

# Bezpečnostní projekt průmyslového areálu kovovýroby

Bc. Tomáš Malaník

---

Diplomová práce  
2017



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

## ZADÁNÍ DIPLOMOVÉ PRÁCE (PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Tomáš Malaník**  
Osobní číslo: **A15181**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **prezenční**

Téma práce: **Bezpečnostní projekt průmyslového areálu kovovýroby**  
Téma anglicky: **A Security Project for a Metal-Manufacturing Company**

### Zásady pro vypracování:

1. Analyzujte legislativní požadavky návrhu a provozu poplachových a video-dohledových systémů.
2. Pojednejte o technicko-technologických trendech v oblastech poplachových a video-dohledových systémů.
3. Definujte funkční vlastnosti poplachových a video-dohledových systémů a popište jejich vazbu na možné technické řešení nejméně ve třech variantách.
4. Navrhněte metodiku bezpečnostního projektu areálu rozsáhlé výrobní společnosti.
5. Zpracujte bezpečnostní projekt areálu konkrétní rozsáhlé výrobní společnosti.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. ČSN EN 62676-1- 1 Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně. 2014.
2. ČSN EN 62676-4: Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 4: Pokyny pro aplikace. 2016.
3. ČSN EN 50131-1 ed. 2: Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky. 2007.
4. ČSN CLC/TS 50131-7: Poplachové systémy – Elektrické zabezpečovací systémy – Část 7: Pokyny pro aplikace. 2011.
5. VALOUCH, Jan. Projektování bezpečnostních systémů. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012, 152 s. ISBN 978-80- 7454-230- 5.
6. VALOUCH, Jan. Projektování integrovaných systémů. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 152 s. ISBN 978-80- 7454-296- 1.

Vedoucí diplomové práce:

**Ing. Jiří Ševčík**

Ústav bezpečnostního inženýrství

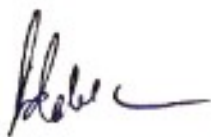
Datum zadání diplomové práce:

**3. února 2017**

Termín odevzdání diplomové práce:

**24. května 2017**

Ve Zlíně dne 3. února 2017



doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



doc. RNDr. Vojtěch Křesálek, CSc.  
*ředitel ústavu*

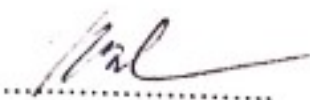
### **Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### **Prohlašuji,**

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 22.5.2017

  
.....  
podpis diplomanta

## ABSTRAKT

V první kapitole teoretické části se diplomová práce zabývá legislativním rámcem a vývoji technicko-technologickými trendy poplachových zabezpečovacích a tísňových systémů a videodohledových systémů. Dále jsou popsány funkční vlastnosti obou systémů a a konci teoretické části je popsána metodika návrhu těchto systémů. Praktická část se zabývá návrhem poplachového zabezpečovacího a tísňového systému a videodohledového systému.

Klíčová slova:

Videodohledový systém, bezpečnostní projekt, analýza, posouzení, riziko, návrh, trend.

## ABSTRACT

In the first chapter of the theoretical part the diploma thesis deals with the legislative framework and the development of technical and technological trends of alarm and emergency systems and video surveillance systems. Further, the functional properties of both systems are described and the methodology of designing these systems is described at the end of the theoretical part. The practical part deals with the design of alarm and emergency system and video surveillance system

Keywords:

Video surveillance systems, security project, analysis, assessment, risk, design, trend.

Tímto bych rád poděkoval Ing. Jiřímu Ševčíkovi za odborné, kvalitní rady a čas, který mi věnoval při konzultacích a úpravách diplomové práce.

# OBSAH

ÚVOD.....	9
<b>I TEORETICKÁ ČÁST.....</b>	<b>10</b>
<b>1    NORMATIVNÍ A LEGISLATIVNÍ POŽADAVKY PRO NÁVRH A       PROVOZ POPLACHOVÝCH ZABEZPEČOVACÍCH A TÍŠŇOVÝCH       SYSTÉMŮ A DOHLEDOVÝCH VIDEOSYSTÉMŮ .....</b>	<b>11</b>
1.1    STRUKTURA NOREM ČSN 5013X.....	11
1.2    ČSN EN 50131 .....	12
1.2.1    ČSN EN 50131-1 ed. 2 (33 4591).....	13
1.2.1.1    Stupně zabezpečení.....	13
1.2.1.2    Třídy prostředí .....	14
1.2.2    ČSN CLC/TS 50131-7 (33 4591) .....	14
1.2.2.1    Návrh systému .....	15
1.2.2.2    Plánování montáže.....	16
1.2.2.3    Prohlídka, funkční zkouška a přejímka.....	16
1.2.2.4    Dokumentace a záznamy o provozu .....	17
1.2.2.5    Provoz systému I&HAS.....	17
1.2.2.6    Údržba a opravy systémů I&HAS .....	17
1.3    ČSN EN 62676 .....	18
1.3.1    ČSN EN 62676-1-1 (33 4592) .....	19
1.3.2    Funkční popis .....	19
1.3.3    Funkční požadavky .....	20
1.3.4    Třídy prostředí.....	20
1.4    ČSN EN 62676-4 (33 4592).....	21
1.4.1    Obecně.....	21
1.4.2    Specifikace provozních požadavků.....	22
1.4.3    Výběr zařízení a výkonnost.....	22
1.4.4    Ukládací prostor .....	23
1.5    LEGISLATIVA DOHLEDOVÝCH VIDEOSYSTÉMŮ .....	24
<b>2    TECHNICKO-TECHNOLOGICKÉ TRENDY I&amp;HAS A VSS .....</b>	<b>26</b>
2.1    POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY .....	26
2.1.1    Inteligentní detektory .....	26
2.1.2    Vývoj ovládacích dotykových panelů.....	27
2.1.3    Integrace I&HAS .....	27
2.1.4    Vzdálená správa .....	27
2.2    DOHLEDOVÉ VIDEOSYSTÉMY .....	28
2.2.1    Termovizní kamery .....	29
2.2.2    Přísvit .....	31
2.2.3    Moderní kompresní algoritmy.....	33
2.2.4    Video-analytické funkce .....	35
2.2.5    Širokoúhlé objektivy .....	35
<b>3    POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY A JEJICH       FUNKČNÍ VLASTNOSTI.....</b>	<b>39</b>
3.1    ÚSTŘEDNY .....	39
3.1.1    Ústředny smyčkové.....	40

3.1.2	Ústředny s přímou adresací detektorů .....	41
3.1.3	Ústředny smíšené .....	41
3.1.4	Ústředny s bezdrátovou komunikací .....	42
3.2	DETEKTORY NARUŠENÍ .....	42
3.2.1	Detektory obvodové ochrany .....	44
3.2.2	Detektory plášťové ochrany .....	47
3.2.3	Detektory prostorové ochrany .....	48
3.2.4	Detektory předmětové ochrany .....	51
3.3	KLÁVESNICE .....	52
3.4	SIGNALIZAČNÍ ZAŘÍZENÍ .....	52
3.5	PRVKY TÍŠŇOVÉ OCHRANY .....	53
3.5.1	Veřejné tísňové hlásiče .....	53
3.5.2	Skryté tísňové hlásiče .....	53
<b>4</b>	<b>VIDEODOHLEDOVÉ SYSTÉMY A JEJICH FUNKČNÍ VLASTNOSTI .....</b>	<b>54</b>
4.1	SNÍMÁNÍ OBRAZU .....	54
4.1.1	Snímací čip .....	55
4.1.2	Objektiv .....	57
4.2	PROPOJENÍ .....	59
4.2.1	Přenosová cesta .....	59
4.2.2	Přenosové protokoly síťového videa .....	62
4.2.3	Síťová zařízení .....	63
4.2.4	Zabezpečení sítě .....	64
4.3	ZPRACOVÁNÍ OBRAZU .....	65
4.3.1	Analýza obrazu .....	65
4.3.2	Záznamová zařízení .....	65
4.3.3	Zobrazovací prvky .....	65
4.3.4	Kompresa obrazu .....	66
<b>5</b>	<b>METODIKA TVORBY NÁVRHU BEZPEČNOSTNÍHO PROJEKTU .....</b>	<b>67</b>
5.1	POŽADAVKY ZADAVATELE PROJEKTU .....	67
5.2	METODIKA NÁVRHU I&HAS .....	67
5.2.1	Bezpečnostní posouzení .....	67
5.2.2	Informace návrhu systému I&HAS .....	70
5.2.3	Technické posouzení .....	70
5.3	METODIKA NÁVRHU VSS .....	71
5.3.1	Posouzení rizik .....	71
5.3.2	Specifikace provozních požadavků .....	71
5.3.3	Volba zařízení a výkonnost .....	72
5.3.4	Charakteristiky videa .....	72
<b>II PRAKTICKÁ ČÁST .....</b>		<b>74</b>
<b>6</b>	<b>BEZPEČNOSTNÍ POSOUZENÍ .....</b>	<b>75</b>
6.1	INFORMACE O OBJEKTU .....	75
6.2	BEZPEČNOSTNÍ POSOUZENÍ JEDNOTLIVÝCH SEKTORŮ .....	77
6.2.1	Výroba a sklady .....	77
6.2.2	Administrativa a kanceláře .....	79
6.2.3	Perimetr .....	80



6.2.4	Ostatní .....	81
6.3	PROVOZ V OBJEKTU.....	82
6.3.1	Častý pohyb vysokozdvížných vozíků.....	82
6.3.2	Plášť .....	83
6.3.3	Chodby, schodiště .....	84
<b>7</b>	<b>BEZPEČNOSTNÍ ANALÝZA.....</b>	<b>86</b>
7.1	PROVEDENÍ ANALÝZY .....	88
7.2	VYHODNOCENÍ ANALÝZY .....	91
<b>8</b>	<b>NÁVRH SYSTÉMU .....</b>	<b>92</b>
8.1	I&HAS .....	92
8.1.1	Stupeň zabezpečení .....	92
8.1.2	Typy napájení.....	92
8.1.3	Třída prostředí.....	93
8.1.5	Legenda místností .....	93
8.1.6	Rozmístění prvků .....	95
8.1.7	Použité technické vybavení.....	96
8.1.8	Kabeláž.....	109
8.1.9	Zóny .....	109
8.2	VSS.....	109
8.2.1	Zvolené komponenty.....	110
8.2.2	Praktické řešení .....	114
8.2.3	Úložný prostor.....	115
8.3	FINANČNÍ NÁKLADY .....	120
	<b>ZÁVĚR .....</b>	<b>122</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>124</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>128</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>129</b>
	<b>SEZNAM TABULEK.....</b>	<b>132</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>134</b>

## ÚVOD

Zabezpečovací systémy v současné době nabývají čím dál většího významu a postavení ve společnosti. Kvalitní poplachové zabezpečovací a tísňové systémy kombinované s videodohledovými systémy jsou efektivním prostředkem k ochraně zdraví, majetku před poškozením, zničením nebo jiným narušením chodu společnosti.

