Defence-In-Depth na základě integrální bezpečnosti a přístupu All-Hazard-Approach.

Z výše uvedeného je patrné, že předložená diplomová práce dosáhla všech definovaných cílů. Výsledky práce lze navíc aplikovat v praxi ve formě informačně vzdělávacího materiálu, jelikož obsahuje komplexní pohled na problematiku řízení bezpečnosti ve více vrstvách. Dále lze z informací uvedených v práci vycházet i pro případné návrhy k doplnění současné legislativy, což povede ke zvýšení bezpečnosti objektů kritické infrastruktury. Předložená diplomová práce také otevírá cestu k dalšímu výzkumu bezpečnostních rizik hlavně z hlediska vzájemných vazeb mezi systémy (SoS) a mezi jednotlivými vrstvami systémů zajištění bezpečnosti. Daným směrem se bude ubírat také má další akademická práce i činnosti v praxi.

Seznam literatury a zdroje

[1] PROCHÁZKOVÁ, Dana. *Bezpečnost kritické infrastruktury*. Praha: České vysoké učení technické v Praze, 2012. ISBN 978-80-01-05103-0.

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

[3] PROCHÁZKOVÁ, Dana. *Analýza a řízení rizik*. V Praze: České vysoké učení technické, 2011, 405 s. ISBN 978-80-01-04841-2.

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

[5] PROCHÁZKOVÁ, Dana. *Krizové řízení pro technické obory*. V Praze: České vysoké učení technické, 2013, 303 s. ISBN 978-80-01-05292-1.

[6] ARCHIV HLAVNÍHO MĚSTA PRAHY. *Archivní katalog* [online]. 2015 [cit. 2015-04-19]. Dostupné z: http://www.ahmp.cz/index.html?wstyle=2&catalogue=1

[7] PROCHÁZKOVÁ, Dana. *Přehled metodik pro analýzu rizik*, Ministerstvo vnitra - Generální ředitelství HZS ČR, 2004. Č. j.: PO-58-7/PLA-2004

[8] PROCHÁZKOVÁ, Dana. *Metody, nástroje a techniky pro rizikové inženýrství*. V Praze: České vysoké učení technické, 2011, 369 s. ISBN 978-80-01-04842-9.

[9] KERTIS, Tomáš. Snížení kritičnosti objektů kritické infrastruktury v drážním prostředí [online]. Regionální rozvoj mezi teorií a praxí 2015 – v tisku. ISSN 1805-3246. Dostupné z: http://www.regionalnirozvoj.eu/

[10] ČR. ČSN EN 61511-1. Funkční bezpečnost - Bezpečnostní přístrojové systémy pro sektor průmyslových proces - Část 1: Požadavky na systémy hardwaru a softwaru, struktura, definice. Praha: ÚNMZ, 2005.

[11] ČR. ČSN EN 61508-1 ed. 2 (180301). Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky. Praha: ÚNMZ, 2005.

[12] ČR. ČSN EN 50126-1 (333502). *Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS): Část 1: Základní požadavky a generický proces*. Praha: Český normalizační institut, 2001.

[13] PROCHÁZKOVÁ, Dana. *Strategie řízení bezpečnosti a udržitelného rozvoje území.* ISBN 978-80-7251-243-0, Praha 2007

[14] IAEA. *Safety Reports Series: Assessment of Defence in Depth for Nuclear Power Plants*. Vienna: International Atomic Energy Agency, 2005. ISBN 92-0-114004-5. Dostupné z: http://www-pub.iaea.org/books/IAEABooks/7099/Assessment-of-Defence-in-Depth-for-Nuclear-Power-

Plants

[15] PROCHÁZKOVÁ, Dana. *Ochrana lidí před dopady nebezpečných látek implementovaná v konceptu řízení integrální bezpečnosti technologických objektů a infrastruktur.* ISBN: 978-80-7385-158-3, ISSN 1803-7372**.** *Ochrana obyvatelstva - Nebezpečné látky 2015.* Ostrava: SPBi 2015, p 138-143.

[16] ČR. *Směrnice Evropského Parlamentu a Rady 2004/49/ES ze dne 29. dubna 2004: o bezpečnosti železnic Společenství a o změně směrnice Rady 95/18/ES o vydávání licencí železničním podnikům a směrnice 2001/14/ES o přidělování kapacity železniční infrastruktury, zpoplatnění železniční infrastruktury a o vydávání osvědčení o bezpečnosti.* In: Úř. věst. L 220. 2004. Dostupné z: http://www.dicr.cz/uploads/dokumenty/2004_49.pdf

