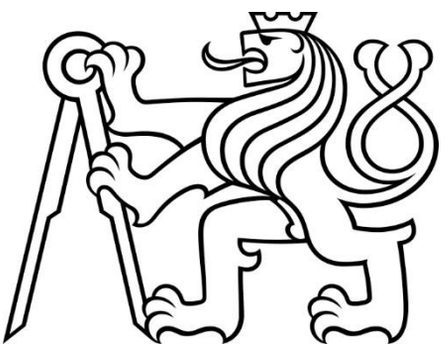
**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**

**FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ**



# BAKALÁŘSKÁ PRÁCE

**2018**

**TOMÁŠ ŠVAGR**

**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE**

**Fakulta biomedicínského inženýrství**
**Katedra zdravotnických oborů a ochrany obyvatelstva**

# Hodnocení vlivu unifikované grafické nadstavby nad bezpečnostně-dohledovými prvky v pražském metru na efektivitu dohledu – případová studie

# Assessment of the influence of the unified graphic superstructure on security-supervisory elements in the Prague underground on the effectiveness of supervision - case study

Bakalářská práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Plánování a řízení krizových situací

Vedoucí práce: Ing. Václav Navrátil

**Tomáš Švagr**

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva | Akademický rok: 2017/2018

# Zadání bakalářské práce

| | |
|---|---|
| Student: | **Tomáš Švagr** |
| Obor: | Plánování a řízení krizových situací |
| Téma: | **Hodnocení vlivu unifikované grafické nadstavby nad bezpečnostně-dohledovými prvky v pražském metru na efektivitu dohledu - případová studie** |
| Téma anglicky: | Assessment of the Influence of the Unified Graphic Superstructure over Security-Supervisory Elements in the Prague Underground on the Effectiveness of Supervision - Case Study |

Zásady pro vypracování:

Cílem bakalářské práce bude přinést ucelený pohled na problematiku unifikovaných grafických nadstaveb nad bezpečnostně-dohledovými prvky, a to včetně jejich eventuálních alternativ, s důrazem na možnost implementace v podmínkách pražského metra a hodnocení efektivity dohledu po nasazení konkrétního řešení. V teoretická část se bude věnovat popisu současného stavu bezpečnostně-dohledové infrastruktury a dohledových postupů v pražském metru a obecným důvodům nasazování unifikovaných grafických nadstaveb a obdobných řešení. V praktické části bude zpracován postup implementace konkrétní unifikované grafické nadstavby a zdůvodněny její dílčí kroky, následně bude objektivně hodnoceno zvýšení efektivity dohledu a zjištěno subjektivní hodnocení nově implementovaného systému na kohortě bezpečnostních pracovníků pražského metra.

Seznam odborné literatury:

[1] LUKÁŠ, Luděk, Bezpečnostní technologie, systémy a management I. , Zlín: VeRBuM, 2011, ISBN 978-80-87500-05-7
[2] ANDERSON, Stephen P., Přitažlivý interaktivní design: jak vytvářet uživatelsky přívětivé produkty, Brno: Computer Press, 2012, ISBN 978-80-251-3722-2
[3] WALKER, Ian, Výzkumné metody a statistika, Praha: Grad, Z pohledu psychologie, 2013, ISBN ISBN 978-80-247-3920-5

Zadání platné do: 20.09.2019

Vedoucí: Ing. Václav Navrátil

.....
vedoucí katedry / pracoviště

.....
děkan

V Kladně dne 19.02.2018

**Kladno, květen 2018**

# Prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Hodnocení vlivu unifikované grafické nadstavby nad bezpečnostně-dohledovými prvky v pražském metru na efektivitu dohledu – případová studie vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití 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 Kladně dne 15.05.2018

……..

Tomáš Švagr

# Poděkování

Rád bych poděkoval vedoucímu mé práce panu Ing. Václavu Navrátilovi za odborné vedení, za pomoc a rady při zpracování této práce. Dále bych chtěl také poděkovat vedoucímu bezpečnostního úseku Dopravního podniku hl. města Prahy panu Lubomíru Šmídovi, za poskytnutí informací a údajů pro praktickou část práce.

# Abstrakt

Práce je věnována bezpečnostním nadstavbám s popisem jejich možných výhod při rozsáhlých instalacích, jako je například Pražské metro. Je zde srovnáno několik nadstaveb nabízených na českém trhu s popisem jejich konkurenčních výhod s následným srovnáním metodou multikriteriální analýzy. Dále je popsán způsob implementace vybraného systému v Pražském metru a popis jeho přínosu v oblasti bezpečnosti.

Pro uvedení do problematiky se práce zabývá popisem bezpečnostních systémů, seznámení s objektovou bezpečností a legislativou, která je k tomuto vztažena.



# Klíčová slova

Softwarová nadstavba, bezpečnost, DPP hl. města Prahy, metro, multikriteriální analýza, komparace, bezpečnostní systém

# Abstract

The work is dedicated to unified graphical extensions - superstructures, describing their possible advantages in large-scale installations, such as the Prague Metro. This work covers several extensions offered on the Czech market with a description of their competitive advantages followed by comparison using a multi-criteria analysis. Furthermore, it describes how to implement the chosen system in the Prague Metro and a description of its contribution in the field of security.

For an introduction to the problematics, this work also covers a description of security systems, building security and safety, and relevant legislation.



# Keywords

Unified Graphical Extensions, The Prague Public Transport Company, a.s., Prague Metro, Prague Subway System, MCDA, Multi-Criteria Decision Analysis, Security System

# Obsah

Použité zkratky ..... 12

1 Úvod ..... 13

2 Bezpečnostní nadstavbové SW ..... 14

3 Objektová bezpečnost ..... 16

3.1 Způsoby zajištění ochrany z pohledu objektové bezpečnosti ..... 16

3.1.1 Fyzická ostraha objektu ..... 16

3.1.2 Technická ochrana ..... 17

3.1.3 Mechanická ochrana ..... 17

3.1.4 Režimová ochrana ..... 18

3.2 Legislativa v objektové bezpečnosti ..... 19

3.2.1 Vyhláška NBÚ o objektové bezpečnosti č. 258/1998 Sb. ..... 19

3.2.2 Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti č. 412/2015 Sb. ..... 20

4 Objektové zabezpečení z technologického hlediska ..... 21

4.1 Mechanické zábranné systémy ..... 21

4.1.1 Obvodové prvky ..... 22

4.1.2 Plášťové prvky ..... 22

4.1.3 Předmětové prvky ..... 22

4.2 Elektronické systémy ..... 23

4.2.1 Elektrická zabezpečovací signalizace ..... 23

4.2.2 Elektronická požární signalizace ..... 24

4.2.3 Kamerový systém ..... 26

4.2.4 Elektronická kontrola vstupu ..... 28

5 Bezpečnostní rizika – pojem, ocenění a projekty ostrahy ..... 30
5.1 Bezpečnostní analýza ..... 30
5.2 Ocenění rizika ..... 31
6 Dopravní podnik hl. m. Prahy ..... 32
6.1 Historie ..... 32
7 Požadovaný přínos projektu JIP ..... 34
8 Popis současného stavu implementace technologií v metru ..... 36
8.1 Informace o plánovaném rozsahu integrace ..... 36
8.1.1 Integrované technologie ..... 36
8.1.2 Integrované území ..... 37
9 Softwarová nadstavba JIP ..... 39
9.1 Stručný popis řešení JIP ..... 39
10 Popis požadavků DPP na software JIP ..... 41
10.1 Klíčové požadavky ..... 41
10.1.1 Vytváření bezpečnostního systému JIP ..... 41
10.1.2 Analýza uložených dat ..... 41
10.1.3 Různé typy incidentů ..... 42
10.1.4 Vazby a skripty ..... 42
10.1.5 Zobrazování mapových podkladů ..... 42
10.2 Obecné požadavky ..... 45
10.2.1 Flexibilita aplikace pro operátory ..... 45
10.2.2 Archivace dat ..... 45
10.2.3 Zálohování dat ..... 45
10.2.4 Bezpečnost systému ..... 46

11 Možné SW nadstavby pro uplatnění v projektu JIP ..... 47
11.1 Nabídka nadstavbových systémů na trhu ..... 47
11.1.1 C4 ..... 47
11.1.2 MrGuard ..... 48
11.1.3 Security Center ..... 49
11.1.4 Latis ..... 50
11.1.5 ALVIS ..... 51
11.1.6 WINMAG ..... 52
11.2 Přínosy nadstavbových systémů pro DPP ..... 53
12 Výběr vhodného systému pro projekt JIP ..... 55
12.1 Multikriteriální analýza pro výběr vhodného systému ..... 55
12.2 Porovnání funkcionalit vybraných systémů ..... 57
13 Realizace projektu s vybraným systémem splňující požadavky JIP ..... 61
13.1 Časový harmonogram projektu JIP ..... 62
14 Komparace odbavení incidentu před implementací a po implementaci ..... 63
14.1 Definice modelového incidentu ..... 63
14.2 Komparace odbavení před a po nasazení SW systému ..... 64
14.3 Vyhodnocení ..... 65
14.3.1 Vyhlášení požáru ..... 65
14.3.2 Vyhodnocení situace ..... 66
14.3.3 Práce na místě zásahu ..... 67
14.3.4 Po zásahové práce ..... 67
15 Diskuze ..... 69
16 Závěr ..... 71

17 Seznam použité literatury ..... 72

18 Seznam použitých obrázků ..... 76

19 Seznam tabulek ..... 77

# Použité zkratky

CCTV – Closed Circuit Television

DPP – Dopravní podnik hl. m. Prahy

DB – Databáze

EKV – Elektronická kontrola vstupu

EPS – Elektronická požární signalizace

HW – Hardware

HZS – Hasičský záchranný sbor

JIP – Jednotná implementační platforma

MZS – Mechanické zábranné systémy

NBÚ – Národní bezpečnostní úřad

PROVAS – Protichemická varovný systém

PTV – Průmyslová televize

PZTS – Poplachový zabezpečovací a tísňový systém

SRV – Server

SW – Software

# 1 Úvod

V dnešní době je stále častěji skloňováno slovo bezpečnost, a to jak z pohledu jedince, tak z pohledu státu, který je zodpovědný za vytvoření bezpečného prostředí pro své obyvatele. Aktuální situace z pohledu evropského měřítka není taková, jakou by bylo možné prohlásit za stabilní a bezpečnou pro evropské státy. Velký podíl na tom mají časté teroristické útoky, migrační krize a jiné bezpečností incidenty. Toto se samozřejmě odráží i v bezpečnostním dění České republiky. Aktuálně jsou státem investovány velké finanční prostředky na zlepšení bezpečnostní situace ve společnosti. V rámci bezpečnostní analýzy je možné jako jeden z kritických objektů v rámci bezpečnosti vyhodnotit Dopravní podnik hl. m Prahy, a to především z důvodu velkého počtu cestujících kteří jsou přepravování a jejich velká zranitelnost v případě jakéhokoli útoku či nehody.

Zlepšení bezpečnostní situace lze docílit jednak prevencí vzniku bezpečnostních hrozeb ale také rychlou reakcí na již vzniklé bezpečnostní hrozby a následnou její eliminací. K těmto účelům je využívána kombinace elektronických bezpečnostních systémů, mechanických zabezpečovacích systémů a v neposlední řadě lidské síly. Problémem je ale tyto tří elementy správně koordinovat a řídit. Jedna z možností, která si získává stále větší oblibu jsou softwarové nadstavbové systémy, které do sebe integrují prvky elektronické bezpečnosti, lidské síly a zohledňují mechanická bezpečnostní opatření.

Jaké konkrétní nadstavbové systémy lze využít pro implementaci v prostorách metra DPP, jaké benefity tyto systémy z pohledu bezpečnosti přináší, jaké technologie lze implementovat nebo jak složitá je jejich implementace a co je třeba při implementaci zohlednit?

Takovéto otázky jsem si kladl při zpracování této práce, která je koncipována jako případová studie nasazení jednoho z vybraných softwarových řešení v podmínkách Dopravního podniku hl. města Prahy a věřím, že přečtením této práce čtenář získá nové informace z této sféry a lepší porozumění zmíněné problematice.

# 2 Bezpečnostní nadstavbové SW

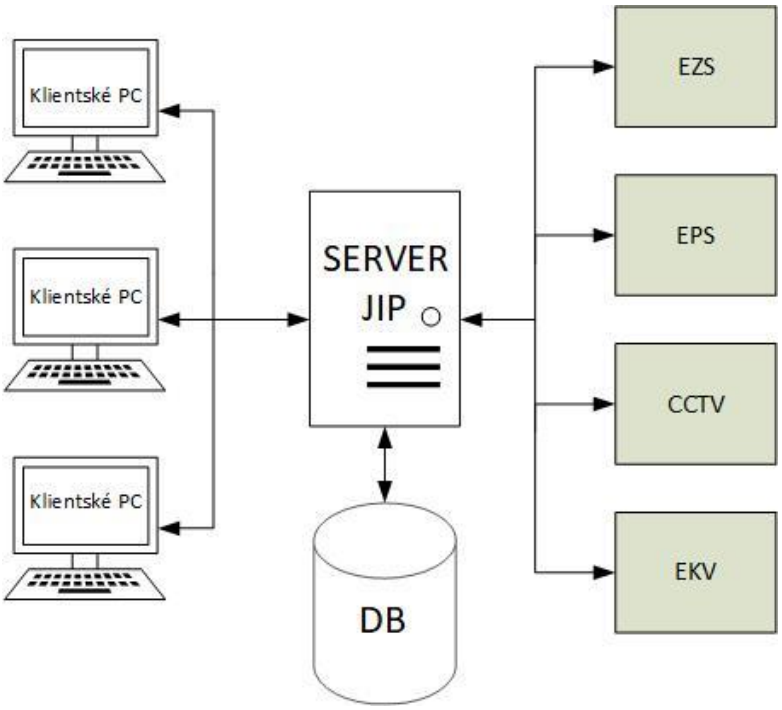
Elektronické bezpečnostní systémy jsou zejména na velkých instalacích (několik druhů různých technologií) integrovány do softwarových nadstaveb. Právě tyto nadstavby zabezpečují centralizované a uživatelsky přívětivější řešení pro správu elektronických systémů. Přínos pro uživatele je zejména v:

- centrální správě zabezpečovacích technologií,
- vizualizaci monitoring bezpečnostních systémů,
- automatizaci bezpečnostních systémů,
- analýze a vyhodnocení bezpečnostních informací,
- centrálním managementu identity,
- podpoře krizového managementu,
- snížení nákladů (zvýšení efektivity, automatizace, lepší alokaci lidských zdrojů),
- možnost připojení různých technologií mnoha výrobců,
- zvýšení bezpečnosti, snížení rizik,
- možnosti využití pro koordinaci činnosti krizových týmů,
- rychlé a efektivní identifikaci místa bezpečnostního incidentu (grafický podklad),
- snížení reakčních časů (likvidace požáru ve fázi jeho rozvoje, rychlá reakce při napadení objektu atd.).

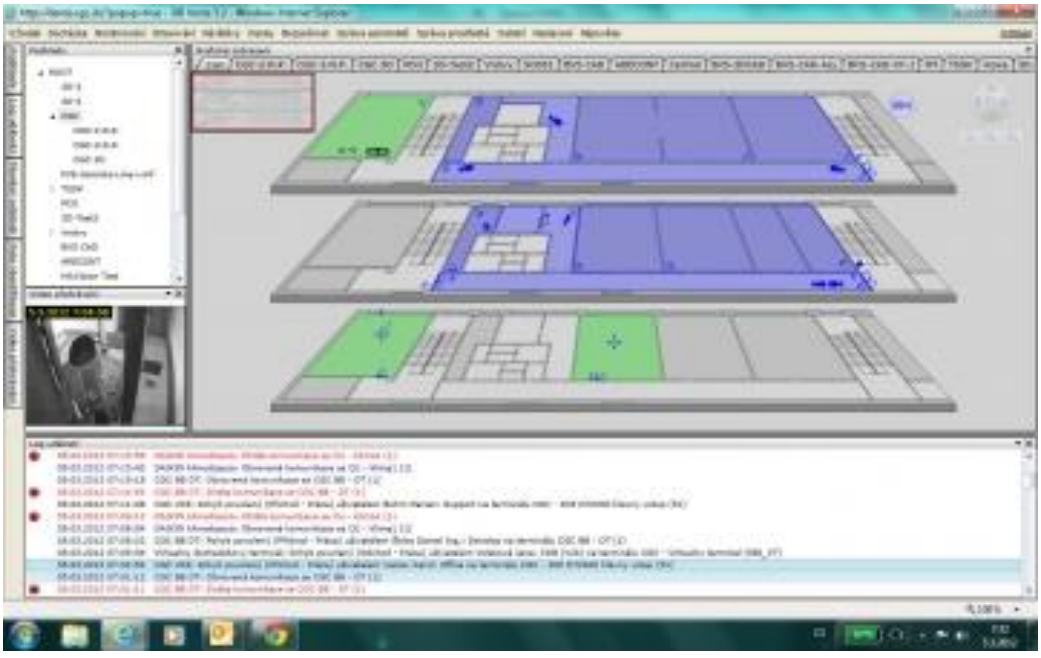
Nadstavbové systémy do sebe integrují prvky (jednotlivé bezpečnostní ústředny) bezpečnostní ochrany objektů. Dále tyto softwary musí respektovat a reflektovat základní principy, právní rámec a zásady objektové bezpečnosti. Proto, aby byl integrační SW správně navržen, je třeba, aby analytik navrhující systém spolupracoval s bezpečnostním expertem anebo sám velmi dobře znal problematiku objektové bezpečnosti. Toto je zásadní aspekt vytváření systému, který uživateli skutečně poskytne výše zmíněné benefity.