Tématem diplomové práce je bezpečnostní projekt rozsáhlé výrobní společnosti, která se zabývá především kovovýrobou, ale i výrobou plastových a gumových výrobků. Zabezpečovaný areál a objekt je rozsáhlý a mělo by se k němu i tak přistupovat.

K vytvoření kvalitního návrhu bezpečnostního projektu je nutné získat informace o zabezpečovaném objektu od zadavatele. Dalším východiskem je bezpečnostní posouzení objektu a analýza. Je tedy nutné vyhodnotit kritické a potenciálně nebezpečné prostory.

Teoretická část diplomové práce je rozdělena na 5 kapitol. V první kapitole je popsána problematika technických norem vztažených k návrhu poplachových zabezpečovacích a tísňových systémů a videodohledových systémů a je zmíněn i legislativní rámec vztažený k provozu videodohledových systémů. Dále jsou popsány technicko-technologické trendy, kde jsou uvedeny současné technologie využívané v těchto systémech. Poté je čtenář seznámen s funkčními vlastnostmi obou systémů, kde je popsán například princip funkce IP kamerového zařízení a popis jednotlivých komponentů nebo způsob zapojení detektorů k ústředně. Poslední kapitolou teoretické části je metodika tvorby I&HAS a VSS, která vychází z příslušných technických norem, která je poté použita k vytvoření návrhu bezpečnostního projektu.

V praktické části je provedeno bezpečnostní posouzení objektu zobrazující ty části, které jsou pro návrh systému nejdůležitější. Patří mezi ně plášť, otvory do budovy, perimetr nebo i výrobní hala, která je nejdůležitější částí celého podniku. Dále je provedena bezpečnostní analýza, která slouží k přesnému zobrazení hrozeb a rizik vyskytujících se v jednotlivých částech budovy a areálu. Nakonec je proveden návrh obou bezpečnostních systémů, ve kterém je uveden výčet použitých komponentů, jejich rozmístění, nastavení a zapojení.

## **I. TEORETICKÁ ČÁST**

# 1 NORMATIVNÍ A LEGISLATIVNÍ POŽADAVKY PRO NÁVRH A PROVOZ POPLACHOVÝCH ZABEZPEČOVACÍCH A TÍŠŇOVÝCH SYSTÉMŮ A DOHLEDOVÝCH VIDEOSYSTÉMŮ

V úvodní části práce jsou popsány legislativní požadavky pro návrh a provoz poplachových zabezpečovacích a tísňových systémů a video-dohledových systémů, které jsou úzce spjaty s tématem diplomové práce. Jsou to technické normy, které popisují například samotný výrobek, jeho celkovou konstrukci, použitý materiál a základní bezpečnostní požadavky.

*„Je vyjádřením požadavků na to, aby výrobek, proces nebo služba byly za specifických podmínek vhodné pro daný účel. Stanoví základní požadavky na kvalitu a bezpečnost, slučitelnost, zaměnitelnost, ochranu zdraví a životního prostředí.“*

*V současné době je technická norma kvalifikované doporučení, není závazná. Její používání je dobrovolné, avšak všestranně výhodné.“* [1]

Česká technická norma je schválena Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví a označuje se písemným označením ČSN. [1]

## 1.1 Struktura norem ČSN 5013x

Struktura norem popisující poplachové systémy je popsána v Tab. 1.

Tab. 1: Struktura souboru norem 50 13x [2]

Označení normy	Problematika
ČSN EN 50 130-x-y	Poplachové systémy (všeobecné požadavky)
ČSN EN 50 131-x-y	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy
ČSN EN 50 132-x-y	Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích
ČSN EN 60 839-x-y	Poplachové systémy - Elektronické systémy kontroly vstupu
ČSN EN 50 134-x-y	Poplachové systémy - Systémy přivolání pomoci
ČSN EN 50 136-x-y	Poplachové systémy - Poplachové přenosové systémy a zařízení
ČSN EN 50 137-x-y	Poplachové systémy - Systémy kombinované nebo integrované

Tab. 2: Obecné rozdělení skupiny norem 50 13x [2]

Označení normy	Problematika
ČSN EN 50 13x-1	Systémové požadavky
ČSN EN 50 13x-2~4	Požadavky na komponenty systému
ČSN EN 50 13x-5	Požadavky na komunikaci a propojení
ČSN EN 50 13x-6	Požadavky na napájení
ČSN EN 50 13x-7	Pokyny pro aplikace

K diplomové práci se vztahují především normy ČSN EN 50131 a ČSN EN 62676.

## 1.2 ČSN EN 50131

Soubor norem a technických specifikací s označením ČSN EN 50131 se vztahuje na poplachové zabezpečovací a tísňové systémy. Specifikuje poplachové zabezpečovací a tísňové systémy instalované v budovách. Obsahuje následující části, které jsou uvedené v Tab. 3:

Tab. 3: Jednotlivé části normy EN 50131 [2]

Část 1	Systémové požadavky
Část 2-2	Požadavky na pasivní infračervené detektory
Část 2-3	Požadavky na mikrovlnné detektory
Část 2-4	Požadavky na kombinované pasivní infračervené a mikrovlnné detektory
Část 2-5	Požadavky na kombinované pasivní infračervené a ultrazvukové detektory
Část 2-6	Požadavky na kontakty dveří (magnetické)
Část 2-7	Detektory vniknutí - detektory rozbíjení skla akustické nebo otřesové
Část 3	Ústředny EZS
Část 4	Výstražná zařízení
Část 5-3	Požadavky na zařízení využívající bezdrátové propojení
Část 6	Napájecí zdroje
Část 7	Pokyny pro aplikace
Část 8	Zabezpečovací zamlžovací zařízení

Diplomová práce z celkového souboru technických norem ČSN EN 50131 vychází z ČSN 50131-1 a ČSN EN 50131-7.

### 1.2.1 ČSN EN 50131-1 ed. 2 (33 4591)

Technická norma ČSN EN 50131-1 ed. 2 (33 4591) Poplachové systémy – Poplachové systémy zabezpečovací a tísňové systémy – Část 1: Systémové požadavky je českou verzí evropské normy EN 50131-1:2006. Od roku 2009 nahrazuje ČSN EN 50131-1 (33 4590) z července 1999, která již není v účinnosti. Popisuje požadavky na poplachové zabezpečovací systémy instalované v budovách.

Na rozdíl od předchozí normy rozlišuje poplachové systémy pro detekci vniknutí a poplachové systémy pro detekci přepadení. Proto byla zavedena zkratka I&HAS (Intruder and Hold-up Alarm system), vedle již užívaných HAS (Hold-up Alarm System) a IAS (Intruder Alarm System). České ekvivalenty těchto zkratk jsou následující: I&HAS=PZTS, IAS=PZS, HAS=PTS.

Norma také definuje třídy prostředí a stupně zabezpečení, do kterých se jednotlivé komponenty I&HAS člení. Tyto komponenty se nesmí navzájem ovlivňovat a musí být do systému voleny dle třídy prostředí a stupně zabezpečení. [2]

#### 1.2.1.1 Stupně zabezpečení

Stupeň zabezpečení musí mít přiřazen každý I&HAS. Pokud je systém jasně dělen do jednotlivých podsystémů, je možné přiřadit jednotlivým podsystémům vlastní stupeň bezpečnosti. Stupeň zabezpečení systému odpovídá stupni zabezpečení komponentu s nejnižším stupněm zabezpečení. [2]

Jsou stanoveny následující stupně zabezpečení:

Tab. 4: Stupně zabezpečení [2]

Stupeň zabezpečení	Stupeň rizika zabezpečení	Možnosti vetřelce nebo lupiče
1	Nízké riziko	Vetřelec nebo lupič mají malou znalost I&HAS a disponují omezeným sortimentem snadno dostupných zdrojů.
2	Střední riziko	Vetřelec nebo lupič mají omezené znalosti I&HAS a používání běžného náradí a přenosných přístrojů.

3	Střední až vysoké riziko	Vetřelec nebo lupič jsou obeznámeni s I&HAS a disponují rozsáhlým sortimentem nástrojů a elektronických zařízení.
4	Vysoké riziko	Vetřelec nebo lupič mohou zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů I&HAS.

### 1.2.1.2 Třídy prostředí

Třídy prostředí udávají, v jakém prostředí jsou komponenty schopny pracovat.

Tab. 5: Třídy prostředí [2]

Třída prostředí	Popis prostředí	Rozsah teplot
I – vnitřní	vnitřní prostory se stálou teplotou	+5 °C až +40 °C
II – všeobecné	vnitřní prostory s nestálou teplotou	-10 °C až +40 °C
III – venkovní	vnější prostory bez expozice povětrnostním vlivům	-25 °C až +50 °C
IV – venkovní všeobecné	vnější prostory s plnou expozicí povětrnostním vlivům	-25 °C až +60 °C

### 1.2.2 ČSN CLC/TS 50131-7 (33 4591)

Technická norma ČSN CLC/TS 50131-7 (33 4591) Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace je českou verzí technické specifikace CLC/TS 50131-7:2010. Od roku 2009 nahrazuje ČSN CLC/TS 50131-7 (33 4591) z listopadu 2009.