[17] ČR. NAŘÍZENÍ KOMISE (ES) č. 352/2009: o přijetí společné bezpečnostní metody pro hodnocení a posuzování rizik, jak je uvedeno v čl. 6 odst. 3 písm. a) směrnice Evropského parlamentu a Rady 2004/49/ES. In: *Úřední věstník Evropské unie*. 2009. Dostupné z: http://www.mdcr.cz/NR/rdonlyres/FCA4F75A-04B5-485F-A2CD-57F25CB17B9E/0/32009R0352hodnoceni_rizik.pdf

[18] IRIS Rev. 02.1. *International Railway Industry Standard*. Belgium: UNIFE, 2012. Dostupné z: http://www.iris-rail.org/

[19] ČR. ČSN EN ISO 9001:2009 (01 0321). *Systémy managementu kvality – Požadavky.* Praha: ÚNMZ, 2009.

[20] ČR. ČSN EN 50129 (34 2680). Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy. Praha: ÚNMZ, 2012.

[21] ČR. ČSN EN 50128 (342680). Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídicí a ochranné systémy. Praha: ČNI, 2002.

[22] ČR. ČSN EN 50159 (342670). Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat. Praha: ÚNMZ, 2011.

[23] ČR. ČSN ISO/IEC 15408-1 (36 9789). *Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT: Část 1: Úvod a všeobecný model*. Praha: ČNI, 2001.

[24] ANSI/ISA–62443-1-1 (99.01.01)-2007. Security for Industrial Automation and Control Systems: Terminology, Concepts, and Models. EU: ISA, 2007.

[25] PROCHÁZKOVÁ, Dana. *Plány řízení rizik usnadňují řízení podniků zacílené na rozvoj.* In: Rizika podnikových procesů 2014. Tištěný - ISBN: 978-80-7414-766-1. Elektronický – ISBN: 978-80-7414-767-8. Ústí n. L: UJEP 2014,73-80.

[26] *METROWEB* [online]. 2015 [cit. 2015-03-15]. ISSN 1802-2820. Dostupné z: http://www.metroweb.cz/

[27] KOLEKTIV PRACOVNÍKŮ METROPROJEKTU PRAHA A. S. *Publikace IV. C2*. 2008. Dostupné z: http://www.praha.eu/public/0/a3/da/186337_4_Publikace_IV._C2.pdf

[28] UNICONTROLS A. S. *Case Study: Metro Praha*. 2014.

[29] Dopravní podnik hl. m. Prahy. *DP kontakt: Časopis zaměstnanců Dopravního podniku hl. m. Prahy, akciové společnosti*. Praha: DPP, 1999-2005. ISSN 1212-6349. Dostupné z: http://www.dpp.cz/dp-kontakt

[30] ČR. ČSN EN 13816 (269389). *Doprava – Logistika a služby – Veřejná přeprava osob – definice jakosti služby, cíle a měření.* Praha: ČNI, 2003.

[31] ČR. 376/2006 Sb.: Vyhláška o systému bezpečnosti provozování dráhy a drážní dopravy a postupech při vzniku mimořádných událostí na dráhách. In: *SBÍRKA PŘEDPISŮ ČESKÉ REPUBLIKY*. 2006.

[32] ČR. ČSN EN 62290-1:2006 (33 3530). *Drážní zařízení - Systémy řízení městské dopravy s vyhrazenou vodicí dráhou: Část 1: Systémové principy a základní pojmy*. Praha: ČNI, 2007.

[33] ČR. ČSN EN 62267:2009 (333532). *Drážní zařízení - Automatizovaná městská doprava s vyhrazenou vodicí dráhou (AUGT) - Bezpečnostní požadavky*. Praha: ÚNMZ, 2010.

[34] ČR. Zákon č. 2/1969, o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky. In: *2/1969 Sb.* 1969. Dostupné z:

http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=31338&nr=2~2F1969&rpp=15#local-content

[35] Mapy.cz. SEZNAM.CZ, a.s. *Mapy.cz* [online]. 2015 [cit. 2015-03-15]. Dostupné z:

www.mapy.cz

[36] UN. *Human Development Report*. New York 1994. Dostupné z:

http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

[37] EU: PASR project. EU 2006.

[38] Odborové orgány Dopravního Podniku hl. m. Prahy: ústní sdělení.

[39] Odborové orgány Magistrátu hl. m Prahy: ústní sdělení.