Obrázek č. 2 znázorňuje jednu z možností vizualizace stavu monitorované oblasti. Zpravidla je zobrazen strom lokace (levá horní část), mapa (střední část obrázku) která obsahuje zákresy jednotlivých čidel s vizualizací jejich stavu, zprávy

z připojených ústředen (dolní část obrázku). Dále mohou být systémy doplněny o další moduly jako je například alarm management, možnost zasílání emailů atd.




*Obrázek 1 - Schéma zapojení SW nadstavby.*



*Obrázek 2 - Vizualizace klienta pro nadstavbový systém. [18]*

# 3 Objektová bezpečnost

Objektem v objektové bezpečnosti se rozumí budova, nebo stavební prostor, který jsme se rozhodli chránit.

Objektová bezpečnost má za cíl navrhnout takový systém, kterým bude reálně zajištěna bezpečnost objektu. Aby bylo možné toto splnit, je nutné znát dvě základní veličiny: předmět ochrany a cíl ochrany. Předmět ochrany stanový, co je chráněno a cíl ochrany stanový jaká je reálná hrozba ohrožení cíle ochrany. [2]

Objektová bezpečnost je proces, který technicky a personálně zajišťuje ochranu objektu. Tento proces má zajistit, aby narušení nebo napadení chráněného objektu bylo eliminování na nejnižší možnou míru [2]

## 3.1 Způsoby zajištění ochrany z pohledu objektové bezpečnosti

Způsoby zajištění ochrany objektové bezpečnosti lze rozdělit do čtyř základních skupin. Jedná se o mechanickou ochranu, režimovou ochranu, fyzickou ostrahu objektu a technickou ostrahu. Důležitým bodem je vyhodnotit účelnost těchto čtyř základních skupin, tak aby byla ochrana maximálně efektivní.

### 3.1.1 Fyzická ostraha objektu

Tato ochrana majetku je vykonávána živou silou. Cílem je zajistit ochranu majetku a osob, bezpečnost střežených objektů a veřejný pořádek. Největší výhodou této ochrany je, že dokáže jako jediná okamžitě započít zákrok k odvrácení nebezpečí, čímž minimalizuje následné možné škody a umožňuje bezprostřední dopadení pachatele. Proto je v kombinace technické ochrany často propojována s fyzickou ostrahou, radikálně se tím zvyšuje procento efektivity. Tuto ostrahu vykonávají příslušnici bezpečnostních sborů, soukromé agentury, strážníci, nebo policie. Finančně je tento způsob ochrany nejnáročnější. Je třeba stále platit mzdy příslušníkům ostrahy, na rozdíl od řešení technické ochrany, kde je vysoká primárně prvotní investice a nadále je systém v podstatě bez nákladný. [12] [11]

Fyzická ostraha má několik možných rozdělení (hledisko výkonu, hledisko časové, hledisko způsobu zajištění, z hlediska výzbroje a výstroje) [12]

*Obrázek 3 - Strážný (Fyzická ostraha) [14]*

### 3.1.2 Technická ochrana

Technické prostředky spolu s fyzickou ochranou vytvářejí základní zabezpečení objektu. Touto kombinací dosahujeme vysoké efektivity. Technické prostředky vyplňují slabá místa fyzické ochrany a podporují režimové opatření. Technická ochrana znamená rychlé, nepřetržité střežení a monitorování objektu. Technická ochrana využívá mechanické prvky bezpečnosti a elektronické prvky bezpečnosti. [10], [11]

### 3.1.3 Mechanická ochrana

Je založena na zabezpečení objektů pomocí mechanických zábranných prostředků, které znesnadňují vniknutí do objektů. Tato ochrana je jedna z nejstarších a nejrozšířenějších metod ochrany vůbec. Jedná se o základní formu ochrany majetku. Mechanická ochrana se dlouhodobě ukazuje jako nedostatečná, pokud je instalována samostatně, proto se často používá v kombinaci s dalšími druhy ochrany. Mechanická ochrana se postupem času modernizuje a technicky

vylepšuje, stejně tak se ale i zdokonalují techniky narušitelů. Prvkem mechanické ochrany jsou například ostnatý drát na plotě, mříže, ale také mechanické zámky atd. [7]

*Obrázek 4 - Plotový perimetr (příklad kombinace mechanické a elektrické ochrany [24]*

### 3.1.4 Režimová ochrana

Jedná se o ucelený soubor opatření, pokynů, příkazů, zákazů a omezení stanovených řídícími předpisy a dokumenty vlastníka objektu. Režimové opatření stanovují řád způsobu použití bezpečnostních opatření a zajistit vazby mezi uživateli objektu, opatřeními technické ochrany a výkonem fyzické ostrahy. [8], [9]

*„V ČR není v platnosti právní předpis upravující oblast režimových opatření u jednotlivých subjektů či institucí. Povinnosti subjektu k zavedení režimových opatření však může vyplývat z právních předpisů upravující jeho podnikatelskou činnost (např. požární ochrana, jaderná energetika, prevence závažných havárií) nebo podmínek pro její výkon (ochrana utajovaných informací, krizový zákon apod.)“.* [8]

Režimová ochrana v rámci systému fyzické ochrany propojuje ostatní části (technickou ochranu, fyzickou ostrahu). Základními výstupy režimové ochrany jsou Bezpečnostní politika a Analýza bezpečnostních hrozeb a rizik. [8][9]

## 3.2 Legislativa v objektové bezpečnosti

Protože se objektová bezpečnost týká mnoha dalších odvětví, upravuje jí hned několik právních předpisů. V současné době neexistuje jeden zastřešující právní předpis pro objektovou bezpečnost. Jednotlivé právní předpisy, které ve svém znění upravují, nebo se dotýkají problematiky objektové bezpečnosti jsou zmíněny níže.

### 3.2.1 Vyhláška NBÚ o objektové bezpečnosti č. 258/1998 Sb.

Předmět úpravy:

§1 *„Zajištěním objektové bezpečnosti se rozumí systém opatření, kterým se určují podmínky, prostředky a způsoby zabezpečení ochrany objektů před seznámením se nepovolané osoby s utajovanou skutečností, a stanovení opatření směřující k zajištění ochrany utajované skutečnosti při ohrožení objektu.“ [3]*

§2 *„Cílem provádění objektové bezpečnosti je zabránit proniknutí nepovolané osoby do objektu, zjišťovat proniknutí nepovolané osoby do objektu, činit opatření k minimalizaci následků proniknutí nepovolané osoby do objektu a předcházet úniku, ztrátě, znehodnocení nebo zničení utajované skutečnosti v důsledku vzniku mimořádné události.“ [3]*

Kategorie objektu:

§4 *“Ochrana objektu se zabezpečuje pomocí bezpečnostních opatření, kterými jsou:*

*a) fyzická ostraha objektu,*
*b) mechanické zábranné prostředky,*
*c) technické zabezpečovací prostředky,*
*d) režimová opatření,*
*e) vzájemná kombinace opatření uvedených pod písmeny a), b), c) a d).*

*Rozsah, způsob a podmínky použití bezpečnostních opatření určuje statutární orgán provozovatele objektu.“ [3]*

### 3.2.2 Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti č. 412/2015 Sb.

*„Ochrana utajovaných informací je poměrně specifickou oblastí ochrany informací a v současnosti je vymezena a upravena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.“* [6]

Problematika zákonu o utajovaných informacích je natolik složitá, že i když je popsána zákonu a dalších právních předpisech, vyžaduje značnou dávku praktické zkušenosti a vyžaduje specifické znalosti z dané oblasti. Obtížné se stává pochopení rozdílnosti bezpečnostních opatření v důsledku klasifikace utajovaných informací na stupně utajení Vyhrazené, Důvěrné, Tajné a Přísně tajné, ale i rozdílná struktura stanovené bezpečnostní dokumentace pro fyzické osoby, podnikatele a orgány státu. [6]

Předmět úpravy:

§1 *„Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.“* [4]

# 4 Objektové zabezpečení z technologického hlediska

Z předešlých kapitol vyplývá, že se jedná o soubor systémů, prvků a komponent, které vytvářejí nepřetržité podmínky pro střežení objektů. V této kapitole blíže popíši jednotlivé systémy spadající do „rodiny“ technického zabezpečení.

## 4.1 Mechanické zábranné systémy

Za mechanické zábranné systémy se označují veškeré prostředky, určené k ochraně proti násilnému vniknutí neoprávněných osob. Jsou to historicky nejstarší technickými zabezpečovacími prostředky. Hlavním úkolem MZS je narušitele, co nejvíce zdržet při jejich překonávání. Všechny MZS jsou v konečném čase překonatelné. Doba na její překonání ovšem řadu pachatelů odradí, jelikož je pro ně velké riziko, že si jich po dobu překonávání někdo všimne nebo že na místo stihne přijet přivolaná hlídka. Doba překonání závisí především na jejich kvalitě a umístění. Do skupiny mechanického zabezpečení můžeme zařadit například bezpečnostní oplocení, dveře, mříže nebo trezorové skříně. [13]

*„Při návrhu MZS je výchozím podkladem pro výběr vhodných prvků bezpečnostní posouzení zabezpečovaného objektu. S ním úzce souvisí analýza potencionálních hrozeb v dané lokalitě a jejich pravděpodobnosti výskytu (míry rizika). S ohledem na identifikaci a ohodnocení chráněných aktiv v zabezpečovaném objektu se poté volí jednotlivé prvky MZS v odpovídajícím provedení a třídě bezpečnosti.“* [14]

MZS můžeme podle typu chráněných aktiv rozdělit následovně:

- obvodovou,
- plášťovou,
- předmětnou.

### 4.1.1 Obvodové prvky

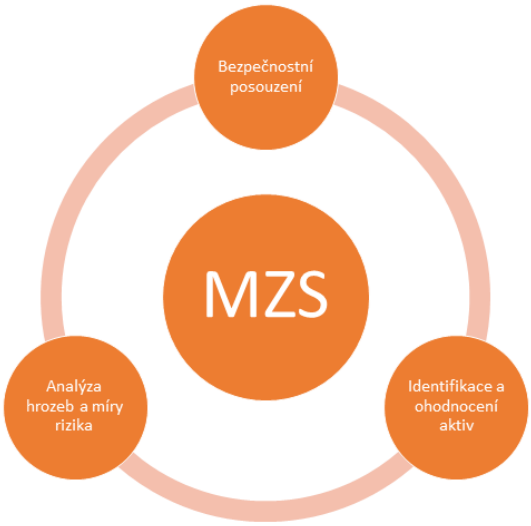
Tyto prvky jsou instalovány vně chráněného objektu. Hlavním úkolem je zajištění bezpečnosti ve vyhrazeném prostoru. Prostor je obvykle vymezen katastrálními hranicemi pozemku, většinou tvořenými přírodními nebo umělými překážkami. Jedná se tedy o oplocení či ohrazení pozemku včetně průchodů a průjezdů jako jsou branky, brány, závory apod. [14]

### 4.1.2 Plášťové prvky

V případě plášťové ochrany hovoříme o zabezpečení vnější části chráněného objektu tedy veškerých standardních i nestandardních stavebních otvorů, jako jsou dveře, okna, zásobovací otvory a šachty apod. Typickým příkladem jsou bezpečnostní dveře, skla, fólie, rolety, mříže, kování, pomocné zámkové a zamykací systémy aj. [14][13]

### 4.1.3 Předmětové prvky

Primárním určením je zabezpečení cenných předmětů či utajovaných informací před odcizením, znehodnocením nebo neoprávněné manipulaci. Obecně se jedná o pokladny, trezory, trezorové a bezpečnostní skříně, bezpečnostní zavazadla pro přepravu cenin a hotovosti, bezpečnostní plomby apod. [14]




*Obrázek 5 - MZS diagram [14]*

## 4.2 Elektronické systémy

Elektronické a elektrické zabezpečovací systémy nahrazují, nebo doplňují fyzickou ostrahu. Zajištění objektů je v tomto případě zajištěno elektrickými prvky. Úlohou těchto prvků je monitorování, informování a dokumentování. Primární výhodou je možnost online náhledu stavu zabezpečeného objektu, druhotnou výhodou je, že na pachatele působí i z psychologického hlediska. Pachatele může odradit od možného působení škody už to, že vidí v objektu zabezpečovací čidla nebo kamery. Typickými elektronickými prvky jsou elektronická zabezpečovací signalizace, elektrická požární signalizace, kamerové systémy, elektronická kontrola vstupu. [7], [10]

### 4.2.1 Elektrická zabezpečovací signalizace

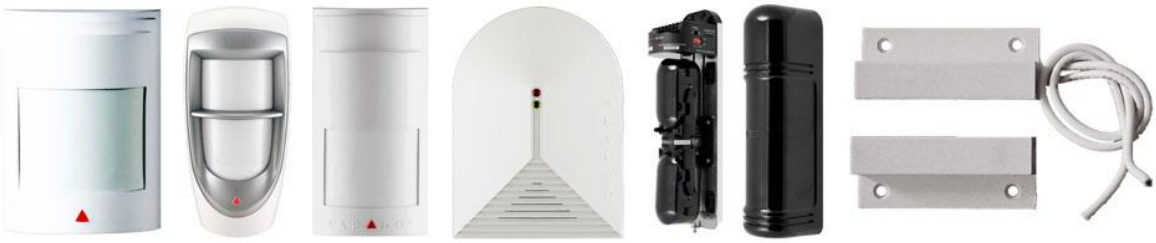
*„EZS, neboli elektronické zabezpečovací systémy slouží k signalizaci nebezpečí ve střeženém objektu.“* [17] Tyto systémy zejména informují o vniknutí do střeženého objektu. Mohou však být a velmi často jsou kombinovány i se systémy indikujícími jiné nebezpečí (požární nebezpečí, únik plynu, zaplavení atd.). Podrobné údaje jsou uvedeny v ČSN EN 50131-1 a ČSN CLC/TS 50131-7. [17], [19]

Systém EZS je v principu složen ze dvou hlavních komponent. Prvním je koncové čidlo, které je nainstalováno v dané místnosti, nebo prostoru a reaguje na změny ve svém okolí. Ve chvíli, kdy čidlo sepne (např. detekuje pohyb) zašle informaci druhé komponentě. Druhou komponentou je řídící ústředna, která informaci přijme a dle přednastavených parametrů signál vyhodnotí. Výsledkem může být například vyhlášení poplachu a zápis zprávy do databáze nebo pouze zápis do databáze bez vyhlášení poplachu. [17], [20]

Rozdělení detektorů:

- Pasivní detektory – Nevyužívají pro svou funkci elektrickou energii. Jsou vhodné pro vnější i vnitřní využití. Pasivní detektory představují především magnetické spínače, destrukční detektory, zajišťovací kontaktní prvky. Tyto detektory slouží především pro zabezpečení dveří, vrat atd. [2], [7]

- Aktivní detektory – Tyto detektory již využívají napájení elektrickým proudem proto, aby mohli plnit svou funkci. Aktivní detektory vysílají vlnění, které se odráží od okolních předmětů, a to je detektorem následně přijímáno a vyhodnoceno. Pokud je vlnění konstantní, jedná se o odraz od nehybných předmětů. Pokud se v prostředí nalézá pohyblivý předmět, dochází ke změně vlnění. Aktivní detektory se dále dělí na klasické a duální. [2] [7]



*Obrázek 6 - Ukázka detektorů EZS [21]*

### 4.2.2 Elektronická požární signalizace

*„Elektrická požární signalizace zajišťuje včasnou a rychlou identifikaci a lokalizaci vzniku požáru již v počínajícím stádiu hoření. Nasazením systému EPS je tak možné zabránit vzniku velkých materiálových ztrát a v horších případech i ztrátě lidských životů.“* [22]

EPS zajišťuje včasné zjištění vznikajícího požáru a aktivuje návazné zařízení, které se spolupodílí na protipožárních opatřeních. Je to důležitá součást protipožární ochrany objektů. Instalace EPS se stává nepsaným standardem vybavení budov a v mnohých případech povinností pro dodržení platných závazných předpisů a norem. [22]

Systém EPS tvoří vyhodnocovací ústředna, různé typy hlásičů a koncová a popřípadě ovládaní zařízení. Uživatel je akusticky a opticky informován o vzniku požáru. Informace je předána buď přímo v objektu nebo na stanoviště pultu centrální ochrany, který je umístěn u hasičského záchranného sboru. Detekci vzniku požáru zajišťují detektory založené na různých principech. Je žádoucí, aby EPS nejen signalizovala vznik požáru, ale aby také dávala signál zařízení zabraňujícímu

rozšíření požáru - např. protipožární větrací zařízení, stabilní hasící zařízení, požární uzávěry otvorů, zejména dveře a vrata, přetlakové ventilátory apod. [10], [11], [22]