Tato technická norma poskytuje návod pro návrh, montáž, provoz a údržbu poplachových zabezpečovacích a tísňových systémů. Slouží k minimalizaci množství planých poplachů při plnění požadovaných funkčních vlastností.

Specifikace pro stupeň zabezpečení a třídu prostředí jsou shodné se specifikacemi z normy ČSN EN 50131-1 uvedenou v kapitole 1.2.1.

Dále se technická norma dělí na 7 hlavních kapitol, ve kterých jsou uvedeny jednotlivé etapy projektování systému I&HAS, dle kterých by měla osoba odpovědná za činnost postupovat. [3]

### *1.2.2.1 Návrh systému*

V rámci návrhu systému je nutné posoudit a rozhodnout o rozsahu poplachového zabezpečovací a tísňového systému, zvolit komponenty splňující funkční vlastnosti, stupně zabezpečení, třídy prostředí a rozvrhnout umístění jednotlivých detektorů, jakožto i zvolit počet a typ jednotlivých detektorů. Ke stanovení odpovídajícího stupně zabezpečení, je nutné provést analýzu rizik. Při analýze rizik je nutné brát v úvahu, jaká rizika hrozí majetku, kterých se nachází v prostoru chráněného objektu. Dále s v rámci analýzy objektu posuzuje druh stavebních konstrukcí, lokalita objektu, osídlení a historie krádeží a vloupání do střežených prostor. [3]

Při návrhu I&HAS se dále posuzují vlivy vyskytující se uvnitř a vně střežených prostor.

Volba správných komponentů systémů je další etapou, při které je nutné dbát dodržení požadovaného stupně zabezpečení a třídy prostředí. Komponenty se mají umísťovat na základě jejich funkčních vlastností. Ústředna musí být umístěna uvnitř střeženého prostoru, pokud možno v prostoru s nejvyšším stupněm zabezpečení. Doplnkové ovládací zařízení má být umístěno takovým způsobem, aby bylo eliminováno riziko pozorování postupu obsluhy nepovolanými osobami. Detektory mají být instalovány v souladu doporučení výrobce při zajištění pokrytí, které bylo stanovené analýzou rizik. [3]

Pokud se systém propojuje pevným metalickým vedením, má být toto vedení umístěno uvnitř střeženého prostoru. Jestliže je toto umístění nevhodné, vedení vně střežené prostory by mělo být chráněno, a to uložením například v pancéřové trubce. Kably mají být vedeny tak, aby nemohlo bylo jejich poškození redukováno na minimum. Před mechanickým poškozením lze kably chránit například ve žlabech nebo trubkách, které, pokud jsou vyrobeny z kovového materiálu, mají být uzemněny. Pokud jsou propojovací kably vedeny zároveň se silovými, mají tyto kably být vhodně mechanicky odděleny a/nebo stíněny, aby nedošlo ke vzájemnému ovlivňování a elektromagnetickému rušení. Kabeláž má být řádně označena k jednoduché identifikaci v případě poruchy. [3]



### ***1.2.2.2 Plánování montáže***

Při plánování montáže má být bráno v potaz, zda komponenty je vhodné provozovat v daném prostředí. Také, ke správné funkci komponentu, má být posouzeno technické posouzení prostorů, které mají být střeženy, aby byly zajištěny funkční vlastnosti I&HAS systému, které byly specifikovány v návrhu systému. Technickým posouzením se také zjišťuje, zda byly zvoleny vhodné komponenty. [3]

Na základě rozsahu a komplikovanosti navrženého systému I&HAS má se brát na zřetel potřeba zhotovení realizačního dokumentu. V realizačním dokumentu mají být opraveny chyby a nepřesnosti v dokumentaci návrhu systému zjištěné při technickém posouzení prostorů. [3]

### ***1.2.2.3 Prohlídka, funkční zkouška a převjímk***

Po zhotovení systému a kompletním provedení montáže má být uskutečněna kontrola potvrzující kompletnost montáže systému I&HAS. Veškeré odchylky mají být doplněny do dokumentace skutečného stavu. [3]

Každý detektor má být přezkoušen a jeho funkce jsou porovnány s požadavky v návrhu systému, a pokud byl zpracován, tak i v realizačním dokumentu. Mají být ověřeny veškeré konfigurace k potvrzení, že veškerá indikace a signalizace poplachu je v souladu s požadavky uvedenými v návrhu systému. Má být provedena kompletní zkouška systému I&HAS.

Při předání, které je provedeno pracovníky s příslušnými znalostmi a zkušenostmi je předvedeno fungování systému I&HAS, ovládacích zařízení a přenosového systému. V rámci převjímk je také předán návod k obsluze obsahující popis ústředny I&HAS a jednotlivé kroky k uvedení systému do stavu střežení a klidu. Má být zvaženo i školení obsluhy na základě složitosti systému. [3]

Na základě změn provedených při montáži systému má být zpracována dokumentace skutečného stavu. Tato dokumentace přesně odpovídá stavu nainstalovaných komponentů I&HAS. Zákazníkovi je vystaveno osvědčení o shodě, že je I&HAS nainstalován v souladu s dokumentací skutečného stavu. [3]

#### ***1.2.2.4 Dokumentace a záznamy o provozu***

Dokumentace a záznamy o provozu má být zpracována a udržována v souladu se skutečným stavem a zákazník má být požádán o předložení této dokumentace v případě opravy, údržby nebo úpravy systému I&HAS. [3]

Dokumentace a záznamy o provozu má obsahovat následující části:

- dokumentace skutečného provedení;
- podrobný návod k obsluze obsahující pokyny k provádění činností, jako uvedení zařízení do stavu střežení a do stavu klidu;
- kontakt na fyzickou či právnickou osobu, která zhotovila montáž;
- kontakt na fyzickou či právnickou osobu odpovědnou za údržbu systému;
- kontakt na monitorovací středisko, odpovědné za odezvu na hlášení I&HAS;
- kroky k ověření poplachových stavů;
- předávací protokol;
- osvědčení o shodě. [3]

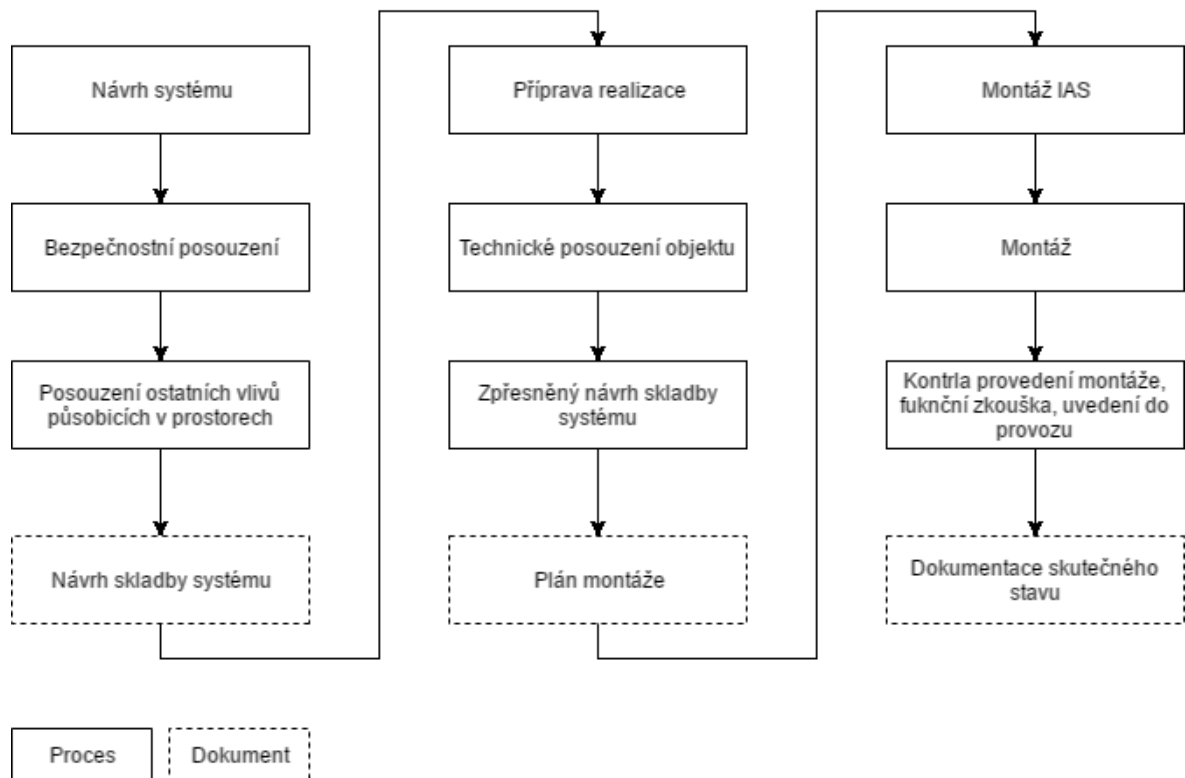
#### ***1.2.2.5 Provoz systému I&HAS***

Zákazník a osoby pověřené k údržbě systému I&HAS mají mít povinnost zajistit, aby systém obsluhovaly osoby k této činnosti pověřené. Dále má být povinen zajistit, aby nedocházelo k planým poplachům, ohlašovat odpovědné bezpečnostní firmě závady. Má být povinen hlásit změny v chráněném prostoru, které by mohly mít negativní vliv na funkci systému. [2]

#### ***1.2.2.6 Údržby a opravy systémů I&HAS***

Zákazník je odpovědný za pravidelné funkční zkouška a údržbu systému. Po montáži má být dohodnut program údržby a servisu s příslušnou bezpečnostní firmou. Má být zajištěno pravidelné měnění akumulátorů a baterií, které nepřekročí doporučení výrobce akumulátorů a baterií. Veškerá činnost týkající se údržby a servisu systému má být zaznamenána do provozní knihy. Pokud je detekována porucha nebo disfunkce jakékoliv části systému I&HAS má uživatel nebo odpovědná osoba za údržbu a servis povinnost nahlásit tuto skutečnost příslušné bezpečnostní firmě. [3]

Na obr. 1 jsou uvedeny jednotlivé kroky činností při zřizování systému I&HAS.