[40] *Google* [online]. 2015 [cit. 2015-05-20]. Dostupné z: www.google.com

[41] ČR. Zákon č. 266/1997, o drahách, In: *Sbírka zákonů ČR*. 1997. Dostupné z:

http://www.podnikatel.cz/zakony/zakon-o-drahach/uplne/

ČR. Zákon č. 183/2006, o územním plánování a stavebním řádu (stavební zákon), In: *Sbírka zákonů* ČR. 2006. Dostupné z: http://business.center.cz/business/pravo/zakony/stavebni/

[42] ČR. Zákon č. 22/1997, o technických požadavcích na výrobky a o změně a doplnění některých zákonů. In: *Sbírka zákonů* ČR. 1997. Dostupné z: http://www.tzb-info.cz/pravni-predpisy/zakon-c-22-1997-sb-o-technickych-pozadavcich-na-vyrobky

[43] ČR. Nařízení vlády č. 163/2002 Sb., kterým se stanoví technické požadavky na vybrané stavební výrobky. 2002. Dostupné z: http://www.unmz.cz/cz/30/163_02.htm

[44] ARTEMIS Joint Undertaking. *Integrated Design and Evaluation Methodology.* In: *SESAMO: Security and Safety Modelling* [online]. 2014 [cit. 2015-03-26]. Dostupné z: http://sesamo-project.eu/sites/default/files/downloads/publications/integrated-design-and-evaluation-communication-material.pdf

[45] ČR. Zákon č. 181/2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů ČR*. 2014. Dostupné z:

http://www.zakonyprolidi.cz/cs/2014-181

[46] CSIRT - Služby. *CSIRT.CZ* [online]. 2015 [cit. 2015-04-12]. Dostupné z:

https://www.csirt.cz/page/2764/sluzby/

[47] ČR. Zákon č. 240/2000, o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů ČR*. 2000. Dostupné z: http://www.zakonyprolidi.cz/cs/2000-240#cast1

[48] ČR. Zákon č. 430/2010, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. In: *Sbírka zákonů ČR*. 2010. Dostupné z: http://www.zakonyprolidi.cz/cs/2010-430

[49] ČR. ČSN EN 54-1 (342710). *Elektrická požární signalizace - Část 1: Úvod.* Praha: ÚNMZ, 2011.

[50] ČR. ČSN EN 60849 (368012). *Nouzové zvukové systémy*. Praha: ČNI, 1999.

[51] PROCHÁZKOVÁ, Dana. *Základy řízení bezpečnosti KI.* ISBN 978-80-01-0579-6, Praha: ČVUT 2013, 223 p.

[52] PROCHÁZKOVÁ, Dana. *Safety of Complex Technological Facilities.* ISBN 978-3-659-55964-2, Saarbtuecken: Lambert Academic Publishing. 2015, 171 p.

Seznam obrázků

Obr. 1: Účinky extrémních pohrom na veřejná aktiva [5]. 15
Obr. 2: Kategorie pohrom ve sledovaném území [2]. 16
Obr. 3: Pětistupňový model řízení bezpečnosti technologického objektu [15]. 23
Obr. 4: Schema řízení systému pražského metra. 30
Obr. 5: Metro Praha - mapa linek [28]. 31
Obr. 6: Vnější prostory vybrané stanice [27]. 46
Obr. 7: Jižní vestibul vybrané stanice [27]. 47
Obr. 8: Severní vestibul vybrané stanice [27]. 47
Obr. 9: Příčné řezy stanice [27]. 48
Obr. 10: Mapa [35]. 49
Obr. 11: Mapa obecných chráněných aktiv. 49
Obr. 12: Obecný plán řízení bezpečnostních rizik. 80

Seznam tabulek

Tabulka 1: Plán řízení rizik projektu [25]. 26
Tabulka 2: Stupně automatizace [32]. 36
Tabulka 3 Požadavky na rozhraní systému. 36
Tabulka 4: Tabulka četností a pravděpodobnosti výskytu pohrom dle zdroje [7]. 41
Tabulka 5: Příklad tabulky What, If. 42
Tabulka 6: Veřejná chráněná aktiva okolí 50
Tabulka 7 Rozdělení pohrom - relevantní, specifické, kritické. 53
Tabulka 8: Analýza WHAT, IF pro výpadek elektřiny a vliv na okolní aktiva. 55
Tabulka 9: Analýza WHAT/IF pro výpadek elektřiny a vliv na aktiva stanice. 55
Tabulka 10: Analýza WHAT, IF pro útok na tok informací a vliv na veřejná aktiva. 58
Tabulka 11: Analýza WHAT/IF pro útok na tok informací a vliv na aktiva stanice. 59
Tabulka 12: Srovnání nároků pětistupňového modelu na zajištění bezpečnosti s reálným stavem. 72
Tabulka 13: Návrh ochranných mechanizmů. 75
Tabulka 14: Pokrytí vrstev ochrannými mechanizmy. 77
Tabulka 15: Pokrytí vrstev ochrannými mechanizmy - pokračování 78
Tabulka 16: Plán řízení bezpečnostních rizik vybraného objektu na drahách. 83
Tabulka 17: Plán řízení bezpečnostních rizik vybraného objektu na drahách - pokračování. 84