### Základní rozdělení EPS:

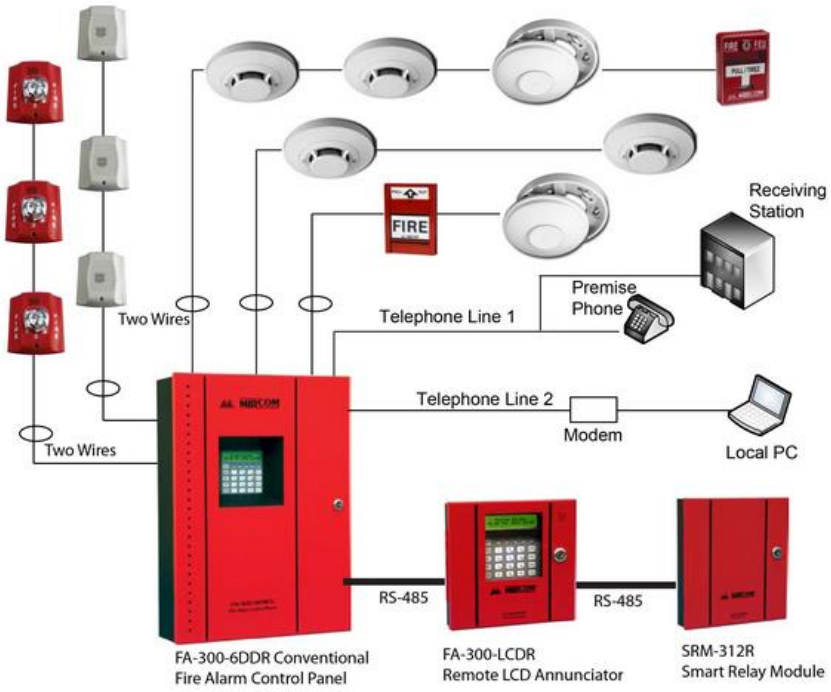
- Konvenční – na smyčku lze připojit více hlásičů, nevýhodou je, že pokud je v poplachu jedno čidlo ze smyčky, ústředna hlásí poplach na smyčce, ale nevíme, na kterém konkrétním čidle.
- Adresovatelné – o uvedení do poplachu rozhodne konkrétní hlásič. Do ústředny přijde poplach z konkrétní adresy čidla a ústředna tedy ví, který hlásič byl uvedený do poplachu.
- Analogové – tyto hlásiče mají adresu a provádějí měření fyzikálních veličin. O vyhlášení poplachového stavu rozhoduje ústředna na základě své vnitřní logiky. [10], [11], [22]

### Hlásiče požáru:

- Tlačítkové hlásiče – reagují na promáčknutí ochranného skla a stlačení spínače. Využívají se tam, kde je stálá přítomnost lidí nebo do únikových prostor.
- Samočinné hlásiče – na základě vyhodnocení změn sledovaných fyzikálních veličin se uvádějí do poplachového stavu. Hlásiče reagují buďto na přítomnost teploty nebo kouře.
- Ionizační hlásič kouře – snímací část hlásiče se skládá ze dvou komor – otevřené vnější komory a vnitřní polouzavřené referenční komory. V referenční komoře se nachází fólie s malým množstvím radioaktivního Americia 241. Po připojení napájení k hlásiči protéká touto fólií elektrický proud. Jakmile do hlásiče vnikne kouř dojde ke snížení proudu ve vnější komoře a následkem toho vzroste napětí mezi vnější a vnitřní komorou. Toto napětí je elektronicky monitorováno a po překročení určité statické hodnoty se hlásič přepne do poplachového módu. Z ekologických důvodů se v Evropě od instalací těchto hlásičů upouští.
- Optický hlásič kouře – využívá ke své činnosti pulzující LED umístěnou uvnitř hlásiče. LED je umístěna v komoře, do které nemůže vniknout světlo z žádného

externího zdroje, ale je umožněn bezproblémový přístup kouře. Částice kouře způsobí rozptyl světla emitovaného LED a tuto změnu zaregistruje fotodioda. Hlásič se následně přepne do poplachového módu.

- Hlásiče teplot – využívají termistory. Pokud začne v blízkosti hlásiče rychle vzrůstat teplota, vnější termistor tuto změnu zaznamená. Vnitřní termistor zaregistruje tuto změnu s určitým zpožděním. Pokud nerovnováha mezi termistory překročí určitou mez, dojde k vyhlášení poplachu. V případě, že teplota vzrůstá pomaleji, zareaguje hlásič na překročení stanovené teploty. Tímto vhodným uspořádáním zajišťuje hlásič včasnější zahlášení poplachu. [10], [11], [22]




*Obrázek 7 - Schéma zapojení EZS. [23]*

### 4.2.3 Kamerový systém

Kamerové systémy jsou stále používanější systémy pro zabezpečení objektů. CCTV neboli Closed Circuit Television (překlad: uzavřené televizní okruhy) se stávají nedílnou součástí bezpečnostních instalací středně velkých a velkých objektů. CCTV umožňuje střežení rozsáhlého okolí z jednoho či více míst najednou, a to obsluhou dozorující monitory v jednom místě. Účelem instalace je identifikace osob,

monitoring jejich pohybu, odhalování a prevence kriminality a dohlížení na bezpečnost práce a technologické procesy. Nahrávané časové úseky jsou ukládány v databázi, ze které je možné je zpětně přehrávat a analyzovat zaznamenanou situaci. Dříve používané analogové kamery jsou pomalu vytlačovány digitálními IP kamerami, které poskytují násobně vyšší rozlišovací schopnost a přináší i další výhody. [2]

Při výběru kamer pro konkrétní instalaci je nutné zohlednit místní podmínky a kameru posoudit dle parametrů, tak aby na co nejvíce vyhovovala místu instalace. Hlavními parametry při posouzení jsou:

- rozlišovací schopnost,
- citlivost,
- snímání,
- přenos obrazu,
- přísvit,
- druh snímaného čipu. [2]

### Záznamové zařízení

Záznamové zařízení u systému CCTV se obvykle označuje zkratkou DVR (Digital Video Recorder). Výrobci systémy DVR vyrábějí v určitých řadách, které jsou dány počtem připojených kamer. Existují systémy pro připojení 2, 4, 8 a 16, 24 kamer. Dle počtu kamer a také kvality a doby nahrávání volíme velikost uložiště. Systém DVR má většinou výstupy na připojení monitoru anebo pro streamování do sítě LAN. Pomocí monitoru můžeme nahlížet přímo na jednotlivé kamery nebo přehrávat záznam. [29]

### Rozdělení kamer

Samotné kamery můžeme rozdělit do několika skupin bez ohledu na použitou technologii. Hlavním kritériem rozdělení je, zda se bude kamera používat ve vnitřních či venkovních prostorách. Základní typy kamer:

- deskové kamery,
- kompaktní kamery,
- kompaktní venkovní kamery,
- DOME kamery (statické, pohybové, vnitřní a vnější). [29]


*Obrázek 8 - Sestava kamer včetně DVR. [30]*

### 4.2.4 Elektronická kontrola vstupu

EKV je v základu tvořeno čtečkou, elektrickým zámkem a řídící jednotkou. Řídící jednotka vyhodnocuje a zaznamenává veškeré události v systému. Výstupní informace se přenášejí do PC. Systém kontroly vstupu (EKV) provádí identifikaci a výběr osob pro příchod/odchod do definovaných prostor. [25], [26]

Nejběžnějším prostředkem identifikace, používaným v přístupových systémech je personální karta, kterou se osoby registrují u čteček. Čtecí zařízení přečte informaci obsaženou na kartě, předá ji řídící jednotce a ta podle systému přístupových práv rozhodne o vpuštění osoby do střeženého prostoru. Aktuálně jsou populární instalace tzv. biometrických čteček, které dokážou identifikovat osoby podle otisku prstu nebo očního pozadí. Vzájemnou kombinací těchto identifikačních faktorů lze zvýšit stupeň zabezpečení kontroly vstupu. [25], [26]

Chod systému zajišťuje řídící jednotka, ve které je udržována databáze uživatelů, jejich práva vstupu do jednotlivých oblastí objektu, která mohou být definována nejen místně ale i časově. Všechny vstupy nebo i jen pokusy o vstup jsou s příslušnými časovými údaji uloženy a mohou být využity pro pozdější analýzu. Přístupové systémy bývá možné připojit k internetu a z libovolného počítače nastavit povolení vstupu do objektu. [25] [26]

### Základní technické požadavky:

Výrobky elektrické kontroly vstupu jsou řešeny harmonizovanými evropskými normami ČSN EN řady 50 133, popřípadě i Národním bezpečnostním úřadem dle Zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti a vyhlášky NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. [4], [27], [28]


*Obrázek 9 - přístupové čtečky s klávesnicí a ústřednou [25]*

# 5 Bezpečnostní rizika – pojem, ocenění a projekty ostrahy

*„Bezpečnostní riziko je situace ve střeženém objektu, v jehož důsledku může vzniknout krizová situace, a to v příčinné souvislosti mezi jednáním a následkem.“* [2]

Bezpečnostní riziko je možné rozdělit na:

- bezprostřední (okamžitě viditelné),
- následné (které mohou přivodit značné škody),
- latentní (skryté).

Správné stanovení bezpečnostního rizika je jednou z klíčových rolí řídících pracovníků SBS při organizování objektové bezpečnosti. Každý objekt sebou nese odlišnou množinu možných rizik. Základem pro stanovení a ocenění bezpečnostních rizik je analýza vstupních informací o chráněném objektu. Získání kvalifikovaných podkladů pro provedení správné analýzy ke stanovení bezpečnostních rizik je jedním z nejobtížnějších úkolů analýzy. Získání těchto informací je závislé na zkušenostech bezpečnostního managementu. Získání relevantních informací je složité i proto, že osoby zodpovědné za objekt (majitelé, ředitelé apod.) neuvádějí podstatné informace (například že budova byla již několikrát vykradena, nebo že v objektu pracují osoby se zápisem v rejstříku trestů apod.). Z tohoto důvodu by měl bezpečností manager využít všechny možné dostupné možnosti pro zjištění, co možná největšího počtu informací o objektu, jedině pak lze zhotovit kvalitní analýzu rizik. [2]

## 5.1 Bezpečnostní analýza

Bezpečnostní analýza obsahuje souhrn bezpečnostních poznatků ovlivňující střežení objektu. Bezpečnostní analýza vyhledává a zkoumá vnitřní zranitelnosti, vnější hrozby a implementované a plánované ochranné mechanizmy, které mají vliv na předmětný objekt ve zvolených vrstvách bezpečnosti: technologické (počítačové a komunikační), fyzické, personální a administrativní (organizační).

*„Cíle bezpečnostní analýzy jsou identifikovat maximum zranitelností obsažených ve zkoumaném objektu, odhadnout hrozby, rizika a možné negativní dopady na zkoumaný objekt, určit efektivitu a funkčnost stávajících ochranných mechanizmů a navrhnout nové tak, aby byla všechna rizika efektivně snížena nebo pokryta na akceptovatelnou úroveň.“* [5]

## 5.2 Ocenění rizika

Oceněné riziko je zpravidla určeno slovní definicí: malé, střední, vyšší a podobně. Postup ocenění rizika:

a) Vyhledat zdroj rizika a její identifikace

Zde je vhodné využít statistické analýzy krizových situací (počty vloupání, počet incidentů bezpečnostního charakteru atd.). V položkách identifikace hrozeb bude následně uveden výčet pravděpodobných druhů událostí ohrožující objekt. Do položek celkové škody se zahrnou přímé ztráty jako například obnova, následná škoda, nemožnost podnikat. [2]

b) Stanovení dílčích pojmů a metod rizikové analýzy

Podmínkou pro kvalitní analýzu je poznání všech veličin rizika v objektu.

- ČAS – průniková analýza
- PRAVDĚPODOBNOST – analýza druhů rizik
- NÁSLEDEK PŘÍMÝ – kvalitativní analýzy propočtů
- NÁSLEDEK NEPŘÍMÝ – analýza souvztažností
- SPOLEHLIVOST LIDSKÝCH ZDROJŮ – analýza osobnostních psychotestů. [2]

$$Riziko = pravděpodonost \times následek \ (R = P \times N)$$

c) Komplexní analýzy souvztažností rizik

Jedná se seriózní ocenění jednotlivých hrozeb rizik a krizových situací, z hlediska časové posloupnosti, z pohledu pravděpodobnosti a z hlediska možných vzájemných vazeb. [2]

# 6 Dopravní podnik hl. m. Prahy

Dopravní podnik hl. m. Prahy je hlavním provozovatelem veřejné dopravy v hlavním městě ČR. V jeho působnosti je provoz metra, tramvají, autobusů a zároveň je provozovatelem městských drah na níž tuto dopravu provozuje. [31], [32]

*Tabulka 1 - Provozně technické ukazatele [33]*

| ukazatel | metro | tramvaje | autobusy | celkem |
|---|---|---|---|---|
| počet linek [1.] | 3 | 33 | 142 | 178 |
| délka linek [1.] | 65,4 | 547,4 | 1 695,3 | 2 308,1 |
| průměrná cestovní rychlost (km/h) | 35,65 | 18,77 | 25,31 | 26,58 |
| dopravní výkony (v tis. vozkm) | 57 529 | 54 578 | 60 327 | 172 434 |
| počet přepravených osob (v tis.) | 461 160 | 368 609 | 356 967 | 1 186 736 |

Z tabulky vyplívá, že v Pražském metru je přepravováno více jak 1 milion cestujících ročně, z toho přepraví metro téměř půl milionu cestujících. Takto vysoký počet cestujících klade vysoké nároky na bezpečnost.


*Obrázek 10 - Logo DPP [33]*

## 6.1 Historie

Historie vzniku DPP sahá do roku 1890, kdy ale ještě provoz veřejné dopravy zajišťovali soukromí dopravci. V počátcích byl DPP odvozován od pražské radniční komise, která vznikla k posouzení návrhu vzniku parní tramvaje propojující jednotlivé části města. K dohodě sice nedošlo, ale komise byla provozována i nadále pod názvem Komise pro elektrické dráhy. Dne 27. června 1897 odkoupila Praha

dosud soukromou síť pražské koňky, následně byl do pražského podniku sloučen vinohradský podnik Městská elektrická dráha Královských Vinohrad. V roce 1900 pak podnik odkoupil Hlaváčkovu dráhu do Košíř a v roce 1907 Křižíkovu dráhu do Vysočan, čímž byl proces komunalizace a monopolizace pražské veřejné hromadné dopravy završen. Název Dopravní podnik hl. m. Prahy byl ustanoven 6. září 1946. Dopravní podnik za dobu své existence začleňoval mimo nynější provoz také provoz taxislužeb, lodní dopravy, půjčovnu automobilů, v průběhu let byly tyto činnosti opět vyčleněny. [31], [32]

Podnik má od roku 1991 formu akciové společnosti. Jedinou akcii v hodnotě přibližně 32 miliard Kč vlastnilo hlavní město Praha. V roce 1995 byla tato akcie rozdělena na 3001 ks akcií, jejichž vlastníkem bylo stále hl. město Praha. [31], [32]

Od roku 1999 používá DPP nové logo. Je jím bílý nebo červený kruh symbolizující autobusy, s dvěma přes něj probíhajícími zakřivenými liniemi, které symbolizují tramvaje, svislá linie pak představuje metro. Logo se používá se jak na autobusech, tak i tramvajích či v metru. V devadesátých letech každý odštěpný závod ale používal své vlastní logo; metro trojúhelník s písmenem M, tramvaje stylizovanou Prašnou bránu (podobné logo bylo do 80. let užíváno pro celý DP) a autobusy stylizované písmeno A. [31], [32]

# 7 Požadovaný přínos projektu JIP

Cílem projektu JIP v DPP je sloučení klíčových bezpečnostních a některých podpůrných technologických systémů v oblasti metra do Jednotné Integrační Platformy a doplnění nezbytné infrastruktury pro integrování technologií a vybudování nových pracovišť pro práci s Jednotnou integrační platformou. [1]

Integrací je myšleno spojení jednotlivých bezpečnostních a podpůrných technologií ve vyšší celek. Jednoúčelové technologie propojit mezi sebou a uživateli zprostředkovat komplexní pohled na bezpečnostní technologie v prostředí DPP. Integrované technologie lze samostatně chápat jako jednoúčelové vstupy, kdy komplexní pohled uživatele skrz vazby v systému zajistí daleko lepší možnosti vyhodnocení mimořádných situací v DPP, což se bude přímo podílet na zvýšení bezpečnosti v prostředí DPP. [1]

Očekávaný přínosem projektu je snížení reakčního času na mimořádnou událost ve sledovaném prostoru a tím snížení rizika vzniku škody při nastalé mimořádné události. Systém bude dále také ukládat veškeré informace týkající se události (jak uživatelské úkony, tak zprávy z technologií) a tím bude umožněno následně průběh řešení analyzovat a navrhovat například vhodnější postupy při řešení událostí. Dalším z přínosů bude odlehčení zatíženosti lidských zdrojů v oblasti fyzické ochrany, které bude možné alokovat na lokality, kde bude jejich využití efektivnější.

# Praktická část

# 8 Popis současného stavu implementace technologií v metru

V současné době je v Pražském metru implementován nadstavbový systém MrGuard3. Do tohoto systému ale nejsou implementovány všechny úseky metra a systém není využíván všemi složkami podílejícími se na bezpečnosti v Pražském metru a nejsou v něm implementovány potřebné technologie využívané pro bezpečnostní dohled (například kamerové systémy). Stávající systém například neřeší nově vystavěný úsek na trase A – Bořislavka – Nemocnice Motol.

## 8.1 Informace o plánovaném rozsahu integrace

V následujících dvou podkapitolách jsou uvedeny konkrétní typy technologií, které jsou plánovány integrovat do systému JIP s jejich stručným popisem. Dále je definováno území, kterého se integrace do JIP týká, zejména se jedná o jednotlivé stanice metra a depa.

### 8.1.1 Integrované technologie

Níže jsou jednotlivé integrované technologie uvedeny a popsány s ohledem na využití pouze těch informací, které nejsou v tomto projektu chápány jako důvěrné, vyhrazené, nebo tajné. V rámci projektu JIP budou integrovány technologie, které jsou chápány jako klíčové:

- EPS,
- PZTS,
- EKV,
- PTV,
- PROVAS.