Obr. 1: Vývojový diagram činností při zřizování I&HAS [3]

### 1.3 ČSN EN 62676

Soubor technických norem ČSN EN 62 676 upravuje problematiku videosystémů. Pojem CCTV je v této normě nahrazen pojmem videosystémy (VSS).

Tab. 6: Soubor norem ČSN EN 62676 [4]

Číslo normy	Název normy
ČSN EN 62676-1-1	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky - Obecně
ČSN EN 62676-1-2	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-2: Systémové požadavky - Výkonové požadavky na video přenos
ČSN EN 62676-2-1	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 2-1: Video přenosové protokoly - obecné požadavky

ČSN EN 62676-2-2	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 2-2: Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založených na využití HTTP a REST
ČSN EN 62676-2-3	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 2-2: Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založené na síťových (web) službách
ČSN EN 62676-3	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 3: Analogové a digitální video rozhraní založené na síťových (web) službách
ČSN EN 62676-4	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 4: Pokyny pro aplikace založené na síťových (web) službách

### 1.3.1 ČSN EN 62676-1-1 (33 4592)

Technická norma ČSN EN 62676-1-1 (33 4592) Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně je českou verzí evropské normy EN 62676-1-1:2014. Je v účinnosti od března 2014.

Norma zavádí pojem videosystémy (VSS – Video Surveillance System), které byly dosud nazývané CCTV. Popisuje minimální požadavky a doporučení používané pro bezpečnostní aplikace, specifikuje minimální výkonové a funkční požadavky. [4]

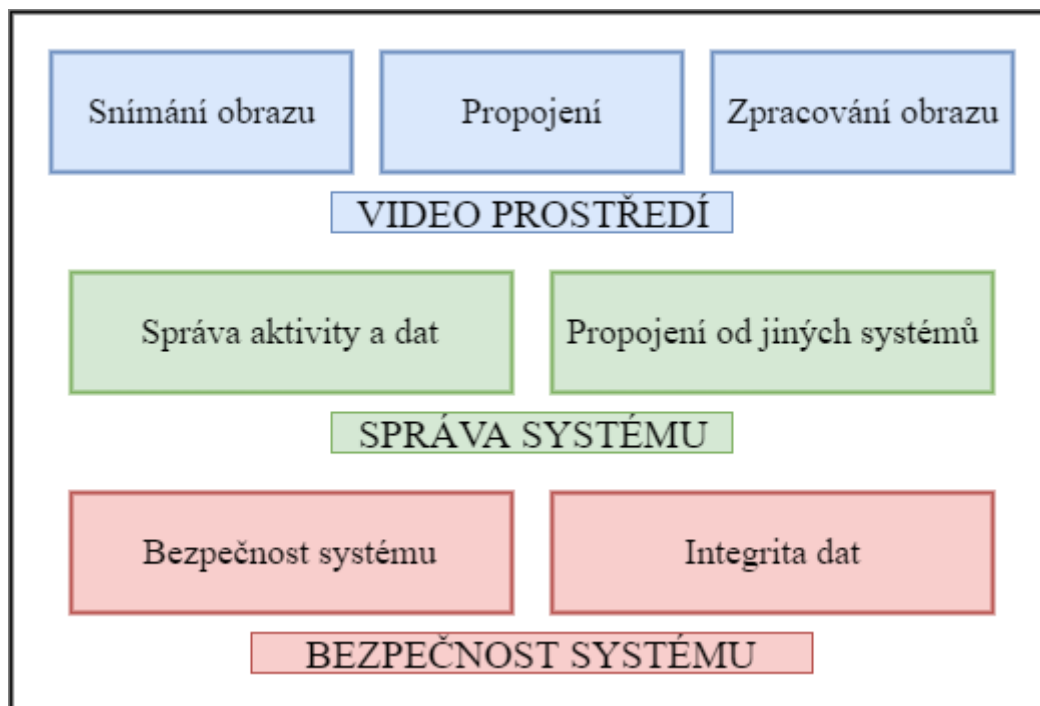
### 1.3.2 Funkční popis

Dohledový videosystém slouží ke generování video obrazu, přenosu a následně k zobrazení a zpracování tohoto videa.

*„Účelem VSS je snímání obrazu scény, zpracování těchto obrazů a jejich zobrazení operátorovi spolu se souvisejícími informacemi pro snadné a efektivní využití.“*

Jednotlivá zařízení dohledového videosystému mohou být propojena například pomocí koaxiálního kabelu nebo optického vlákna, který slouží k přenosu videosignálů a řídicích datových signálů. Obraz může být zobrazován na monitoru nebo projektoru a dále ukládán na paměťovém médiu pro pozdější vyhodnocení.

Videosystém je schopen snímat uživatelem nastavené události, které mohou spustit další přednastavené kroky. Například pomocí signálu z detektoru, kterým může být například detektor kouře, lze spustit poplachovou proceduru, jež spustí předem nadefinované úkony. Tímto úkonem může být například změna pohledu kamery za účelem zaznamenání probíhajících událostí. [4]



Obr. 2: Funkce VSS [4, upraveno Malaník]

### 1.3.3 Funkční požadavky

Snímaný obraz má mít dostatečnou kvalitu k zajištění získání požadovaných relevantních informací. Způsob propojení systému musí být navržen, aby byla minimalizována odezva systému na minimum. Výrobce v dokumentaci musí deklarovat informace o maximálním počtu současně zobrazených obrazů, rozlišení snímku, velikost snímku, obnovovací frekvenci, čas odezvy a barvu obrazu. [4]

### 1.3.4 Třídy prostředí

VSS prvky musí být vhodně použity na základě rozdělení do následujících tříd prostředí.

Tab. 7: Třídy prostředí VSS [5]

Třída prostředí	Popis prostředí	Rozsah teplot
I – uzavřené prostory	uzavřené prostory se stálou teplotou	+5 °C až +40 °C

II – uzavřené prostory obecně	uzavřené prostory s nestálou teplotou	-10 °C až +40 °C
III – vnější prostory kryté před povětrnostními vlivy	vnější prostory bez plného vystavení vlivům počasí	-25 °C až +50 °C
IV – vnější prostory obecně	vnější prostory s vystavení vlivům po- časí	-25 °C až +60° C

#### 1.4 ČSN EN 62676-4 (33 4592)

Technická norma ČSN EN 62676-4 (33 4592) Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 4: Pokyny pro aplikace je českou verzí evropské normy EN 62676-4:2015. S účinností od 14.3.2018 nahrazuje ČSN EN 50132-7 ed. 2 (33 4592) z dubna 2013, která do uvedeného data platí souběžně s touto normou. [5]

*„Tato část IEC 62676 poskytuje doporučení a požadavky pro výběr, plánování, instalaci, přejímku, údržbu a zkoušení dohledových videosystémů (VSS), zahrnující snímací prvky, propojení a zařízení pro zpracování obrazu pro použití v bezpečnostních aplikacích.“ [5]*

##### 1.4.1 Obecně

Před návrhem VSS má být provedena analýza rizik a identifikace hrozeb. VSS by měl být navržen za účelem zmírnění analyzovaných rizik. Při analýze rizik je nutné brát v úvahu, jaká rizika hrozí majetku, kterých se nachází v prostoru chráněného objektu. Dále se v rámci analýzy objektu posuzuje druh stavebních konstrukcí, lokalita objektu, osídlení a historie krádeží a vloupání do střežených prostor. Cílem hodnocení rizik je poskytnout východisko pro stanovení stupně zabezpečení.

Po zvolení umístění VSS má být provedena prohlídka prostorů. Projektant má být tímto způsobem obeznámen se specifiky místa pro návrh VSS, jako je například omezení přístupu a umístění klíčových komponentů. Veškeré skutečnosti mají být zaznamenány pro fázi návrhu systému.

Po prohlídce lokace je zpracováno rozmístění jednotlivých komponentů. Projektant má brát v úvahu veškeré požadavky a místní faktory. [5]

*„Po navržení VSS musí být zpracován plán zkoušek umožňující, aby byl instalovaný systém vhodným způsobem vyzkoušen. Tento plán má obsahovat veškeré kritické aspekty VSS, jako kvalitu obrazu, propojitelnost systému, pokrytí, záběry kamer atd.“ [5]*

#### **1.4.2 Specifikace provozních požadavků**

Zákazník má jasně specifikovat požadavky, které má VSS vykonávat. Musí být specifikováno k jakému účelu VSS má sloužit, zda k monitorování místa, detekci napadení osob a majetku atd. Dále musí být omezen dohled kamery vyplývající z právních předpisů. Je nutné definovat aktivity, které mají být zachyceny, mezi které lze zařadit sledování přístupové cesty, detekování osob pohybující se neoprávněně ve střeženém prostoru atd.

Následující výkonové parametry jsou pokryty:

- funkční vlastnosti systému (čas obsluhy pro monitorování osob),
- rozlišení snímaného obrazu,
- funkce analýzy obrazu.

Dále zákazník specifikuje dobu provozu systému, podmínky prostředí, požadavky na monitorování a ukládání obrazu a následný export obrazového záznamu. [4]

#### **1.4.3 Výběr zařízení a výkonnost**

Každý prvek musí být posouzen, zda splňuje požadavky zákazníka.

Volba kamerového zařízení musí být provedena tak, aby rozlišení, záběr a výkonnost při nízkém osvětlení splňovaly příslušné požadavky.

Při výběrů kamery a objektivu se mají brát v úvahu následující kritéria:

- citlivost kamery odpovídající předpokládaným nejhorším světelným podmínkám,
- ohnisková vzdálenost objektivu k poskytnutí požadovaného zorného pole,
- rozlišení obrazu k poskytnutí nezbytných informací.