#### Technologie EPS

V rámci Elektrické požární signalizace bude integrováno celkem 156 systémů postavených na technologické platformě Schrack a Esser. Pro účely dohledu v metru budou využity primárně kombinované hlásiče, teplotní hlásiče, manuální hlásiče,

optické hlásiče. Ke zmíněnému počtu 156 ústředen bude celkem připojeno 13 241ks hlásičů.

#### Technologie PZTS

V rámci Elektrické zabezpečovací signalizace bude integrováno celkem 56 stávajících systémů a 37 systémů v přípravě v předprodejních místech postavených na technologické platformě Galaxy. K ústřednám bude připojeno celkem 2 730ks čidel, která budou zejména typově zastoupena magnetickými kontakty, pohybovými detektory a detektory tříštění skla.

#### Technologie EKV

V rámci Elektronické kontroly vstupů bude integrováno celkem 1054 řídících jednotek, které budou postaveny na platformě systému S4.

#### Technologie PTV

V rámci PTV bude integrováno celkem 100 serverů vycházející z technologické platformy Guetebrück. K těmto serverům bude integrováno celkem 1914 kamer. Do systému budou integrovány analogové i IP kamery.

#### Technologie PROVAS

Do systému JIP bude integrována technologie PROVAS, ze které bude systém JIP přijímat datové věty, které zajistí předání informace operátorovi. Informace bude specifickým způsobem zobrazována na JIP klientech (klientských aplikacích) vlakového dispečinku a dispečinku HZS. Celá tato technologie a veškeré další informace týkající se této technologie jsou vedeny v režimu „Vyhrazené“ dle platných předpisů a vyhlášek NBÚ.

### 8.1.2 Integrované území

Do nadstavbového softwaru JIP budou integrovány všechny stanice Pražského metra, včetně stanic depa a přidružených prostor. Konkrétně se jedná o:

Integrované stanice:

- **Trasa A** – Bořislavka, Dejvice, Depo Hostivař, Flora, Hradčanská, Jiřího z Poděbrad, Malostranská, Můstek A, Muzeum A, Nádraží Veleslavín, Náměstí Míru, Nemocnice Motol, Petřiny, Skalka, Staroměstská, Strašnická, Želivského (celkem 17 stanic) [34]

- **Trasa B** – Anděl, Černý most, Českomoravská, Florenc, Hloubětín, Hůrka, Invalidovna, Jinonice, Karlovo náměstí, Kolbenova, Křižíkova, Luka, Lužiny, Můstek, Náměstí Republiky, Národní třída, Nové Butovice, Palmovka, Radlická, Rajská zahrada, Smíchovské nádraží, Stodůlky, Vysočanská, Zličín (celkem 24 stanic) [34]

- **Trasa C** – Budějovická, Florenc, Háje, Hlavní nádraží, Chodov, I. P. Pavlova, Kačerov, Kobylisy, Ládví, Letňany, Muzeum, Nádraží Holešovice, Opatov, Pankrác, Pražského povstání, Prosek, Roztyly, Střížkov, Vltavská, Vyšehrad (celkem 20 stanic) [34]

Celkem bude integrováno 61 stanic metra, kdy jsou v každé stanici zřízena tři dohledová pracoviště. Na každém dohledovém pracovišti bude instalován jeden dohledový klient SW JIP.


*Obrázek 11 - Mapa Pražského metra [34]*

Integrovaná depa

Do JIP budou integrovány také všechna depa Pražského metra. Jedná se o depo Kačerov, Zličín a Hostivař.

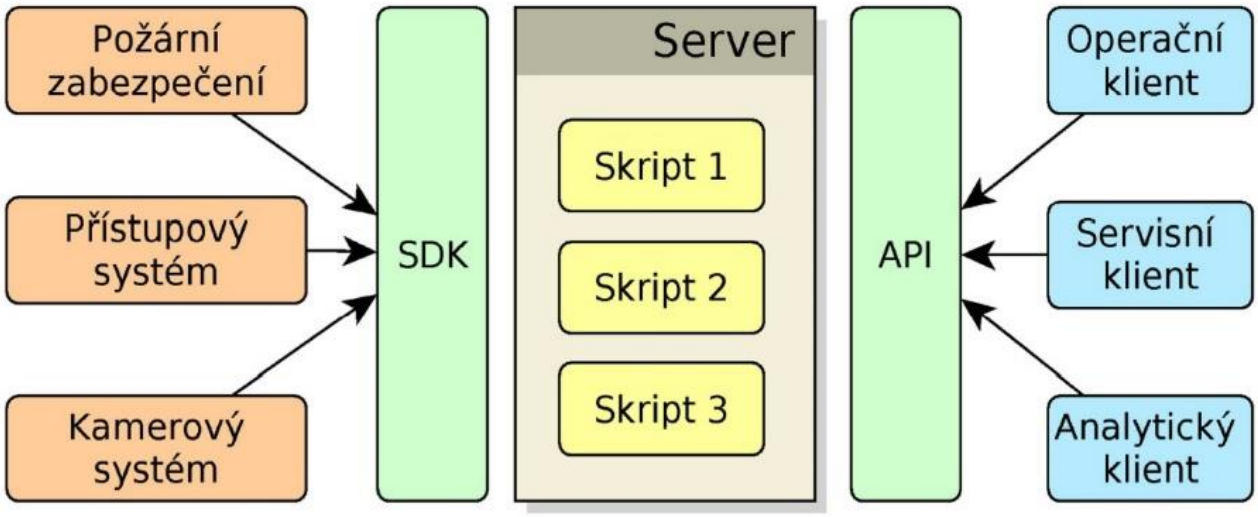
# 9 Softwarová nadstavba JIP

JIP bude softwarová nadstavba nad bezpečnostními technologiemi v Dopravním podniku hlavního města Prahy. Tato nadstavba bude vycházet z produktů dostupných na trhu. Vybraný produkt, který bude požadavkům DPP nejblíže a bude ekonomicky a technicky nevíce vyhovovat bude následně modifikován a doprogramován do stavu, kdy bude plně vyhovovat požadavkům DPP.

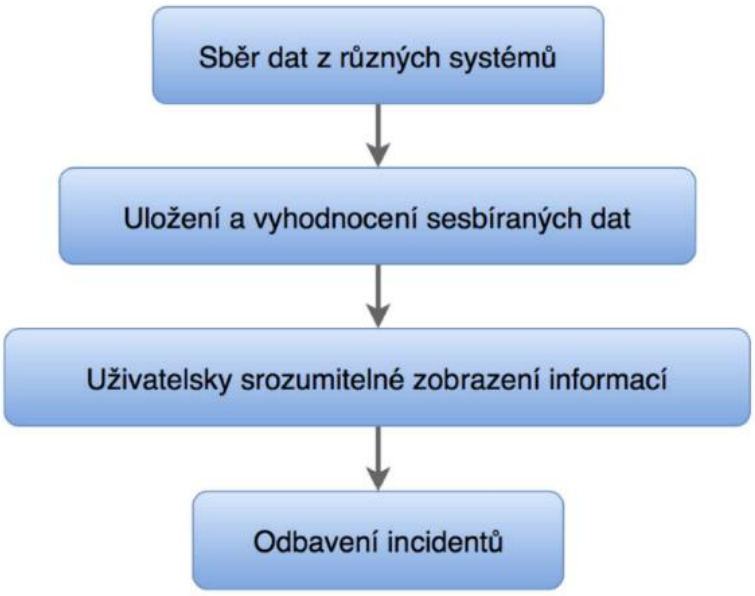
## 9.1 Stručný popis řešení JIP

Základním úkolem nadstavbového systému je sbírat, uchovávat, zpracovávat a předávat informace z integrovaných technologií uživatelům, kteří s JIP budou pracovat. Uživatel může JIP rovněž využít na základě vyhodnocení situace jako ovládací nástroj integrovaných technologií. Vazby mezi jednotlivými systémy dávají uživateli ucelenější informace, které mu pomáhají snadněji vyhodnotit mimořádné situace a zabezpečit kvalitu a bezpečnost provozu v metru. [1]

Systém je navržen v konceptu klient – server. To znamená, že data z připojených technologií se zpracovávají v aplikačním serveru, odkud jsou ukládána do databáze a dále poskytována klientům. Klientem se rozumí uživatelská aplikace instalovaná na PC.




*Obrázek 12: Schéma přístupů technologií a klientů do JIP [1]*




*Obrázek 13: Blokové schéma JIP [1]*

# 10 Popis požadavků DPP na software JIP

U zástupců DPP byly metodou řízených rozhovorů analyzovány klíčové požadavky pro fungování JIP a obecné požadavky na SW. Tyto požadavky jsou níže v této kapitole stručně popsány.

## 10.1 Klíčové požadavky

Díky svému velkému rozsahu bude systém JIP přesahovat před různé úseky DPP. Díky širokému využití velkým spektrem uživatelů je na systém JIP kladeno velké množství různorodých požadavků. Tyto požadavky je nutné zhotovitelem SW řádně analyzovat a navrhnout řešení, které bude působit jednotným dojmem a bude poskytovat maximální možnou přehlednost. Za předpokladu, že budeme vycházet z řešení MrGuard, je nutné ze strany zhotovitele provést komparaci požadavků a vlastností systému a pro rozdílové požadavky navrhnout vhodný dovývoj, tak aby byly požadavky splněny.

### 10.1.1 Vytváření bezpečnostního systému JIP

JIP má obsahovat sadu klientů, kteří umožní definovat vlastní bezpečnostní systém JIP nad zájmovými objekty pomocí vytvářených lokací v kombinaci s technologiemi a uživatelskými skupinami. Cílem je, aby každá uživatelská supina sledovala jen tu část objektů a s tím pohledem, který je vhodný k jejím pracovním potřebám.

### 10.1.2 Analýza uložených dat

Systém bude umožňovat dlouhodobě uchovávat všechna data, která budou v nastavení systému vybrána a nad těmito daty pomocí speciálního klienta vyhledávat. Hlavní požadovaná vlastnost je vyhledávání nad různými typy dat a technologiemi.

### 10.1.3 Různé typy incidentů

Systém JIP musí umožnovat uživatelsky definovat různé typy incidentů, jako například Porucha, Předpoplach, Poplach. Tyto typy incidentů přiřazovat vůči jednotlivým skupinám a zprávám z integrovaných technologií. Incident management včetně eskalace incidentů

### 10.1.4 Vazby a skripty

Vazby jsou klíčovou vlastností celého systému JIP. Umožňují právě onu inteligenci integrovaného systému. Elementárním typem vazby v systému JIP je reakce kamerového systému na definované bezpečnostní incidenty. Tedy při poplachu je automaticky zobrazen živý obraz nebo smyčka z kamerového systému na poplachovém monitoru operátora. Takovéto vazby nejenže eliminují lidskou chybu, ale výrazně zkracují dobu potřebnou pro vyhodnocení bezpečnostního incidentu.

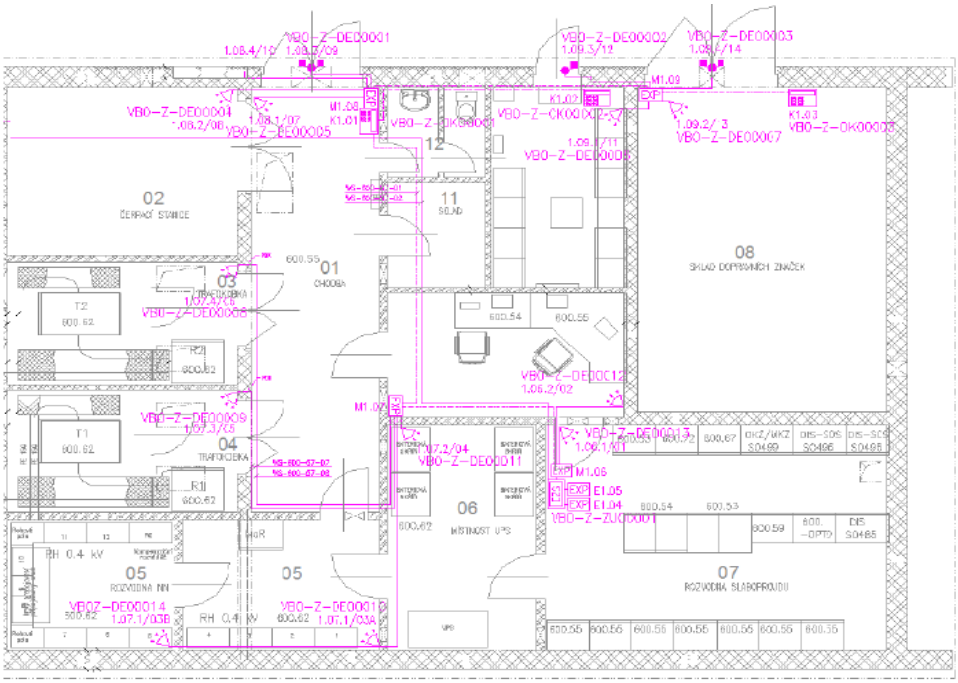
### 10.1.5 Zobrazování mapových podkladů

Protože je působnost Dopravního podniku na celém území hlavního města Prahy systém JIP bude obsahovat geografické mapy OpenStreet celé oblasti působnosti. V těchto mapách budou vyznačeny pomocí barevných zón jednotlivé zájmové lokality. Barevné zóny budou jednak umožňovat proklik do detailu zájmové lokality


*Obrázek 14 - Příklad GIS mapového podkladu. [1]*

na úroveň jednotlivých objektů a jednak pomocí barevné vizualizace bude zřejmé v jakém stavu se zájmová lokalita nachází.

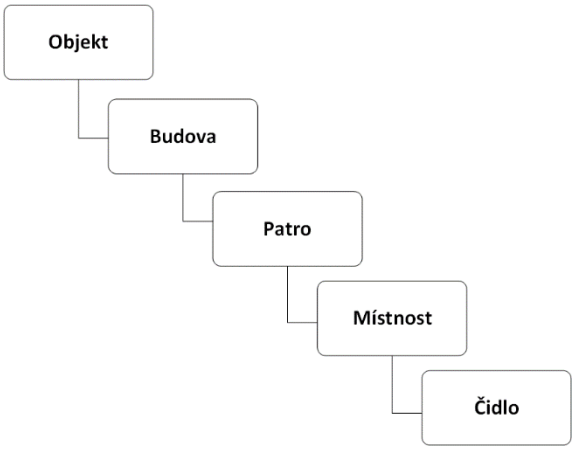
Základním zobrazením zájmového objektu jsou technické výkresy ze systému CAD, které jsou v dopravním podniku standardem. Systém JIP musí umožňovat tyto výkresy importovat. Takto vytvořené mapy budou obsahovat i ikony jednotlivých koncových prvků integrovaných technologií, které budou barevně reagovat na aktuální stav technologie. Mapy mohou, v případě, kdy je to vhodné, obsahovat i proklikávací tlačítka či zóny na další mapy zájmového objektu.




*Obrázek 15 - Příklad mapového podkladu ve formátu AutoCad. [1]*

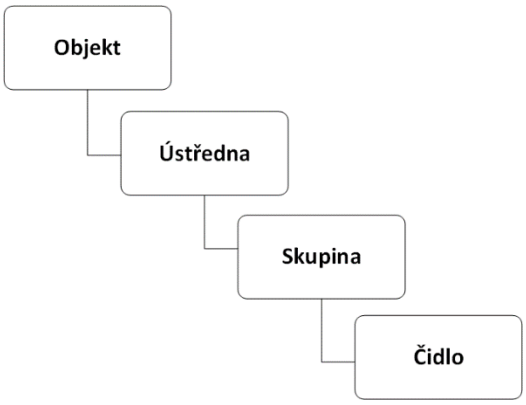
### Vytváření virtuálních lokací

Systém JIP bude umožňovat vytváření lokací. Lokace je specifický pohled na zájmový objekt. Lokace je tvořena logickým stromem s libovolnou úrovní vnoření, kde jednotlivé uzly mohou být buď virtuální uzly typu složka, nebo mohou reprezentovat koncový nebo logický prvek integrované technologie. Lokace umožňují jiný pohled na ten samý objekt. Například bezpečnostní pracovník vnímá objekt jako logický strom:




*Obrázek 16 - Schéma vnímání lokace bezpečnostním pracovníkem.*

Servisní pracovník pak ten samý objekt vnímá jako:




*Obrázek 17 - Schéma vnímání lokace servisním pracovníkem*

Systém JIP musí umožnit vytvoření neomezeného počtu lokací pro každý jednotlivý zájmový objekt. Zobrazení lokací podle přihlášeného počítače.

Notifikace o událostech

Systém JIP bude umožňovat notifikaci o událostech a incidentech v integrovaných technologiích, a to dvěma možnými způsoby:

- Interní notifikace uvnitř klientů systému
- E-mailová notifikace vně systému JIP na interní e-mailové adresy DPP

Systém notifikace bude konfigurovatelný na jednotlivé události a uživatelské skupiny.

## 10.2 Obecné požadavky

### 10.2.1 Flexibilita aplikace pro operátory

Hlavní aplikace systému JIP určená pro operátory musí umožňovat provoz na několika monitorech, a to včetně násobného zobrazení jejích jednotlivých logických částí jako je například mapová oblast, okno zpráv, incident management. Ve výsledku tak bude možné například na jednom monitoru zobrazit několik oken zpráv a v každém z nich zobrazit zprávy pro různé technologie a různé lokace. Dalším možným zobrazením je zobrazení několika map separátně pro různé lokace.