Pro zajištění požadovaného zorného pole lze volit kamery s funkcí PTZ (Pan Tilt Zoom), které jsou schopny zorné pole měnit pomocí mechanických nebo elektronických prostředků ovládaných obsluhou nebo automaticky VSS. Kamera v případě užití funkce PTZ musí mít nadefinovanou výchozí polohu.

K dosažení optimálního zorného pole kamery se musí brát v úvahu aspekty prostředí, ve kterém kamera bude nainstalována. Kvalitu záběru mohou ovlivnit odrazy v oknech, sluneční svit nebo externí světelné zdroje nastavené na určitý časový program. Pokud je kamera určena k identifikaci, je vhodné kameru umísťovat do výšky hlavy, jinak nemusí být kamera schopná poskytnout pohled na obličej osoby. [5]

#### 1.4.4 Ukládací prostor

Při propočítávání požadavků na datové uložení je nutné dbát na následující požadavky:

- počet kamer,
- velikost snímku,
- počet snímků za sekundu,
- počet hodin provozu kamery,
- doba uchování záznamu.

K vytvoření odhadu požadovaného prostoru pro uložení záznamu lze použít následující vzorec:

$$\left( \frac{S \times \text{fps} \times C \times H \times 3600}{1\,000\,000} \right) \times T_R$$

Vzorec je popsán v následující tabulce:

Tab. 8: Popis vzorce [5]

<b>S</b>	velikost obrázku v kB
<b>FPS</b>	počet snímků za sekundu
<b>C</b>	počet kamer v systému
<b>H</b>	počet hodin provozu z 1 dne
<b>T<sub>R</sub></b>	doba uchování záznamu
<b>3 600</b>	převod sekund na hodiny
<b>1 000 000</b>	přibližný převod kB na GB

Tento vzorec lze použít pouze pro systémy, v nichž všechny kamery nahrávají se stejným počtem snímků za sekundu, se stejnou velikostí snímku a se shodnou provozní dobou. K výpočtu celkového požadovaného datového prostoru je nutné spočítat požadavek na paměť



pro každou kameru, který se liší i dle snímané scény a výsledný součet poskytne celkový požadavek na paměťové uložení. [5]

## 1.5 Legislativa videodohledových systémů

Provozování videodohledových systémů je v současnosti považováno za jednu z forem zpracování osobních údajů. Musí být dodržována nejen pravidla stanovená zákonem č. 262/2006, zákoníkem práce, ale také pravidla stanovená zákonem 101/2000 Sb., o ochraně osobních údajů. Provozování kamerového systému z hlediska zákona o ochraně osobních údajů definuje, za jakých podmínek je provozování kamerového systému považováno za zpracování osobních údajů:

- vedle kamerového systému je prováděn i záznam pořizovaných záběrů,
- jsou v záznamovém zařízení uchovávány informace,
- pořízené záběry slouží k identifikaci fyzických osob.

Provozování kamerového systému lze provozovat i bez souhlasu dotčených fyzických osob, ale pouze za předpokladu dále uvedených zásad.

Pořizované záznamy nesmí být ukládány, tedy kamerový systém se musí provozovat výhradně on-line. Pro toto rozhodnutí zaměstnavatel musí předně stanovit účel (např. ochrana osob a majetku), musí seznámit zaměstnance a osoby vstupující do sledovaného prostoru a zároveň musí zdůvodnit, proč tomuto účelu nebylo možné docílit jinak. Nesmí docházet k zásahům do soukromí zaměstnanců a dalších osob.

Pokud se zaměstnavatel rozhodne záznamy z kamerového systému uchovávat, musí se jakožto správce osobních údajů registrovat u Úřadu pro ochranu osobních údajů a je povinen plnit následující povinnosti:

- musí dotčené subjekty informovat o rozsahu, účelu sledování a jakým způsobem tyto záznamy budou zpracovány (vydáním vnitřního předpisu v případě zaměstnanců, jinak písemnou informací např. u vstupu objektu);
- kamerový záznam uchovávat je po dobu nezbytně nutnou, aby případný incident mohl být zpracován (běžně 3 dny);
- zachovat soukromí dotčených subjektů (instalovat kamerový systém tam, kde je to opodstatněné). [6]

## DÍLČÍ ZÁVĚR

V kapitole je popsán legislativní rámec vztažený k I&HAS a VSS. Normativní požadavky na I&HAS jsou popsány normou ČSN 50 131 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy. Normativní požadavky na VSS popisuje technická norma ČSN 62 676.

Dále byla popsána problematika právních požadavků na provoz VSS, které popisuje zákon č. 262/2006, zákoník práce a zákon 101/2000 Sb., o ochraně osobních údajů.

## 2 TECHNICKO-TECHNOLOGICKÉ TRENDY I&HAS A VSS

V současné době nejen technické obory se vyvíjí rychlými kroky dopředu. Náklady na koupi zabezpečovacích systémů se neustále snižují, ovládání těchto systému se stále zjednodušuje, což umožňuje čím dál více využívat zabezpečovací systémy i soukromými osobami.

Výrobci nabízejí nepřehrné množství moderních video-dohledových systémů, kterými lze sledovat osoby v prostorech areálu nebo i postup výrobního procesu speciálními k tomu uzpůsobenými kamerovými zařízeními. Pořízené záběry lze archivovat a použít je v případě zjištění mimořádné události.

### 2.1 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy zjišťují a předávají informace o situaci v chráněném prostoru. Slouží k detekování a indikaci přítomnosti, vniknutí nebo pokusu o vniknutí do střeženého prostoru zároveň s možností úmyslného vyvolání poplachového stavu uživatelem. [2]

#### 2.1.1 Inteligentní detektory

Snaha minimalizování planých poplachů je jasným trendem u detektorů narušení. Integrace více senzorů do jednoho detektoru a inteligentní vyhodnocování dat zajišťuje nejpřesnější rozhodnutí o spuštění poplachu. Technologie zajišťující imunitu vůči bílému světlu, optika se třemi ohnisky a neustálé nastavování a vyvažování citlivosti zajišťuje prakticky eliminování planých poplachů. [7]

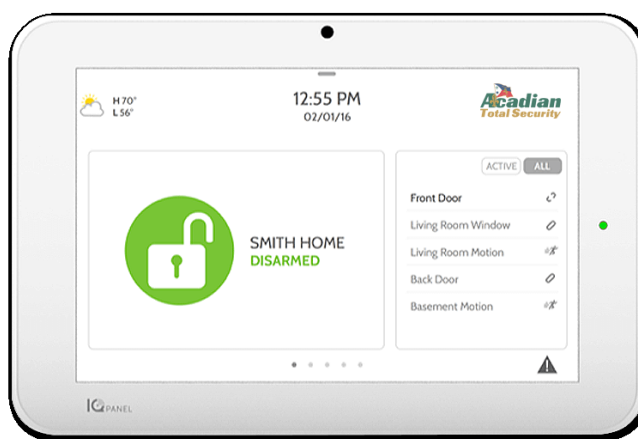
Hlavním cílem je dosáhnout odolnosti vůči negativním vlivům jako jsou počasí, změny teplot nebo zvířata, které by mohly negativně ovlivnit funkci detektoru. [7]



Obr. 3: Více-senzorový detektor pohybu [7]

### 2.1.2 Vývoj ovládacích dotykových panelů

Dotykové ovládací panely zobrazují více informací na jedné ploše. S moderním designem a grafickým zobrazením usnadňují uživateli ovládání systému, které je přehledné a pohodlné. Pomocí dotykových ovládacích panelů lze velmi jednoduše ovládat poplachové i nepoplachové aplikace zabezpečovacího systému, a to především pomocí virtualizačních map. [8]



Obr. 4: Dotykový ovládací panel [8]

### 2.1.3 Integrace I&HAS

Při návrzích bezpečnostních projektů se čím dál častěji požaduje realizace integrace poplachových zabezpečovacích a tísňových systémů. Integrací více systémů dovoluje využít možnosti, díky kterým lze jednotlivým aplikacím svěřit další úlohy, i takových, které pro ně nejsou primárně určené. [9] [10] [11]

Propojení s nepoplachovými aplikacemi, jako jsou např. osvětlení, topení, klimatizace nebo správa energetiky, by mělo přinést spoustu výhod, především snížení provozních nákladů, zjednodušení správy a komfortnějším ovládáním. [9] [10] [11]

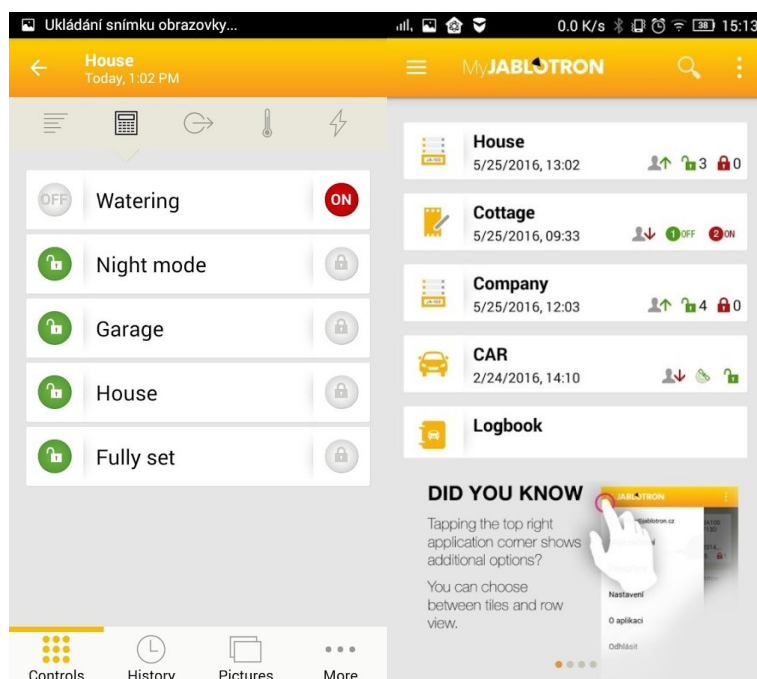
### 2.1.4 Vzdálená správa

Prostřednictvím mobilních telefonů či tabletů lze přijímat stavové informace z ústředny již nějakou dobu, ovšem trendem v posledních letech se stává ovládání poplachových i nepoplachových aplikací pomocí chytrých mobilních telefonů. Pomocí softwarových aplikací lze vzdáleně získat pořízené fotografie video-dohledovým systémem a zobrazit je na mobilním telefonu, také lze vzdáleně ovládat ústřednu I&HAS. [9] [10]

Společnost Jablotron má k dispozici k ovládání jejich zabezpečovacích systémů mobilní aplikaci Můj Jablotron. [12]

Umožňuje:

- aktivovat zastřežení objektu,
- zobrazovat pořízené záběry z VSS,
- vést historii událostí,
- ovládat poplachové aplikace,
- ovládat nepoplachové aplikace,
- sdílet správu se zvolenými osobami. [12]



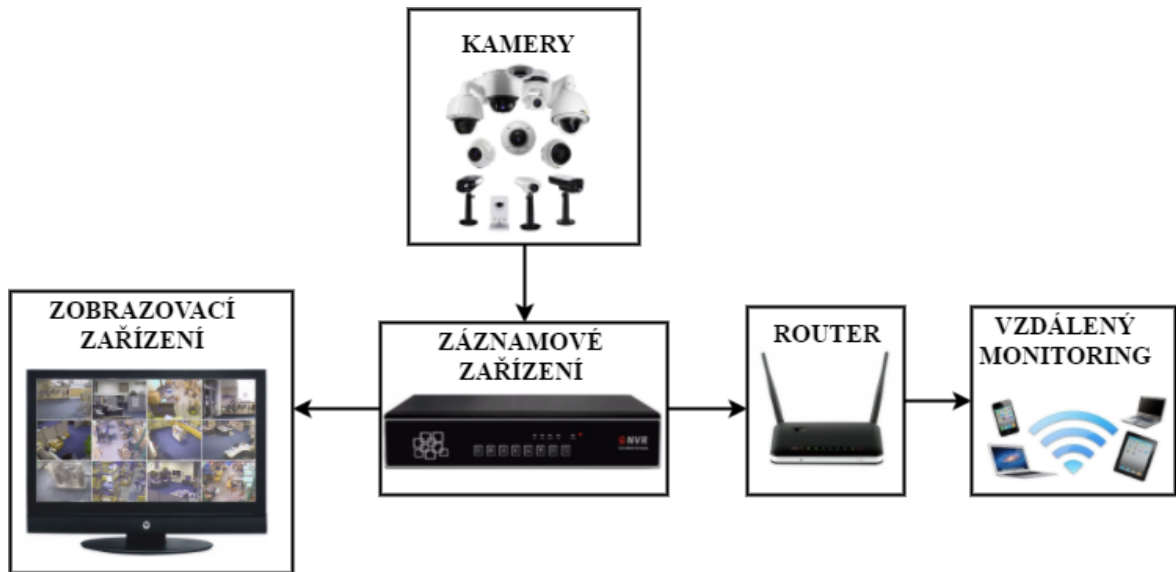
Obr. 5: Náhled do mobilní aplikace Můj Jablotron [12]

## 2.2 Dohledové videosystémy

Dohledové videosystémy slouží ke sledování prostor, zobrazování záběrů z jednotlivých kamer a následné archivování pořízených záběrů. [4]

Hlavními prvky video-dohledových systémů jsou:

- kamera,
- objektiv,
- záznamové zařízení,
- zobrazovací zařízení,
- přenosové médium,
- multiplexor, přepínač. [4]

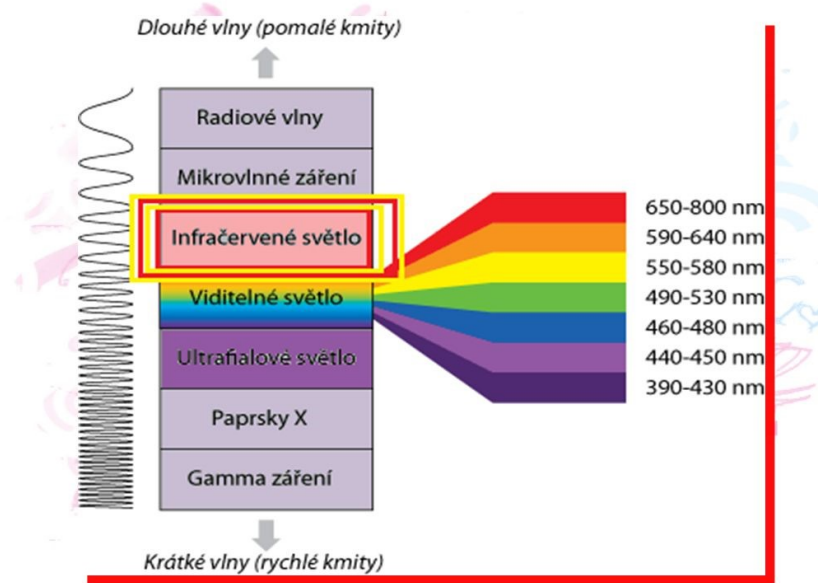


Obr. 6: Blokové schéma VSS [vlastní zdroj]

### 2.2.1 Termovizní kamery

Současným trendem jsou termovizní kamery, které se používají k ostraze objektů ve špatném počasí, v naprosté tmě nebo proti oslňujícímu slunci. Jsou schopné pracovat při velkém rozsahu operačních teplot, tj.  $-50^{\circ}$  až  $+70^{\circ}\text{C}$ . Stejně jako k rozpoznání člověka nebo motorového vozidla, mohou být aplikovány v oblasti požární bezpečnosti nebo při monitorování teploty sledovaných předmětů.

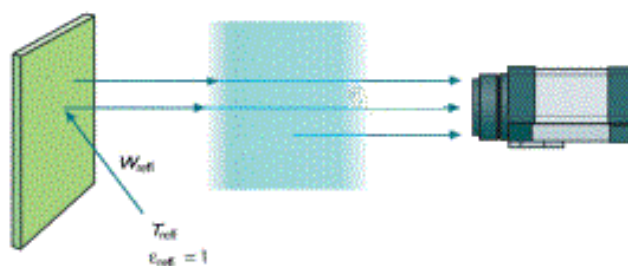
Princip fungování termovizní kamery využívá skutečnosti, že veškerá tělesa vyzařují elektromagnetické záření. Elektromagnetické spektrum je dle úmluvy rozděleno do několika kategorií, které se nazývají vlnová pásma, které se liší vlnovými délkami. [13] [14]



Obr. 7: Elektromagnetické spektrum vlnových délek [14]

Termografie využívá pásmo nazývajícím se tepelné neboli infračervené záření. Intenzita infračerveného záření je závislá teplotě povrchu objektu, který toto infračervené záření vyzařuje a na základě intenzity záření tedy lze určit povrchovou teplotu objektu.

Termovizní kamera ovšem nesnímá pouze záření odražené od objektu, ale také odražené záření z okolí na jeho povrch. Obě tato záření jsou částečně zeslabována prostředím mezi detektorem a měřeným objektem. Z toho plyne, že je nutné, aby systém termovizní kamery byl schopen korekce parametrů ovlivňující výsledný snímek. [13] [14]



Obr. 8: Schématické zobrazení snímání termovizní kamerou [14]

Pro bezpečnostní účely se využívá dlouhovlnných bezkontaktních systémů měření teploty s maticovým detektorem. Pořízený snímek z tohoto typu detektorů je sestavený z matice bodů o určité hodnotě, která je rovna teplotě vyzařované z daného místa měřeného objektu. [14] [15]



Obr. 9: Snímek z termovizní kamery [15]

Tyto termovizní detektory našly uplatnění nejen v průmyslu nebo stavebnictví při detekci úniků tepla, ale i v bezpečnostních oborech pro detekci osob za špatných světelných podmínek, zejména v noci. [14] [15]



Obr. 10: Kamera s termovizí [15]

### 2.2.2 Přisvit

Přisvit je využíván v aplikacích, kdy není ve sledovaném prostoru žádné osvětlení a je na systém požadavek na monitorování ve dne i v noci. Přisvícení scény může být ve viditelném nebo neviditelném spektru.

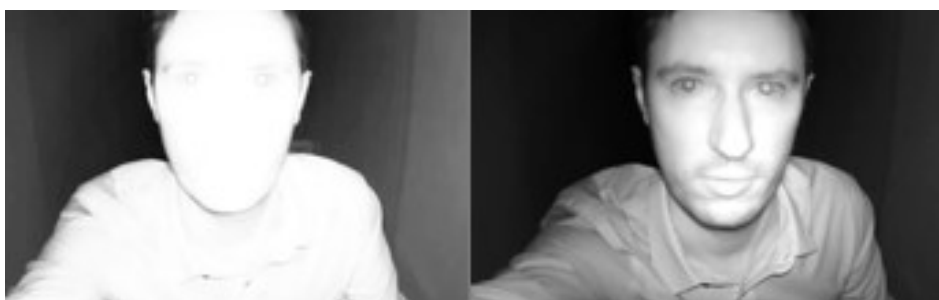
Pro přisvícení bezpečnostních kamer ve viditelném spektru lze použít libovolného světla, které odpovídá citlivosti kamer. K úspoře elektrické energie se využívá pohybového PIR spínače, který aktivuje přisvit pouze při detekování pohybu. V současnosti se nejvíce využívá jako zdroj světla LED světla, které vynikají nízkou spotřebou. [16]



### IR LED přísvit

Infračervený přísvit je pro lidské oko neviditelný, ovšem většina kamer je na tento typ světla citlivá. Kamerový systém je s IR přísvitem je schopný snímat i při naprosté tmě.