### 10.2.2 Archivace dat

Archiv dat bude integrální součástí systému JIP. Systém JIP bude pravidelně, v intervalu podle nastavení, přesouvat data z živé databáze do archivní databáze. Živá databáze tak bude udržována v rozumné velikosti a nebude postupně zpomalována narůstajícím množstvím dat. Díky tomuto kroku budou oddělena data pro každodenní provoz databáze a pro hloubkovou analýzu dat, kterou bude provádět skupina jiných typů uživatelů a jinými nástroji.

### 10.2.3 Zálohování dat

Zálohování dat systému JIP bude probíhat formou denní přírůstkové zálohy databáze. Záloha databáze bude ukládána na diskové pole určené pro primární a sekundární servery JIP. Takto uložená záloha bude díky zrcadlení primárního

a sekundárního diskového pole dostatečně chráněna proti výpadku disků, a tedy proti poškození.

Databáze systému JIP bude obsahovat nejenom data sesbíraná z integrovaných technologií, ale i všechna ostatní data jako uživatelské účty, nastavení práv skupin, definici všech lokací systému atd.

### 10.2.4 Bezpečnost systému

Přístup k veškerým funkcím systému musí být umožněn pouze oprávněným uživatelům na základě jejich přihlášení uživatelským jménem a heslem.

Administrátor systému musí mít možnost globálně pro všechny uživatele nastavit minimální sílu hesla pomocí několika kritérií. Dále musí mít administrátor možnost zapnout a nastavit časové omezení platnosti hesla (počet měsíců). Hesla musí být v systému zpracovávána a uchovávána v šifrované podobě.

Veškerá síťová komunikace mezi jednotlivými částmi systému musí být šifrovaná. Technologie použitá k šifrování musí být standardní a musí podporovat překlad síťových adres s využitím změny zdrojového portu (PAT). Preferovaným řešením je použití HTTPS protokolu.

# 11 Možné SW nadstavby pro uplatnění v projektu JIP

Z informací získaných praxí mohu potvrdit, že se na českém trhu pohybuje řada významných evropských i celosvětových hráčů, kteří mohou být vážným kandidátem pro nasazení v Dopravním podniku hlavního města Prahy. Abychom ale měli širší rozhled a bohatší možnost výběru, budu prověřovat i méně známe systémy, které by se případně mohli využít pro aplikace v DPP.

Cílem je seznámit se blíže alespoň s šesti systémy, ze kterých následně metodou multikriteriální analýzy vyberu dva nejvhodnější kandidáty, se kterými bude dále pracováno.

## 11.1 Nabídka nadstavbových systémů na trhu

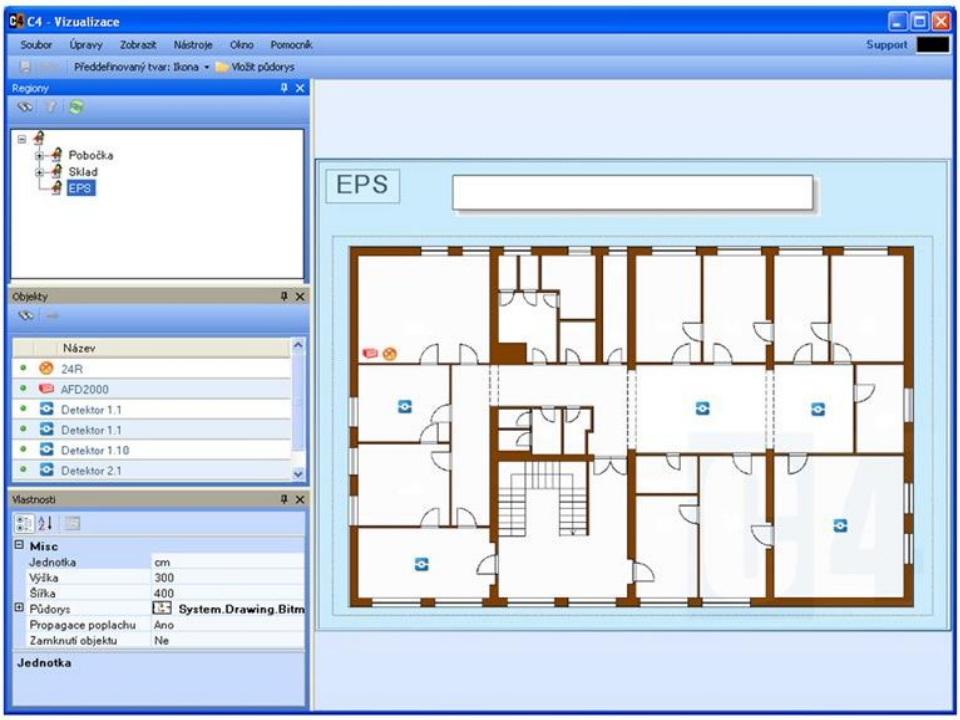
### 11.1.1 C4

Software C4 je produktem slovenské společnosti Gamanet a.s. Tato společnost je jedním z lídrů v oblasti bezpečnostních nadstaveb na českém ale i evropském trhu. V České republice je systém C4 nabízen řadou partnerských společností zabývající se oblastí bezpečnosti a elektroinstalací.

SW nadstavba C4 podporuje integraci systémů EKV, EZS, PTZ, CCTV do jednoho uživatelského rozhraní. Díky své architektuře umožňuje integraci i dalších systémů na přání zákazníka. Výhodou tohoto systému je integrace managementu budov (technologie MaR). C4 je stále vyvíjen a dynamicky vylepšován dle rekcí zákazníků. Dynamický vývoj je považováno za jednu ze zásadních výhod. Tento systém je vhodný pro nasazení v průmyslových objektech větších rozsahů, korporátních společnostech, administračních budovách ale i v dopravě nebo ho lze využít jako systém bezpečnostních agentur. [35]

S C4 mám osobní zkušenost z několika projektů, v jejíž rámci byl systém C4 instalován. Jedná se o velmi komplexní systém, který dokáže pojmout rozsahově i technologicky velké instalace. Slabinou tohoto řešení je z mého pohledu složité

uživatelské rozhraní, které bude vyhovovat spíše technikům a běžní koncový uživatelé se v něm mohou hůře orientovat.



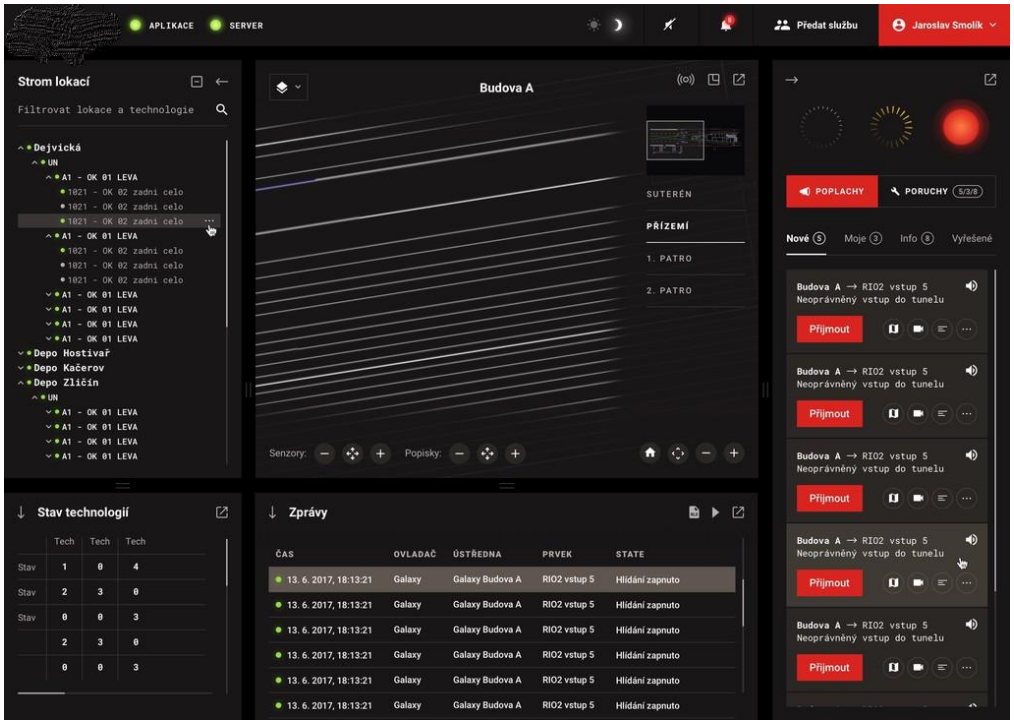

*Obrázek 18 Uživatelské pracovní prostředí C4 [35]*

### 11.1.2 MrGuard

MrGuard je produktem české společnosti Colsys s.r.o., která na trhu bezpečnostních technologií a instalací pohybuje bezmála 25 let a je jednou ze tří největších společností tohoto zaměření v České republice. Produkt MrGuard je na trhu zastoupen již pátou generací, své existence.

MrGuard je vhodný pro efektivní monitoring, ovládání a správu rozsáhlých instalací. Doménou tohoto systému je vektorové zobrazování map, detailní možnost nastavení uživatelských oprávnění a distribuovaná síťová architektura. [36]

Uživatelské rozhraní aplikace je navrženo tak, aby bylo pro uživatele intuitivní. Na rozdíl od konkurenčního systému C4 jsou u MrGuarda rozděleny jednotlivé uživatelské úlohy (dohled, administrace, implementace) do jednotlivých přehlednějších aplikací. Systém je architektonicky koncipován jako modulární. To znamená, že do systému lze doprogramovat relativně snadno nové doplňující funkce, což je jednou z výhod v případném nasazení v DPP.

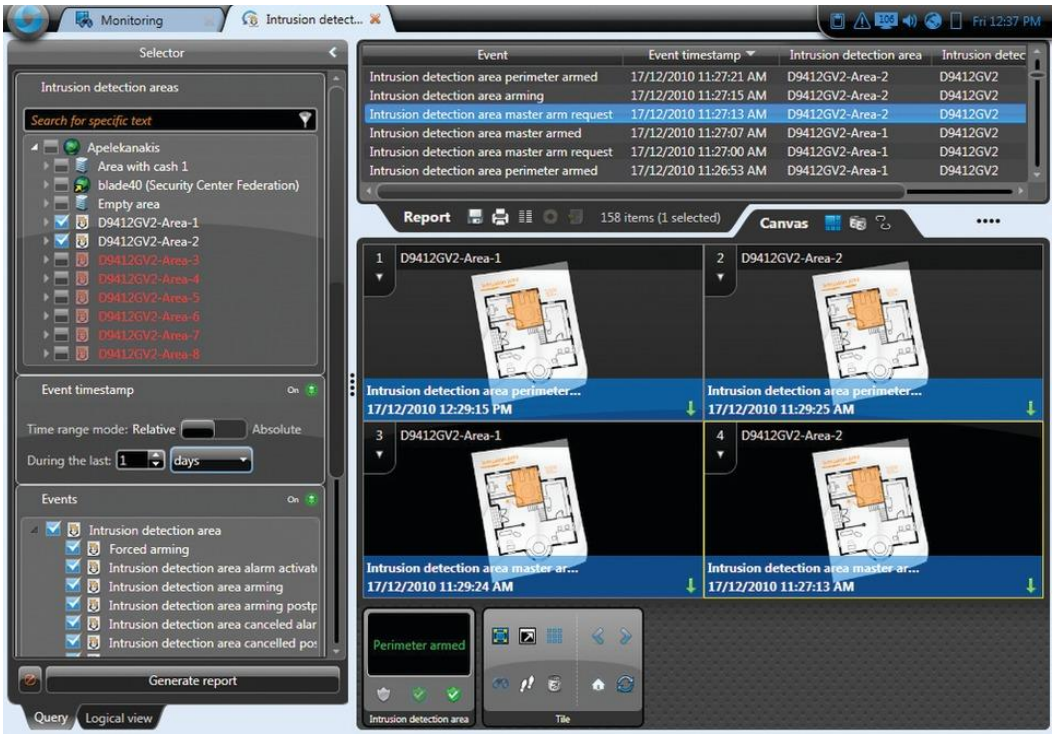



*Obrázek 19 Uživatelské rozhraní MrGuard [36]*

### 11.1.3 Security Center

Produkt Security Center vyvíjí Kanadsko-Francouzská společnost Genetec. Svou koncepcí a architekturou je velmi podobný předešlým dvou systémů. Do svého serveru dokáže integrovat různorodé technologie a uživateli tak podávat informace o stavu střežené lokality jednotným způsobem s přidanou hodnotou ovládání a správy připojených technologií. Dokáže také technologiím přidávat určitou vyšší logiku v podobě možného provázání čidel a následně automatizovaných reakcí na určitý stav ve střeženém prostoru.

Tento systém je primárně nasazován ve velký průmyslových objektech, korporátních společnostech a velký důraz je kladen na prosazení se na světových letištích. Oproti tomu ale stojí vyšší cena oproti konkurenci a v podstatě nemožné, nebo velmi nákladné doprogramování změn na přání uživatele. Společnost Genetec profiluje svůj systém jako typický produkt a jakékoli změny oproti plánu jsou složitě




*Obrázek 20 - Uživatelské rozhraní Security center [37]*

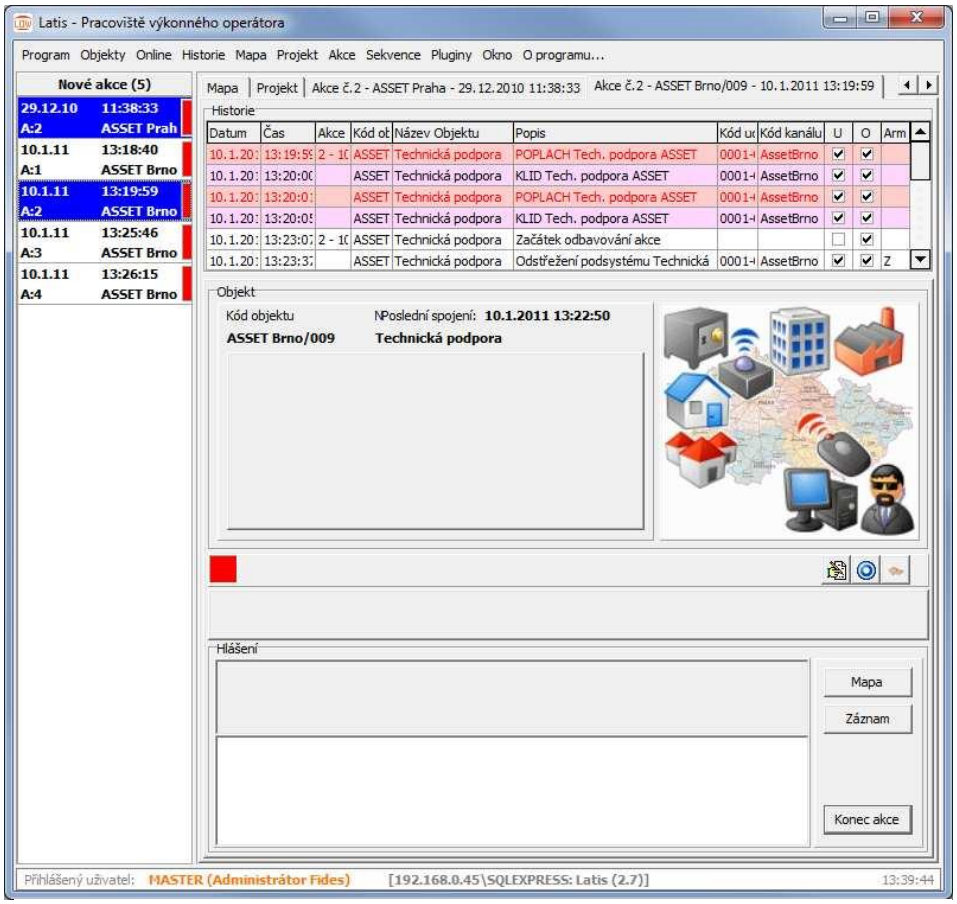
vyjednatelné. Velkou nevýhodou je pak absence české lokalizace. Tyto nedostatky by mohly být v rozhodování o nasazení tohoto systému na DPP rozhodující v jeho neprospěch.

### 11.1.4 Latis

Latis je produktem nabízeným na českém trhu společností FIDES a.s. Jedná se o monitorovací a integrační systém, který je navržen jako otevřený, aby jej bylo možné rozšířit o nové funkcionality. Latis integruje typu EPS, EZS, EKV, CCTV a uživateli utváří jednotný a komfortní pohled na systém. LATIS je koncipován jako systém s rozloženou inteligencí, což zefektivňuje a optimalizuje využití jednotlivých funkčních celků, které si navzájem předávají jen nezbytně nutné minimum

informací. Výkon systému jako celku tím podstatně narůstá a systém je schopen plnit velké množství úkolů požadovaných uživatelem. Monitorovací a integrační systém LATIS SQL je produkt, který může být použit od nejjednodušších aplikací až po nejrozsáhlejší bezpečnostní systémy. [38]

Tento systém není na českém trhu tak silně rozšířen, jako výše zmínění konkurenti a také jeho vývoj není opřen o mnohaleté zkušenosti. Jedná se ale o progresivní a dynamicky se rozvíjející systém. Pro potřeby DPP by ovšem zatím mohl být nedostatečný z pohledu chybějících funkcionalit a absence referencí z velkých instalací. Uživatelské rozhraní systému zatím není na takové úrovni jako například u systému MrGuard.