Inteligentní řízení nočního přisvícení využívající technologie Solid Light automaticky snižuje množství vyzařovaného světla přísvitem, nedochází tedy k přílišnému osvětlení a znehodnocení dat na snímané scéně. Solid Light technologie také umožňuje rovnoměrně nasvítit scénu infračerveným světlem, aby nedocházelo pouze osvětlení středové části snímaného prostoru a zkreslení obrazu. [16] [17]



Obr. 11: Rozdíl ve snímané scéně při použití technologie Solid Light (vpravo) [17]



Obr. 12: IR přísvit s technologií Solid Light [17]

### Laserový přísvit

Další možností, jak se vypořádat s obtížnými světlenými podmínkami je kromě výše zmíněného přísvitu pomocí infračerveného LED přísvitu a přirozeného viditelného světla je laserový přísvit. [16]

LASER (Laser Amplification by Stimulated Emission of Radiation), v překladu zkratkou pro zesilování světla stimulovanou emisí záření, je optický zdroj elektromagnetického záření, ve kterém je světlo vyzařováno pomocí úzkého svazku fotonů. Díky této vlastnosti laser

umožňuje vyzářit svazek světla na velkou vzdálenost s vysokou intenzitou, což je důležitou vlastností laserového přísvitů u bezpečnostních kamer. [16]



Obr. 13: Rozdíly mezi IR LED (vlevo) a laserovým (vpravo) přísvitem [16]

Z obrázku č. 13 je patrné, že IR LED je charakteristické bodovým přísvitem scény, přitom laserový přísvit je schopen scénu nasvítit rovnoměrněji a se širším světleným rozsahem. [16]

V následující tabulce jsou uvedeny rozdíly mezi IR LED a laserovým přísvitem.

Tab. 9: Rozdíly mezi IR LED a laserovým přísvitem [vlastní zdroj]

	<b>IR LED přísvit</b>	<b>Laserový přísvit</b>
<b>Dosah</b>	max. 300 m	jednotky až desítky km
<b>Rozměry</b>	pro vysoký výkon velké množství diod = nekompaktní rozměry	vysoký dosah a výkon při zachování kompaktních rozměrů

### 2.2.3 Moderní kompresní algoritmy

Kompresce videa slouží ke snížení objemu dat nebo datového toku při co nejnižší viditelné degradaci obrazu. Pro převod videa do různých komprimovaných formátů slouží kodek videa. V praxi nejpoužívanějším kodekem je H.264 a H.265. [17]

#### H.264

H.264 je standard pro bezztrátová komprese videa. Principem této komprese je, že se nejprve přenáší tzv. klíčový snímek, který je komprimován. Za ním následuje snímek, který pouze obsahuje rozdíl vůči klíčovému snímku. [17]

**H.265**

Novým nástupcem je standard H.265, který byl přijat v roce 2013, jehož účinnost je o 50 % vyšší než u standardu H.264. Dohledové videosystémy jsou schopné snímat obraz ve vysokém rozlišení, a proto je nutné silně komprimovat získaná data, ovšem to vede k silné degradaci kvality obrazu. Proto se začal používat kompresní standard H.265, který snížil objem dat bez ztráty kvality. [18]

H.265+ je speciální kompresní algoritmus vyvinutý společností Hikvision, který uvedl na trh Ultra HD bezpečnostní kameru. Vzhledem k vysokému rozlišení kamery bylo zapotřebí velká skladovací kapacita. Proto tato společnost vyvinula standard H.265+ vycházející ze standardu H.265. [18]

K zobrazení výhody standardu H.265+ slouží následující tabulka, která je sestavená na základě záběrů pořízených v rozlišení Full HD (1080 p) se 25 snímků za sekundu. [18]

Tab. 10: Porovnání klasických kompresních standardů s Hikvision 265+ [18]

		<b>Datový tok (kb/s)</b>		
<b>č.</b>	<b>Situace</b>	<b>H.264</b>	<b>H.265</b>	<b>H.265+</b>
<b>1</b>	kavárna, dostatečné osvětlení, mnoho pohybujících se objektů	3 481	1 843	650
<b>2</b>	kavárna, dostatečné osvětlení, několik pohybujících se objektů	2 253	1 289	340
<b>3</b>	kavárna, slabé osvětlení (s přísvitkem), bez pohybů	930	453	108
<b>4</b>	silnice, dostatečné osvětlení, mnoho pohybujících se objektů	4 403	2 154	970
<b>5</b>	silnice, dostatečné osvětlení, několik pohybujících se objektů	4 096	1 331	518
<b>6</b>	silnice, slabé osvětlení (s přísvitkem), bez pohybů	2 662	1 946	480

Z předchozí tabulky plyne, že kompresní algoritmy své uplatnění při zpracovávání obrazu rozhodně mají, ovšem při použití účinnějších kompresních algoritmů je nutnější i vyšší výpočetní výkon. Z tabulky lze také vyzorovat rozdíly v datových tocích, které nejsou kon-

stantní. Při minimálních nebo žádných pohybech ve snímané scéně je datový tok nízký, ponechává algoritmus si ponechává výchozí snímek a ukládá a zpracovává se pouze rozdíly vůči tomuto výchozího snímku. Ve scénách, ve kterých je mnoho pohybu, je tedy přirozeně vyšší datový tok. Množství zpracovávaných dat také ovlivňuje osvětlení dané scény. [18]

#### 2.2.4 Video-analytické funkce

Video-analytické a inteligentní funkce umožňují z velkého množství informací, které pořízené záznamy z dohledového videosystému obsahují, vybrat ty relevantní. Mezi nejčastěji využívané video analytické funkce patří: [19]

- detekce pohybu (pro snížení množství ukládaného videa),
- detekce manipulace s kamerou (použití v místech ohrožených vandalismem),
- rozpoznávání registračních značek automobilů,
- počítání osob (lze využít pro marketingové účely),
- počítání objektů překračující virtuální přímku,
- detekce objektů vstupujících nebo opouštějících oblast,
- detekce odstraněných objektů,
- detekce překročení čáry. [19]

Běžící analytické funkce zachycují podrobnosti o všech objektech, které se nachází v zájmovém prostoru. Na pozadí procesu analýzy systém zaznamenává a automaticky generuje tzv. metadata, což jsou jednoduché textové řetězce, které popisují detaily v obrazu. Metadata mohou obsahovat informace o osobách, objektech a jejich vzhledu nebo i registrační značky automobilů. [19]

Metadata jsou velkým přínosem při analyzování pořízených záběrů. Díky nim je možné nastavit podmínky a následující akce, např. při poplachu. [19]

#### 2.2.5 Širokoúhlé objektivy

Popularita širokoúhlých objektivů, také označovaných jako fish-eye, neustále roste. Kamery s objektivem fish-eye jsou schopny pokrýt prostor s širokým úhlem záběru ve vysokém rozlišení. Dříve u těchto typů kamer s objektivy fish-eye byly problémy s kvalitou obrazu, ovšem nové technologie tyto nedostatky odstranily a také přinesly snížení nákladů. Nedostatky PTZ kamer, které mají tendence být nasměrovány v nesprávný čas na nesprávné místo, tyto kamery odstraňují. [20]



Obr. 14: Pořízený záběr z kamery s objektivem fish-eye [20]

## DÍLČÍ ZÁVĚR

V kapitole byly popsány současné vývojové trendy v oblasti I&HAS a VSS.

### I&HAS

V oboru I&HAS byl vždy kladen důraz na minimalizaci planých poplachů. Veškeré detektory pracující na určitém fyzikálním principu jsou charakteristické i svými nevýhodami dané použitou technologií snímání. Aby bylo možné spolehlivě předejít planým poplachům, začaly se integrovat do jednoho pouzdra detektoru více snímacích prvků fungujících na odlišných fyzikálních principech. Kooperací dvou a více různých senzorů bylo dosaženo minimalizace planých poplachů.

Dalším trendem, daný vývojem zobrazovací techniky, je využívání dotykových panelů. Kvalitnější grafický výstup, intuitivní ovládání, uplatnění ve velkém množství aplikací a snižující se pořizovací náklady způsobilo čím dál častější využívání těchto zařízení.

Již dlouhodobým trendem v zabezpečovací technice je integrace I&HAS s dalšími systémy. Minimalizování provozních nákladů, automatizace procesů, možnost ovládání a správy poplachových i nepoplachových aplikací v jednom systému jsou hlavními motivačními členy.

Vzdálená správa, především pro domácnosti, je velmi pohodlným způsobem ovládání domácího zabezpečovacího systému umožňující na dálku ovládat, monitorovat a spravovat poplachové i nepoplachové aplikace.

### VSS

K vypořádání se s náročnými světelnými podmínkami se začaly využívat termovizní kamery, které jsou schopny spolehlivé funkce i v naprosté tmě.

V náročných světlených podmínkách lze videodohledové systémy využívat i s pomocí přísvitů. K přísvit lze využít bílého světla, infračerveného přísvitu pomocí IR LED nebo laserového přísvitu. Veškeré klady a zápory jednotlivých technologických provedení jsou v popsány výše v kapitole.

Zvyšováním rozlišení dohledových videosystémů jsou kladeny čím dál větší nároky na uložení. Proto je nutné veškeré pořízené snímky komprimovat, čímž dojde k razantnímu snížení velikosti souborů při zachování kvality. V současnosti nejpoužívanějším algoritmem je H.264, který začíná být pomalu nahrazován H.265 a jeho modifikacemi.

Vzhledem k velkému množství pořizovaných záběrů, zejména při využití VSS v rozsáhlých aplikacích, naleznou video-analytické funkce své uplatnění. S využitím metadat, lze ukládat informace i o identifikačních značkách automobilů, k verifikaci obličejů s využitím přístupových systémů a mnoha dalších rozmanitých aplikací.