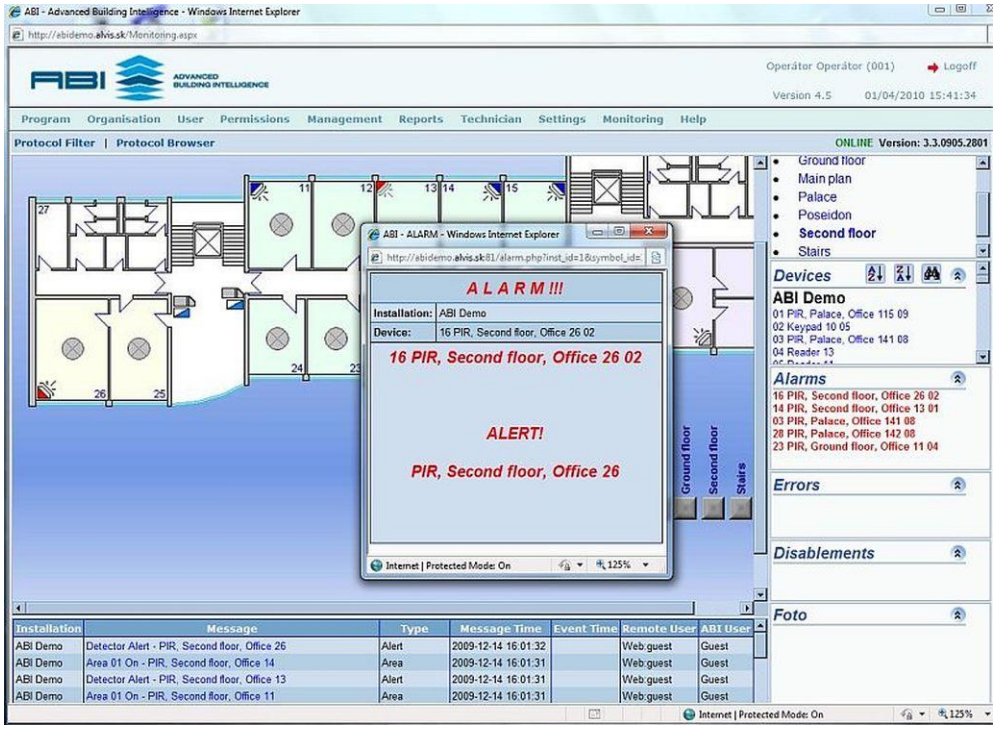



*Obrázek 21 - Pracovní prostředí systému Latis*

### 11.1.5 ALVIS

Tento systém je produktem slovenské společnosti SPIRIT a.s., která sebou nese více jak 20letou zkušenost s vývojem nadstavbových SW. ALVIS mimo integraci

bezpečnostních technologií, CCTV, přístupových systému atd. komunikuje pomocí webového rozhraní i například se systémy personalistiky, nebo mzdovými systémy.




*Obrázek 22 - Uživatelské rozhraní dohledové aplikace ALVIS [39]*

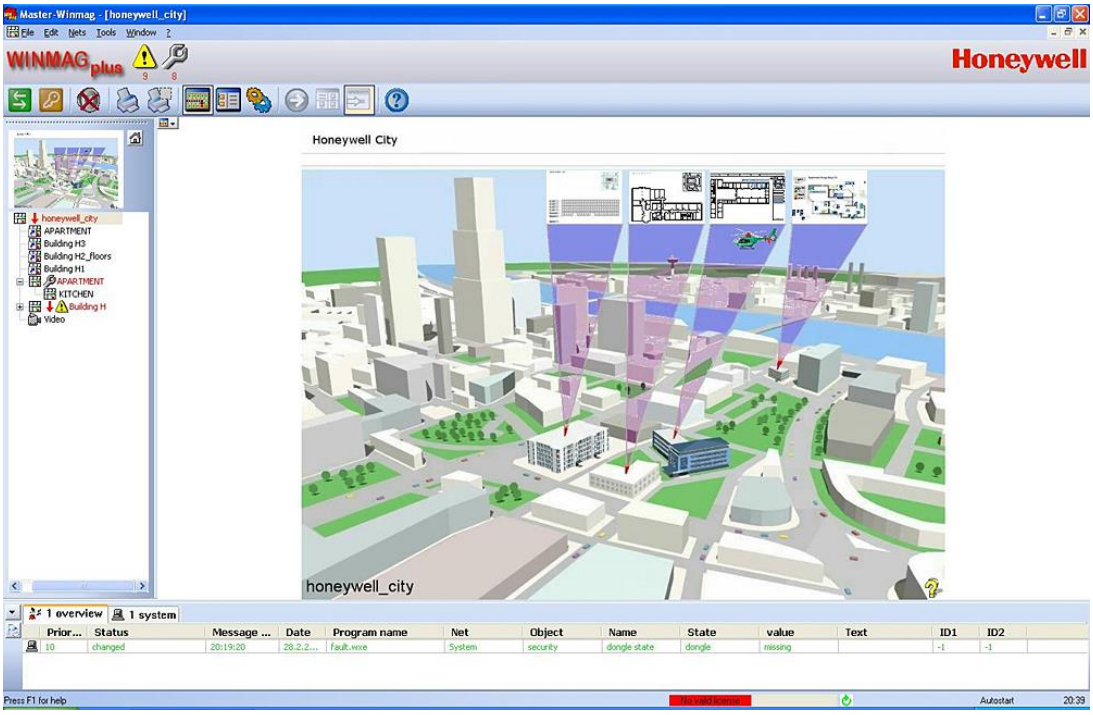
To systém povyšuje z bezpečnostní nadstavby na kompletní správcovský systém. Tato rozsáhlost systému je ale vůči požadavkům DPP nežádoucí, a to z důvodu, kdy je požadována pouze dodávka systému zaměřeného pouze na bezpečnostní dohled. Funkce propojení s dalšími, než jen bezpečnostními systémy by tedy nenašli uplatnění. [39]

### 11.1.6 WINMAG

Systém řízení a správy bezpečnostních technologií WINMAG je vyvíjen společností Honeywell. Tato společnost je předním výrobcem bezpečnostních technologií, požárních systémů a kamerových systémů. Je proto logickým krokem, že na trh dodává i nadstavbový systém pro tyto technologie.

Databáze a uživatelská pracovní plocha jsou vytvořeny dle běžných standardů. Hlášení se zobrazují graficky a v textové formě. Díky modulární struktuře poskytuje WINMAG vhodný software pro zařízení jakéhokoliv rozsahu a pro každou oblast

aplikace. Sortiment zahrnuje rozsah od WINMAG základního balíčku pro systémy jednoho pracoviště až po software aktualizace a přechodu z GEMAG na WINMAG. Značnou výhodou je možnost redundance na úrovni SW, kterou jiní konkurenti nenabízí. Zásadním nedostatkem je, že spol. Honeywell nepodporuje úpravu SW na klíč, to znamená, že dodává systém pouze jako produktové řešení, nikoli projektové. [40]




*Obrázek 23 - Uživatelské rozhraní SW WINMAG [40]*

## 11.2 Přínosy nadstavbových systémů pro DPP

Dle výše zmiňovaných vlastností jednotlivých systémů je předpokládaný přínos po instalaci vybraného systému na DPP jednoznačný. Implementovaný nadstavbový systém musí uživateli přinést jednotnou podobu dohledu nad střeženým prostorem a dát možnost povelování technologií pro daný prostor, a to vše na základě přidělených oprávnění. Tímto bude zjištěna snazší a rychlejší obsluha bezpečnostních technologií, za čímž je očekávaným přínosem úspora času při řešení vzniklých incidentů.

Další přidanou hodnotou systému bude možnost virtuálního provázání koncových čidel navzájem a také propojení například požárních čidel s kamerovým systémem. Uživatel nebude následně muset složitě vyhledávat záznam kamery v zóně poplachu, ale záznam z kamery se mu automaticky spustí na monitoru spolu s upozorněním na vzniklý incident. Opět tímto systém přinese úsporu času při řešení incidentů a značně rychlejší a efektivnější reakci na incident, což v případě například požáru předchází vzniku rozsáhlých škod.

Mimo zmíněné přínosy z hlediska koncového uživatele musí systém splňovat i nároky na snadnou implementaci dat, jejich správu a uživatelskou možnost správy celého systému. To přinese možnost si systém administrovat vlastními zaměstnanci DPP, které tímto nebude vázán na servisní pracovníky dodavatele.

Detailnější pohled na jednotlivé vybrané požadavky ze strany DPP byly získány pomocí řízených rozhovorů se zaměstnanci DPP, konkrétně vedoucím bezpečnostního úseku a vedoucím sdělovacího úseku. Tyto požadavky budou dále popsány v kapitole 7.2.

# 12 Výběr vhodného systému pro projekt JIP

## 12.1 Multikriteriální analýza pro výběr vhodného systému

Jako nástroj pro užší kvalifikaci systémů, které by mohli být použity pro implementaci v DPP jsme se rozhodl použít metodu multikriteriální analýzy. Touto metodou zúžím výše uvedených šest systémů na finální dva, které následně detailně porovnám.

Alternativy, mezi kterými se budu rozhodovat jsou jednotlivé výše zmíněné systémy (6 systémů). Jako klíčová kritéria, která zahrnu do analýzy jsem určil následující:

1. Možnost dovývoje funkcionalit
2. Servisní podpora v ČR
3. Česká lokalizace
4. Významné reference
5. Cena SW (bez dovývoje)

Jednotlivá kritéria mohou nabývat hodnot v číselné řadě od 1 do 5 v závislosti na přínosu, jaký dané kritérium přináší, přičemž jedna je nejmenší přínos, pět naopak největší.

Kritéria budou v tabulce také ohodnocena váhami, které budou určovat význam kritéria. Váhy budou definovány číselným ohodnocením od 1 do 3, kdy jedna je nejméně významná a tři nejvíce významná.

*Tabulka 2 - Ohodnocení kritérií*
*Zdroj: vlastní*

| Alternativa | Možnost dovývoje funkcionalit | Servisní podpora v ČR | Česká lokalizace | Významné reference | Cena SW (bez dovývoje) |
|---|---|---|---|---|---|
| Váha kritéria | **3** | **3** | **2** | **2** | **1** |
| **C4** | 4 | 4 | 5 | 4 | 3 |
| **MrGuard** | 5 | 4 | 5 | 3 | 3 |
| **Security Center** | 2 | 2 | 2 | 5 | 2 |
| **Latis** | 3 | 3 | 5 | 2 | 4 |
| **Alvis** | 3 | 3 | 5 | 2 | 4 |
| **WINMAG** | 2 | 4 | 5 | 1 | 4 |

Hodnoty kritérií a váhy byly uděleny jednotlivým kritériím do tabulky ve spolupráci se zástupci DPP, kteří určili váhu kritériím a přiřadily bodové ohodnocení pro jednotlivá kritéria.

*Tabulka 3 – Výsledková tabulka součinů váhy kritérií a ocenění kritéria.*
*Zdroj: vlastní*

| Alternativa | Možnost dovývoje funkcionalit | Servisní podpora v ČR | Česká lokalizace | Významné reference | Cena SW (bez dovývoje) |
|---|---|---|---|---|---|
| Váha kritéria | **3** | **3** | **2** | **2** | **1** |
| **C4** | 12 | 12 | 10 | 8 | 3 |
| **MrGuard** | 15 | 12 | 10 | 6 | 3 |
| **Security Center** | 6 | 6 | 4 | 10 | 2 |
| **Latis** | 9 | 9 | 10 | 4 | 4 |
| **Alvis** | 9 | 9 | 10 | 4 | 4 |
| **WINMAG** | 6 | 12 | 10 | 2 | 4 |

Číslice v buňkách tabulky představují součiny vah jednotlivých kritérií a bodového ohodnocení kritéria. Následným součtem bodů pro každou alternativu dostaneme

celkový výsledný počet bodů, na základě, kterého stanovým dvě nejvhodnější alternativy.

*Tabulka 4 - Součty bodů pro jednotlivé systémy*
*Zdroj: vlastní*

| Alternativa | Celkový počet bodů |
|---|---|
| **C4** | 45 |
| **MrGuard** | 46 |
| **Security Center** | 28 |
| **Latis** | 36 |
| **Alvis** | 36 |
| **WINMAG** | 34 |

*Tabulka 5 – Pořadí systémů na základě bodových součtů*
*Zdroj: vlastní*

| Pořadí | Alternativa | Celkový počet bodů |
|---|---|---|
| 1 | MrGuard | 46 |
| 2 | C4 | 45 |
| 3 | Latis | 36 |
| 4 | Alvis | 36 |
| 5 | WINMAG | 34 |
| 6 | Security Center | 28 |

Na základě provedené analýzy bylo zjištěno, že dvě nejvhodnější alternativy (systémy), které budu dále detailněji porovnávat jsou systém MrGuard od společnosti Colsys a systém C4 vyvíjený společností Gamanet. Provedená analýza odráží dominantní postavení těchto dvou systémů na českém trhu.

## 12.2 Porovnání funkcionalit vybraných systémů

Pro výběr systému, který bude nejvíce vyhovovat pro nasazení do DPP, budou porovnány podrobné funkce obou vybraných (C4, MrGuard) oproti požadavkům DPP. Seznam požadavků, které jsou v následující tabulce vyjmenovány byly

konzultovány se zástupci DPP, konkrétně vedoucím sdělovacího úseku, vedoucím bezpečnostního úseku a velitelem HZS DPP.

*Tabulka 6 - Porovnání uživatelských funkcí*
*Zdroj: vlastní*

| Seznam funkcionalit | POŽADAVEK DPP | C4 | MrGuard |
|---|---|---|---|
| **Uživatelské funkcionality** | | | |
| Povelování technologií ze stromu lokace | ano | ano | ano |
| Povelování technologií z mapy | ano | ano | ano |
| Zobrazování vrstev v mapách | ano | ne | ano |
| Automatický tisk zásahové mapy | ano | ano | ano |
| Česká lokalizace systému | ano | ano | ano |
| Uživatelsky definované akce | ano | ne | ano |
| Emailové notifikace | ano | ano | ano |
| Reporting | ano | ano | ano |
| Incident management | ano | ano | ano |
| Eskalace incidentů | ano | ano | ano |
| Grafický ukazatel stavu systému | ano | ne | ano |
| Mobilní klient | ano | ne | ano |
| Možnost předání služby | ano | ne | ano |
| Automatické zobrazení streamu kamery | ano | ano | ano |
| Chat okno u incidentu | ano | ne | ano |
| Správa klíčových trezorů | ne | ano | ne |
| Proklikávací zóny v mapě | ano | ne | ne |
| Uživatelské rozhraní pro analýzu dat | ano | ne | ano |
| Ovládání pomocí klávesových zkratek | ano | ne | ne |

Tabulka č.5 porovnává jednotlivé uživatelské funkce systémů a dále je srovnává informací, zda je tato funkce DPP požadována. Cekem bylo porovnáno 19 uživatelských funkcionalit z niž 18 jsou zároveň požadavky DPP.

Porovnání systémů:

- MrGuard splňuje 16/18
- C4 splňuje 10/18

*Tabulka 7 - Porovnání servisních a implementačních funkcí*
*Zdroj: vlastní*

| Seznam funkcionalit | POŽADAVEK DPP | C4 | MrGuard |
|---|---|---|---|
| **Servisní a implementační funkcionality** | | | |
| Videomanagement | ano | ano | ano |
| Vazby mezi technologiemi | ano | ano | ano |
| Vytváření virtuálních lokací | ano | ne | ano |
| Definice závažnosti zpráv z technologií | ano | ne | ano |
| jednotná zpráva uživatelů | ano | ano | ano |
| Oprávnění pro povelování technologií | ano | ano | ano |
| Oprávnění pro řešení incidentů | ano | ano | ano |
| Export mapy zpět do DWG | ne | ano | ne |
| Zakládání různých typů incidentů | ano | ne | ano |
| Automatická archivace dat | ano | ne | ne |
| Možnost přidat ručně čidlo do mapy | ano | ano | ne |
| Uživatelsky definovat zoom na mapu | ano | ano | ano |
| Možnost off-line importu dat | ne | ano | ne |
| Vytváření virtuálního stromu lokace | ano | ne | ano |

Tabulka č. 6 porovnává jednotlivé servisní a implementační funkce systémů a dále je srovnává s informací, zda je tato funkce DPP požadována. Cekem bylo porovnáno 14 servisních a implementačních funkcionalit z niž 12 jsou zároveň požadavky DPP.

Porovnání systémů:

- MrGuard splňuje 10/12
- C4 splňuje 19/12

*Tabulka 8 - Porovnání obecných funkcí*
*Zdroj: vlastní*

| Seznam funkcionalit | POŽADAVEK DPP | C4 | MrGuard |
|---|---|---|---|
| **Obecné funkcionality** | | | |
| architektura klient/server | ano | ano | ano |
| podpora EZS | ano | ano | ano |
| podpora EPS | ano | ano | ano |
| Podpora CCTV | ano | ano | ano |
| Podpora EKV | ano | ano | ano |
| Licencování dle počtu | ne | ano | ano |
| Logování zpráv z technologií | ano | ano | ano |
| Logování uživatelských aktivit | ano | ne | ano |
| neomezená licence | ano | ne | ano |
| vektorové zobrazení map | ano | ano | ano |
| podpora GIS map | ano | ne | ne |
| podpora Bitmapy | ano | ano | ne |
| Možnost konfigurace technologií | ne | ne | ne |
| Jednotná databáze | ano | ano | ano |
| Možná rozšiřitelnost systému | ano | ano | ano |

Tabulka č. 7 porovnává jednotlivé obecné funkce systémů a dále je srovnává s informací, zda je tato funkce DPP požadována. Cekem bylo porovnáno 18 obecných funkcionalit z niž 15 jsou zároveň požadavky DPP.

Porovnání systémů:

- MrGuard splňuje 12/15
- C4 splňuje 11/15

Výsledky zjištěné z porovnání (viz tabulka 5, 6, 7) byly předloženy vedoucímu bezpečnostního úseku na DPP a vedoucímu sdělovacího úseku DPP. Tito dva zástupci, kteří reálně spolurozhodují o investicích do zabezpečovacích technologií v DPP se přiklonili k implementaci systému MrGuard. Důvodem rozhodnutí bylo výše provedené zkoumání s přihlédnutím k faktu, že je aktuálně v DPP využívána starší verze systému MrGuard (řady3), se kterým již mají zkušenosti.

# 13 Realizace projektu s vybraným systémem splňující požadavky JIP

Realizace projektu JIP včetně implementace bude od objednání do ukončení a předání projektu plánován na celkem cca 15 měsíců. Podrobnější diagram viz kapitola 12.1. Modelově byl projekt zasazen do termínu 15. 1. 2018 až 15. 3. 2019. Realizace do sebe zahrnuje mimo dovývoje požadavků do vybraného software také rekonstrukci a doplnění datové sítě v DPP, na které je software JIP a komunikace technologií přímo závislá.

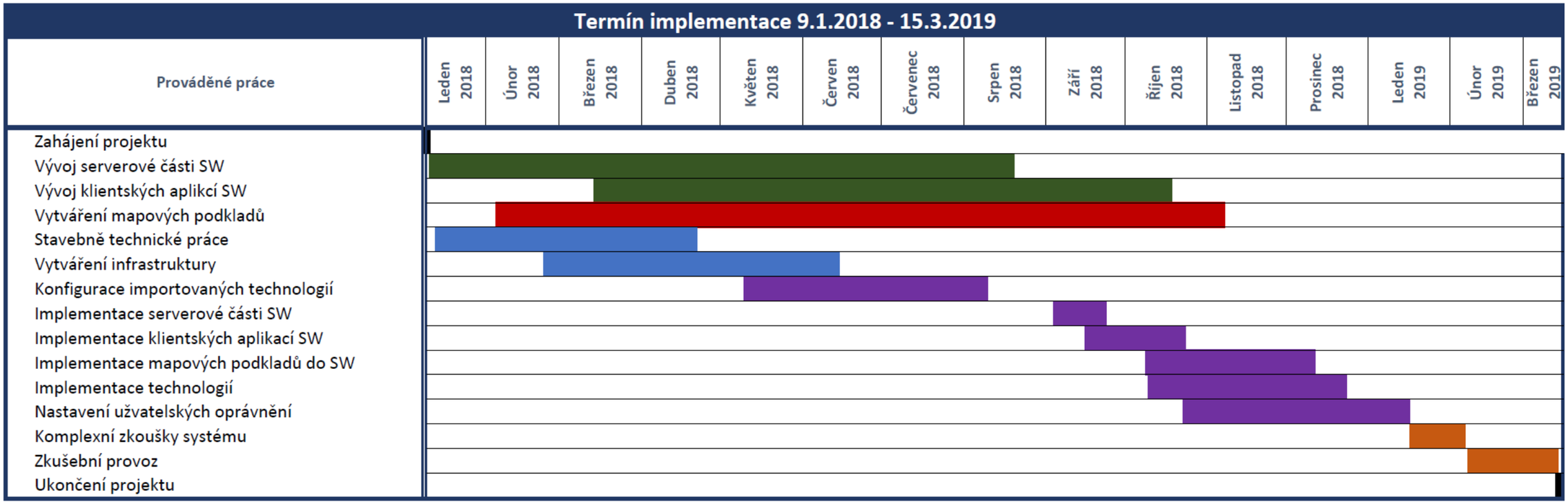
Velmi náročným úkolem je získání a aktualizace mapových podkladů DPP, které jsou nyní neaktuální a na straně DPP není konkrétní osoba, která by za tyto podklady zodpovídala. Do mapových podkladů je dále nutné přesně zakreslit jednotlivá čidla technologií, tak aby odpovídala reálnému stavu. Pracnost na tyto úkoly spojené s mapovými podklady je odhadnuta na cca 8 měsíců. Z tohoto hlediska je to jedno z možných rizik při implementaci systému.

Druhým dlouhodobým a náročným úkolem, který lze považovat za značné riziko, které může případně ohrozit implementaci systému je konfigurace ústředen technologií. Každá z ústředen musí být nakonfigurována přesně v souladu s nadstavbovým softwarem, tak aby podávala správné informace. V případě chybné konfigurace ústředen by se nemuselo vůbec podařit ústřednu připojit. S ohledem na to, že systém implementuje 212 ústředen EPS a EZS, 100 servetů PTV a více jak 1000 kusů řídících jednotek EKV je tato práce plánována ve stejném rozsahu jako aktualizace mapových podkladů, tedy na 8 měsíců.

Aby bylo možné implementaci reálně dokončit ve stanoveném čase 15 měsíců je podmínkou, aby většina prací probíhala paralelně, což je názorně zobrazeno v zmíněné příloze. Toto ale sebou nese vekou zátěž na zařazení lidských zdrojů a jejich následnou koordinaci v průběhu implementace.

## 13.1 Časový harmonogram projektu JIP

Harmonogram graficky znázorňuje rozložení hlavních pracovních bloků rozložených v čase. Harmonogram byl časově zasazen do období od 9.1.2018 – 15.3.2019. Termín realizace je pouze příkladový, rozložení jednotlivých úkolů, jejich délka trvání a závislosti mezi úkoly odpovídají reálnému zpracování.




Legenda:

*Obrázek 24 - Harmonogram projektu JIP.*
*Zdroj: vlastní*

- Zahájení a ukončení projektu
- Vývoj SW dle požadavků DPP
- Projekční práce
- Stavební úpravy v DPP
- Technické práce
- Předání a zkoušky

# 14 Komparace odbavení incidentu před implementací a po implementaci

Pro demonstrování přínosu softwarové bezpečnostní nadstavby bude dále v této kapitole komparovat modelové případy odbavení incidentu, a to ve stavu před nasazením SW a následně po jeho nasazení.

K demonstraci bude sloužit fiktivní incident, a jeho následné odbavení bude popsáno s ohledem na to, že některé informace týkající se bezpečnostního managementu jsou považovány za důvěrné, nebo vyhrazené.

Porovnání stavů před a po nasazení softwaru bude provedeno pomocí komparační tabulky. Cílem je především porovnání z časového hlediska, které je zejména u incidentů spojených například s požárem, nebo bezpečnostním incidente klíčové.

## 14.1 Definice modelového incidentu

Modelovým incidentem je alarm vyvolaný požárem. Požár vznikl v prostoru tunelu trasy A mezi stanicemi Depo Hostivař a Skalka. Příčina požáru je zkrat na elektroinstalaci. V prostoru se ve chvíli vzniku požáru nenacházel žádný technik, nebo jiná osoba. K požáru došlo v 4:30hod., kdy probíhá výluka metra.

Bezpečnostní ostraha má za úkol zjistit, zda se v tunelu nenachází osoby (servisní technici, údržba), na jakém konkrétním místě k požáru došlo, pokud možno jaká byla jeho příčina a jaký je aktuální stav na místě. Tyto informace musí co nejrychleji předat výjezdu HZS a následně o tomto incidentu provézt zápis do deníku hlášení.

## 14.2 Komparace odbavení před a po nasazení SW systému

*Tabulka 9 - Komparace procesu odbavení incidentu před a po implementaci SW nadstavby. Zdroj: vlastní*

| Pořadí | Postup před nasazením SW | Čas | Postup po nasazení SW | Čas | Událostní blok |
|---|---|---|---|---|---|
| 1 | **Vznik požáru** | **0 sec.** | **Vznik požáru** | **0 sec.** | Vyhlášení požáru |
| 2 | Ústředna EPS vyhlásí poplach, spustí se akustický poplašný signál. | 3 sec. | Ústředna EPS vyhlásí poplach, spustí se akustický poplašný signál a do SW nadstavby zašle prostřednictvím komunikačního rozhraní zprávu o změně stavu – SW nadstavba vyhodnotí stav a vyhlásí poplach (založení ticketu + akustické a vizuální upozornění. | 3 sec. | |
| 3 | Zjištění polohy čidla vyčtením čísla čidla na ústředně a následným dohledáním čidla v papírové mapě, či excelovém seznamu. | 20 sec. | Zjištění polohy čidla z mapy v SW, kde se čidlo vizuálně rozbliká v okně s mapou. | 2 sec. | Vyhodnocování situace |
| 4 | Kontrola místa vzniku požáru pomocí kamerového streamu, který obsluha vyhledá v samostatném SW pro kamery a následně zde vyhledá příslušnou kameru a vyhledá zájmový časový úsek. | 35 sec. | Kontrola místa vzniku požáru na automaticky spuštěném streamu z kamery, která je v SW propojena s poplachovým čidle. SW automaticky spustí časovou smyčku 10sec před vyhlášením alarmu. | 2 sec. | |
| 5 | Zjištění okolností zapříčiňujících vznik požáru – možné pouze kontrolou stavů v ústřednách, která mají čidla rozmístěna v okolí místa vzniku požáru. | 40 sec. | Zjištění okolností zapříčiňujících vznik požáru – SW automaticky v poplachovém ticketu vypíše posledních 10 stavů, které se změnily na všech čidlech v okolí vzniku požáru (například zkrat v elektroinstalaci) | 5 sec. | |
| 6 | Zjištění počtu osob v alarmové zóně – kontrola přístupového systému, kdy systém obsluze vypíše po sestavení dotazu počet osob v dotázané zóně. | 40 sec. | Zjištění počtu osob v alarmové zóně – SW automaticky v poplachovém ticketu vypíše díky vazbě do přístupového systému počet osob, které se v zóně nacházejí. | 2 sec. | |
| 7 | Předání informace výjezdové skupině - verbální popis situace, místa a okolností. | 20 sec. | Předání informace výjezdové skupině - verbální popis situace, místa a okolností + předání automaticky vytisknutého výjezdového protokolu s informacemi (mapa, adresace, popis) | 10 sec. | |
| 8 | Výjezd zásahového vozidla na místo | x | Výjezd zásahového vozidla na místo | x | Práce na místě zásahu |
| 9 | Reset poplachu na ústředně EPS + znovu zastřežení zóny – z klávesnice technologie | 20 sec. | Reset poplachu na ústředně EPS + znovu zastřežení zóny – z SW pomocí jednoho povelu ve stromě lokace. | 5 sec. | |
| 10 | Provádění hasebních a likvidačních prací | x | Provádění hasebních a likvidačních prací | x | |
| 11 | Informování dispečinku pouze o postupu prací a o vývoji situace na místě – pouze pomocí vysílačky | x | Informování dispečinku pouze o postupu prací a o vývoji situace na místě – pomocí vysílačky, nebo zadáváním komentářů do poplachového ticketu prostřednictvím mobilního zařízení spojeného se SW | x | |
| 12 | Pořízení fotodokumentace fotoaparátem – velitel zásahu následně přiloží fotografie do zprávy | x | Pořízení fotodokumentace mobilním zařízením – tyto se automaticky nahrají do komentářů k incidentu | x | |
| 13 | Sepsání zprávy o zásahu do denního hlášení (Obsah: místo, čas, popis incidentu, postup řešení, příčina vzniku atd.) - sepsání provádí velitel zásahu ručně | nad 30 min. | Sepsání zprávy o zásahu – automaticky vygenerovaná zpráva obsahující všechny události spojené s incidentem, které byly v SW logovány včetně komentářů k řešení, které velitel zásahu mohl zapisovat na mobilním zařízení. Tato zpráva se automaticky ukládá do DB a lze ji vytisknout. | do 5 min. | Po zásahové práce |

## 14.3 Vyhodnocení

Komparační tabulka v kapitole 14.2 je rozdělena do 4 událostních bloků (událostní blok = souhrn činností a událostí), kdy každý blok obsahuje několik událostí nebo činností prováděných v rámci událostního bloku. Jednotlivé činnosti a události jsou označeny pořadovým číslem a pokud to bylo možné, tak i vyhodnoceny časovým údajem, který určuje dobu trvání činnosti, nebo události.

Použité událostní bloky:

- Vyhlášení požáru
- Vyhodnocení situace
- Práce na místě zásahu
- Po zásahové práce

### 14.3.1 Vyhlášení požáru

Do událostního bloku vyhlášení požáru spadají v podstatě pouze samotný vznik požáru, jeho detekce a následné upozornění na vzniklý požár. Z hlediska časové úspory není rozdíl mezi režimem před a po nasazení SW nadstavby. Zde je nutné hodnotit jiny aspekt, a to časovou prodlevu mezi vyhlášením požáru ústřednou a SW nadstavbou.

Klíčovou vlastností z pohledu bezpečnosti je, aby časová prodleva mezi vyhlášením alarmu na ústředně a v SW nadstavbě byla v řádech desetin sekund. Díky infrastruktuře s vysokou propustností dat se v našem případě jedná takřka o nulovou prodlevu. Z bezpečnostního hlediska tedy hodnotím blok vyhlašování požáru za bezpečný, bez další přidané hodnoty.

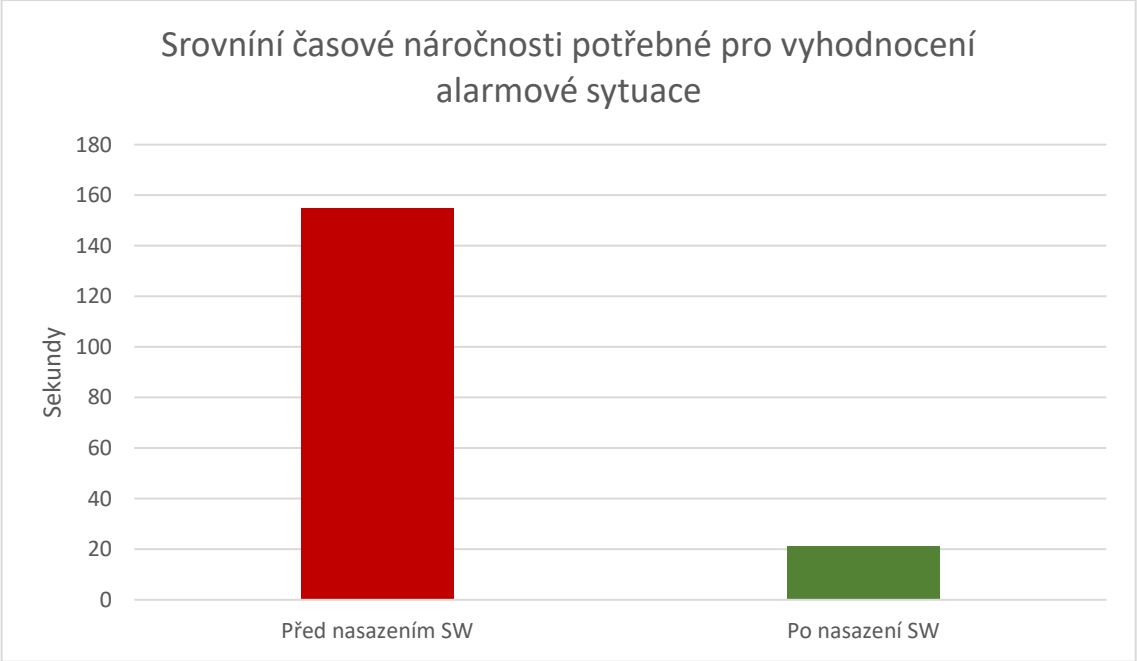
Přidanou hodnotou v této oblasti je, že alarm přijatý SW nadstavbou je adresován konkrétní skupině uživatelů, kteří na něj musí reagovat. SW automaticky loguje časy vzniku alarmu, jeho přijetí obsluhou a následný postup odbavení. Díky tomu lze dlouhodobě sledovat efektivitu práce a navrhovat možné zlepšení procesů

při odbavování alarmů. Ochranou proti neřešení incidentu je eskalace alarmu po uplynutí časového bloku na nadřízenou skupinu uživatelů, čímž je eliminováno riziko lidského selhání.

### 14.3.2 Vyhodnocení situace

Činnosti spojené s vyhodnocením situace před nasazením a po nasazení SW nadstavby jsou již z pohledu srovnání času potřebného na vyhodnocení situace a komfortu pro obsluhu značně rozdílené.

Zatím co vyhodnocení situace bez SW trvá v modelovém příkladu 155 sekund, se systémem je vyhodnocení otázkou 21 sekund.




*Obrázek 25 - Graf srovnání časové náročnosti potřebné pro vyhodnocení alarmové situace. Zdroj: vlastní*

Rozdíl 134 sekund může být v podobné situaci klíčový. Výsledek po nasazení SW nadstavby vnímám jako výrazný posun v možné eliminaci škod v podobných případech.

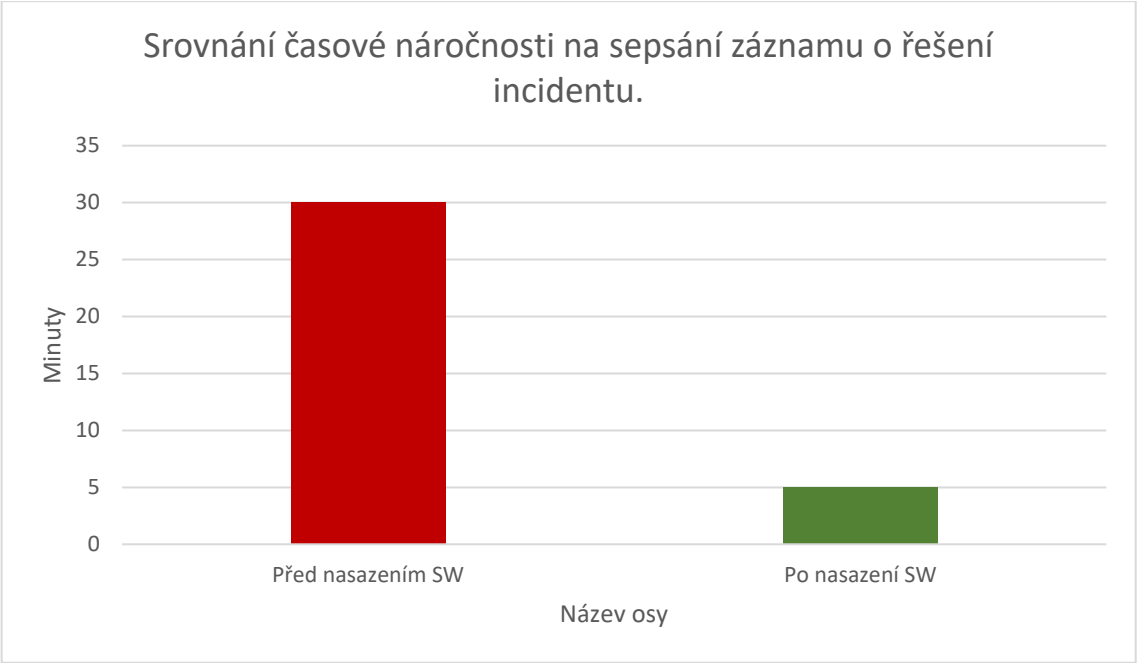
Mimo zmíněné časové úspory vyplývají z komparační tabulky i další výhody po implementaci SW. Jako další značná výhoda může být vnímán komfort s jakým obsluha celou situaci vyhodnocuje. Po implementaci SW je možné vše ovládat a sledovat z jednoho místa (SW nadstavby) namísto sledování několika systémů ve spojení s vyhledáváním v papírových podkladek jako tomu je ve stavu před implementací. Toto může eliminovat riziko pochybení například při přesném určení místa incidentu, nebo zjištění počtu osob v ohrožené zóně.

### 14.3.3 Práce na místě zásahu

Práce na místě zásahu SW nadstavba z pohledu úspory času nijak závažně neovlivňuje. Přináší však zvýšený komfort v podobě práce s mobilním zařízením, které je propojené se SW nadstavbou a díky tomu je možné například komentovat průběh události, kdy se tyto komentáře k vzniklému incidentu zapisují, nebo vkládat k incidentu pořízené fotografie z místa zásahu. Toto následně výrazně zrychluje spisové práce po zásahu.

### 14.3.4 Po zásahové práce

Do této skupiny spadají především činnosti spojené se spisovou povinností. Po vyhodnocení komparační tabulky je patrná značná úspora času a zvýšení komfortu. V případě SW nadstavby se jedná v o zápis jednoho záznamu k incidentu. Všechny ostatní informace (místo incidentu, jednotlivé časy v rámci řešení, zasahující osoby, a další) jsou automaticky k incidentu zapsány. Potřebný čas v případě použití SW nadstavby je do 5 minut, oproti tomu bez použití SW nadstavby by se jednalo o minimálně 30 minut.




*Obrázek 26 - Graf srovnání časové náročnosti na sepsání záznamu o řešení incidentu*
*Zdroj: Vlastní*

Díky této časové úspoře je možné lidské zdroje alokovat na jiné činnosti. Dále je tím získána výhoda jednotného zápisu dat, a tedy i rychlejšího vyhodnocení v případě tvorby statistik jako podpory pro zvýšení efektivity procesů.

# 15 Diskuze

V předložené práci jsem se zabýval nadstavbovými bezpečnostními systémy s ohledem na jejich možné nasazení v podmínkách metra Dopravního podniku hl. m. Prahy. V průběhu zpracování jsem analyzoval požadavky DPP na tyto systémy. Aby bylo možné naplnit očekávání ze strany DPP, provedl jsem průzkum nabídky nadstavbových bezpečnostních systémů na českém trhu, kdy jsem zjistil, že i na našem trhu se nabízí slušné zastoupení produktů v tomto odvětví. Z řady nabízených systémů jsem vybral vzorek, který jsem podrobil multikriteriální analýze, abych dokázal určit ideální systém pro implementaci v podmínkách DPP. Protože se ale jednalo o systémy nabízené českými zástupci, není vyloučené, že se na evropském nebo světovém trhu nenabízí vhodnější systém, které by zjištěné požadavky ze strany Dopravního podniku hl. m. Prahy naplnil lépe. Nicméně z výše zjištěných výsledků jsem zjistil, že po implementaci vybraného nadstavbového bezpečnostního systému se efektivita dohledu nad bezpečnostní situací v metru výrazně zefektivní.

Zde je ale důležité si uvědomit, že se jedná o modelový příklad, ve kterém nelze promítnou všechny aspekty reálného provozu, jako je například lidský přístup k systému, nebo složitost a náročnost udržování aktuálnosti implementovaných dat v systému (mapové podklady a instalace dohledových prvků).

Jako referenční příklad zde není možné uvést jinou bezpečnostní nadstavbu implementovanou v takto velkém rozsahu, na které by se dalo demonstrovat, jakým způsobem byla naplněna očekávání po její implementaci. Důvodem je to, že objekty typu metra, letišť a podobných subjektů tyto data záměrně utajují, aby nemohlo dojít k jejich zneužití při páchání trestné činnosti.

Ze zkušenosti svých kolegů a partnerů ve svém oboru mohu konstatovat, že pokud jsou na začátku projektu dobře pochopeny potřeby uživatele, důkladně zanalyzováno zájmové prostředí a zjištěny všechny možné uživatelské úlohy, které mohou nastat, je skutečný přínos srovnatelný s výsledky zjištění této práce.

bezpečnostního prostředí a pochopení ideologie a potřeb zákazníka a uživatelů systému.

Je důležité si ale uvědomit, že žádný bezpečnostní systém nemůže plně nahradit lidské zdroje. Tyto jsou pro efektivitu dohledu klíčové, a tak je nutné s nimi i správně pracovat ve smyslu kvalitního školení, zadání interních směrnic pro vypořádání se s bezpečnostním incidentem a v neposlední řadě to může být motivační program, který bude iniciovat vlastní vůli po kvalitním dohledu nad bezpečnostní situací.

V práci byla hodnocena pouze efektivita dohledu po implementaci systému a zlepšení obslužnosti a koordinace zdrojů v případě řešení bezpečnostní události. Nebyla zde zohledněna ekonomická stránka, tedy náklady na pořízení takového systému a jeho následnou udržitelnost. Byť by měla být bezpečnost na prvním místě, je důležité, aby vynaložené finanční prostředky byly adekvátní tomu, jak se bezpečnost reálně zvýší.

# 16 Závěr

Cílem práce bylo přinést ucelený pohled na problematiku unifikovaných bezpečnostních nadstaveb s důrazem na implementaci v podmínkách Dopravního podniku hl. m. Prahy. Tento cíl považuji s ohledem na výše vypracovanou práci za splněný. V průběhu práce jsem při zjišťování potřeb u konkrétních uživatelů z řad DPP navázal osobní vazby, na kterých je možné rozšiřovat další spolupráci studentů ČVUT s DPP., což považuji za neocenitelnou přidanou hodnotu této práce pro další studenty. Dále jsem mimo jiné v práci analyzoval současnou situaci na českém trhu s bezpečnostními nadstavbovými systémy, čímž jsem získal širší rozhled v této problematice, který se budu snažit uplatnit dále v mém povolání.

Na závěr bych rád vyjádřil naději, že alespoň některé z myšlenek a poznatků obsažených v této práci si najdou cestu v realizaci skutečného projektu týkajícím se implementace bezpečnostní nadstavby v metru.

# 17 Seznam použité literatury


[1] GEMERLE, Jiří. TECHNICKÁ ZPRÁVA - Softwarová část JIP: Komplexní bezpečností systém KBS. Kladno, 2016.

[2] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-889-4.

[3] ČR. Vyhláška č. 258/1998 Sb.: Národního bezpečnostního úřadu. In: O ochraně utajovaných skutečností a o změně některých zákonů. Ročník 1998. Dostupné také z: https://www.zakonyprolidi.cz/cs/1998-258

[4] ČR. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: 421/2015. 2015. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

[5] Bezpečnostní analýza [online]. Česká republika, 2018 [cit. 2018-03-19]. Dostupné z:http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/Datasheet%20bezpe%C4%8Dnostn%C3%AD%20anal%C3%bdza%20CZ%20040304%20Print.pdf

[6] Qcom.cz: Ochrana utajovaných informací [online]. ČR [cit. 2018-03-20]. Dostupné z: http://www.qcom.cz/systemy-rizeni/ochrana-utajovanych-informaci/

[7] BRABEC, F., I. LÁTAL, R. MUSIL, M. URBAN, T. VEJPULEK a I. PILNÝ. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001. ISBN 80-86445-04-06.

[8] Úvod do režimové ochrany. Http://www.securitye-shop.cz [online]. 2018 [cit. 2018-03-20]. Dostupné z: http://www.securitye-shop.cz/seznam-e-kurzua-a-dokumentaci/fyzicka-ochrana/uvod-do-rezimove-ochrany

[9] Co je režimová ochrana [online]. Bratislava, 2005 [cit. 2018-03-20]. Dostupné z: http://www.dastholding.sk/security/faq/rezimova-ochrana

[10] ČADÍK, Marek. Objektová bezpečnost. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-731-8217-3.

[11] UHLÍŘ, Jan. Technická ochrana objektů. Praha: Vydavatelství Policejní akademie ČR, 2004. ISBN 80-7251-172-6.

[12] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Druhé vydání 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. ISBN 978-80-7318-631-9.

[13] KINDL, Jiří. Projektování bezpečnostních systémů I. Druhé. Zlín, 2007. ISBN 978-80-7318-554-1.

[14] Strážný [online]. [cit. 2018-03-20]. Dostupné z: http://www.henig.cz/cs/zkousky-straznych/

[15] Bezpečnostní poradce [online]. [cit. 2018-03-21]. Dostupné z: http://www.bepo.eu/shortcode/mzs

[16] C4 [online]. 2009 [cit. 2018-03-21]. Dostupné z: https://www.c4portal.com/product/

[17] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín, 2011. ISBN 978-80-87500-05-7.

[18] ACS Íine [online]. 2018 [cit. 2018-03-21]. Dostupné z: http://www.acsline.cz/cs/pristupovy-system

[19] Podniková norma: Poplachové systémy - pravidla zřizování poplachových zabezpečovacích a tísňových systémů objektů. Jablotron, 2007.

[20] Čidla EZS [online]. 2007 [cit. 2018-03-21]. Dostupné z: <http://adela.utko.feec.vutbr.cu/mzsy/prednaska/03_Cidla%20EZS.pdf

[21] Ladinn.cz: Princip fungování EZS [online]. [cit. 2018-03-21]. Dostupné z: http://www.ladinn.cz/ostatni/technika/princip-EZS.html

[22] Http://www.alcamprofi.cz: http://www.alcamprofi.cz [online]. [cit. 2018-03-21]. Dostupné z: http://www.alcamprofi.cz/elektricka-pozarni-signalizace-eps-evakuacni-rozhlas-er.html

[23] ASSIDU: Elektrická požární signalizace, detekce hořlavých plynů a kysličníku uhličitého [online]. [cit. 2018-03-21]. Dostupné z: http://www.assidu.cz/EPS.php

[24] Třídění bezpečnostních systémů [online]. [cit. 2018-03-22]. Dostupné z: https://publi.cz/books/255/01.html

[25] Brilliance Security Magazine [online]. [cit. 2018-03-22]. Dostupné z: http://brilliancesecuritymagazine.com/guest-contributor/by-scott-lindley/a-primer-on-contactless-cards-and-readers-for-electronic-access-control-systems/

[26] Fides: EKV [online]. 2018 [cit. 2018-03-22]. Dostupné z: https://www.fides.cz/technologicke-prostredky/ekv.html

[27] ČSN EN 50 133: Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích. Česko, 2001.

[28] ČESKO. Vyhláška č. 528/2005 Sb.: Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků. In: . Česko, 2005, ročník 2005, číslo 528. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-528

[29] Ladinn.cz: Kamerové systémy [online]. [cit. 2018-03-22]. Dostupné z: http://www.ladinn.cz/ostatni/technika/kamerovy_system.html

[30] VIJA.cz: CCTV DVR KAMEROVÝ SYSTÉM [online]. 2018 [cit. 2018-03-22]. Dostupné z: http://www.vija.cz/bezpecnostni-kamerove-systemy/cctv-dvr-kamerovy-system/

[31] Dpp.cz: Historie [online]. Praha, 2016 [cit. 2018-04-01]. Dostupné z: http://www.dpp.cz/historie/

[32] Výroční zpráva DPP. Praha, 2017, 2017.

[33] Dpp.cz: Dopravní podnik v datech [online]. Praha, 2016 [cit. 2018-04-01]. Dostupné z: http://www.dpp.cz/dpp-v-datech/

[34] Metro Praha [online]. 2017 [cit. 2018-04-03]. Dostupné z: http://metropraha.eu/praha-metro-mapa/

[35] C4portal [online]. 2018 [cit. 2018-04-16]. Dostupné z: https://www.c4portal.com/Product/Areas.aspx

[36] Colsys.cz: Produkt MrGuard [online]. Kladno, 2018 [cit. 2018-04-17]. Dostupné z: http://produkty.colsys.cz/data/cz/mrguard_pl_cz.pdf

[37] Genetec.cz: Products [online]. 2018 [cit. 2018-04-17]. Dostupné z: https://www.genetec.com/

[38] Fides.cz: Latis [online]. 2018 [cit. 2018-04-17]. Dostupné z: https://www.fides.cz/nase-produkty/latis-sql.html

[39] Alvis.sk: Alvis [online]. Slovensko, 2018 [cit. 2018-04-17]. Dostupné z: http://www.alvis.sk/

[40] Honeywell: WINMAG [online]. 2018 [cit. 2018-04-17]. Dostupné z: https://www.hls-czech.com/cs-cz/business/hazard-management-system/products/winmagplus/013610

# 18 Seznam použitých obrázků

Obrázek 1 - Schéma zapojení SW nadstavby. 15
Obrázek 2 - Vizualizace klienta pro nadstavbový systém. [18] 15
Obrázek 3 - Strážný (Fyzická ostraha) [14] 17
Obrázek 4 - Plotový perimetr [24] 18
Obrázek 5 - MZS diagram [14] 22
Obrázek 6 - Ukázka detektorů EZS [21] 24
Obrázek 7 - Schéma zapojení EZS. [23] 26
Obrázek 8 - Sestava kamer včetně DVR. [30] 28
Obrázek 9 - přístupové čtečky s klávesnicí a ústřednou [25] 29
Obrázek 10 - Logo DPP [33] 32
Obrázek 11 - Mapa Pražského metra [34] 38
Obrázek 12: Schéma přístupů technologií a klientů do JIP [1] 40
Obrázek 13: Blokové schéma JIP [1] 40
Obrázek 14 - Příklad GIS mapového podkladu. [1] 42
Obrázek 15 - Příklad mapového podkladu ve formátu AutoCad. [1] 43
Obrázek 16 - Schéma vnímání lokace bezpečnostním pracovníkem. 44
Obrázek 17 - Schéma vnímání lokace servisním pracovníkem 44
Obrázek 18 Uživatelské pracovní prostředí C4 [35] 48
Obrázek 19 Uživatelské rozhraní MrGuard [36] 49
Obrázek 20 - Uživatelské rozhraní Security center [37] 50
Obrázek 21 - Pracovní prostředí systému Latis 51
Obrázek 22 - Uživatelské rozhraní dohledové aplikace ALVIS [39] 52
Obrázek 23 - Uživatelské rozhraní SW WINMAG [40] 53
Obrázek 24 - Harmonogram projektu JIP. Zdroj: vlastní 62
Obrázek 25 - Graf srovnání časové náročnosti potřebné pro vyhodnocení alarmové situace. Zdroj: vlastní 66
Obrázek 26 - Graf srovnání časové náročnosti na sepsání záznamu o řešení incidentu Zdroj: Vlastní 68

# 19 Seznam tabulek

Tabulka 1 - Provozně technické ukazatele [33] ..... 32

Tabulka 2 - Ohodnocení kritérií Zdroj: vlastní ..... 56

Tabulka 3 – Výsledková tabulka Zdroj: vlastní ..... 56

Tabulka 4 - Součty bodů pro jednotlivé systémy Zdroj: vlastní ..... 57

Tabulka 5 – Pořadí systémů na základě bodových součtů Zdroj: vlastní ..... 57

Tabulka 6 - Porovnání uživatelských funkcí Zdroj: vlastní ..... 58

Tabulka 7 - Porovnání servisních a implementačních funkcí Zdroj: vlastní ..... 59

Tabulka 8 - Porovnání obecných funkcí Zdroj: vlastní ..... 60

Tabulka 9 - Komparace procesu odbavení incidentu před a po implementaci SW nadstavby. Zdroj: vlastní ..... 64