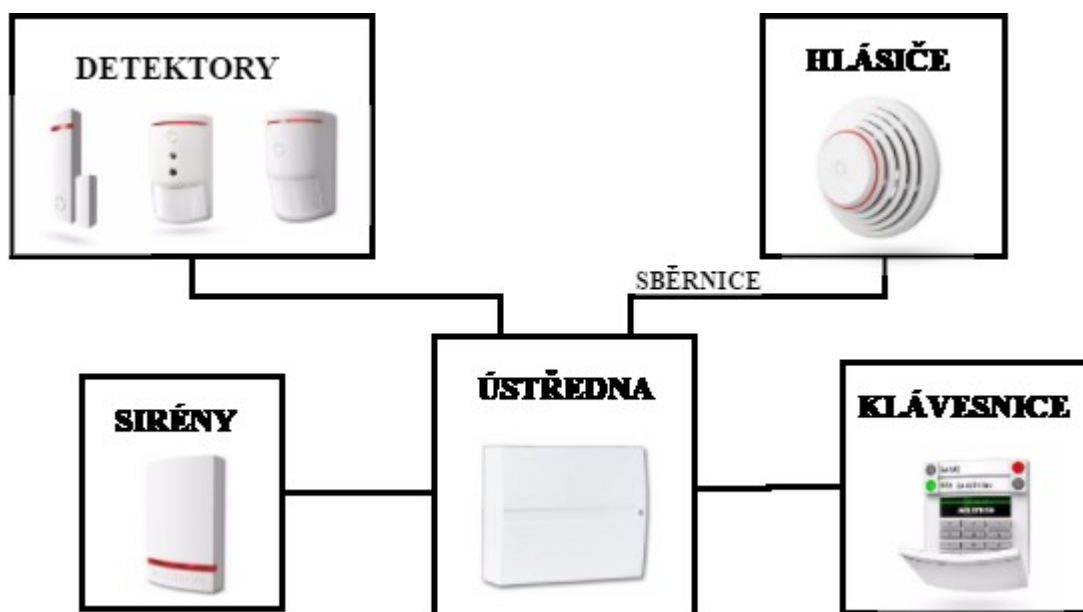
Širokoúhlé objektivy naleznou své uplatnění při zabezpečení prostor, kde lze minimalizovat náklady nahrazením více videodohledových systémů jedním se širokoúhlým objektivem, tzv. fish-eye.

### 3 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY A JEJICH FUNKČNÍ VLASTNOSTI

Poplachové zabezpečovací a tísňové systémy slouží k signalizaci nebezpečí ve střeženém prostoru. Slouží k informování obsluhy o vniknutí do objektu. [2]

Komponenty I&HAS jsou následující:

- detektorů narušení,
- hlásiče,
- ústředny,
- přenosová zařízení,
- ovládací zařízení,
- signalizační zařízení. [2]



Obr. 15: Blokové schéma I&HAS [vlastní zdroj]

#### 3.1 Ústředny

Ústředna I&HAS je řídicí jednotkou, která komunikuje s dalšími připojenými prvky, jako jsou zejména detektory. Získaná data z detektorů vyhodnocuje a informuje uživatele o probíhajících událostech, např. o poplachu, poruše nebo sabotáži. [21]

Hlavními funkcemi ústředny jsou:

- příjem, zpracování a následné vyhodnocení signálů z připojených detektorů;



- napájení detektorů a dalších připojených zařízení (pouze u drátového spojení);
- uvádění stavů do střežení a klidu;
- diagnostické funkce. [21]

Ústředna v reálném čase vyhodnocuje stavy z drátově nebo bezdrátově připojených detektorů. Pokud je zjištěno vniknutí do chráněných prostor, je ústřednou vyhlášen poplach. Tento stav je signalizován indikačními zařízeními, např. sirénou. Dále může stavové hlášení být distribuováno uživateli na mobilní telefon v rámci sítě GSM, na připojené dohledové poplachové a přijímací centrum (DPPC), atd. [21]

Další funkce ústředny jsou realizovány prostřednictvím programovatelných výstupů PGM. Ty umožňují na základě snímaných veličin zprostředkovat určitou událost, v oblasti poplachových i nepoplachových aplikací (klimatizace, větrání, osvětlení apod.). [21]

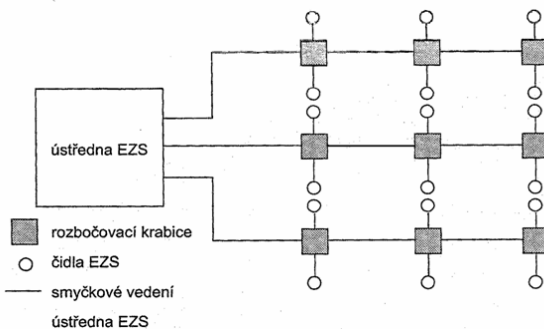
Dále ústředna disponuje pomocnými zvukovými výstupy, které je možné využít ke zvukové indikaci stavů, například otevření dveří, poklesu napětí baterie zařízení u bezdrátových systémů apod. [21]

Ústředny z hlediska propojení s detektory a tísňovými hlásiči lze dělit následovně:

- ústředny smyčkové,
- ústředny s přímou adresací detektorů,
- ústředny smíšené,
- ústředny bezdrátovou komunikací. [21]

### 3.1.1 Ústředny smyčkové

Ústředny smyčkové používají k propojení s detektory a tísňovými hlásiči proudové smyčky, z nichž každá je připojena na samostatný vyhodnocovací obvod se zakončovacím odporem. Při změně odporu ve smyčce dojde k aktivaci poplachu. Smyčky jsou nejčastěji tvořeny sériovým zapojením jednotlivých zařízení. [21]



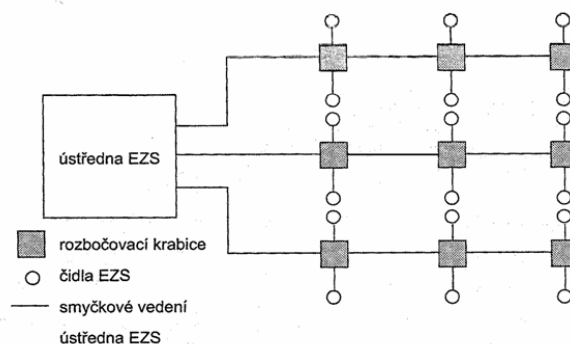
Obr. 16: Blokové schéma smyčkové ústředny [21]

### 3.1.2 Ústředny s přímou adresací detektorů

Ústředny s přímou adresací detektorů používají ke komunikaci sběrnici v časovém nebo frekvenčním režimu. Komunikace probíhá digitálně, každé zařízení musí tedy mít komunikátor s vlastní adresou k určení, který detektor zaznamenal narušení v chráněném prostoru.

Ústředny s přímou adresací detektorů mají v porovnání s ústřednou se smyčkovým zapojením minimální kabeláž. Kromě vyvolání poplachu mohou jednotlivé detektory hlásit ústředně i další stavy, jako jsou např. sabotáž, zkrat na lince, nebo indikace zakrytí detektoru.

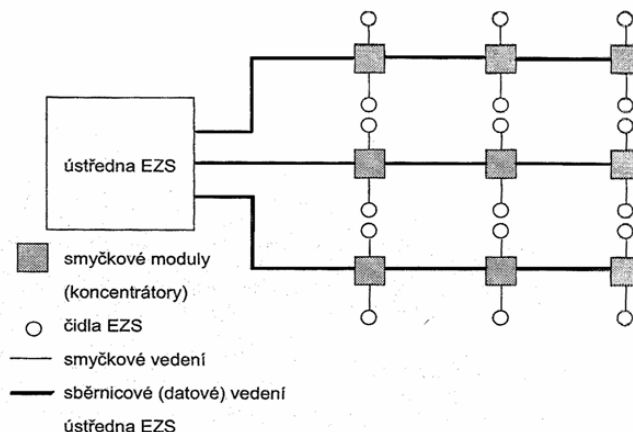
[21]



Obr. 17: Blokované schéma ústředny s přímou adresací detektorů [21]

### 3.1.3 Ústředny smíšené

Ústředny smíšené používají ke komunikaci s připojenými zařízeními koncentrátor, která může probíhat analogově i digitálně. Na koncentrátory mohou být smyčkově připojeny detektory, i detektory s přímou adresací. U tohoto typu zapojení se tedy kombinují oba předešlé způsoby připojení zařízení. [21]



Obr. 18: Blokované schéma smíšeného typu ústředny [21]

### 3.1.4 Ústředny s bezdrátovou komunikací

U ústředny s bezdrátovou připojením probíhá komunikace v pásmu 433MHz nebo 868MHz. Dosah ve volném prostředí se pohybuje mezi 100–200 m, ovšem v objektu je tato vzdálenost razantně snížena. Jednotlivé detektory k napájení elektrickou energií vyžadují vlastní baterii. Blížící se konec životnosti baterie bývá indikován poklesem napětí, který je signalizován ústředně. [21]

Bezdrátová komunikace s připojenými zařízeními může probíhat dvěma způsoby.

#### Jednosměrná komunikace

V systémech s jednosměrnou komunikací zajímá ústředna roli přijímače a detektory vysílače. Detektory periodicky vysílají kontrolní telegramy ústředně. Velkým problémem těchto systémů je rozpor mezi požadavkem na co nejvyšší četnost kontrol a na výdrž baterií detektorů. V praxi je kontrola prováděna jednou za několik hodin. Pokud je detektor poškozen, odcizen nebo dojde k jakékoliv disfunkci, ústředna se dozví o této skutečnosti s určitou odezvou. Proto se častěji využívá systémů s obousměrnou komunikací. [21]

#### Obousměrná komunikace

Ústředna i prvky systému jsou vybaveny přijímací i vysílací elektronikou. Obousměrná komunikace tedy odstraňuje nedostatky systémů s jednosměrnou komunikací. [21]

Hlavní funkce systému s obousměrnou komunikací jsou následující:

- ověření stavu všech prvků při zapnutí systému,
- v klidovém stavu detektory nevysílají, a neplývají tedy energií,
- při rušení komunikace dojde k automatickému přeladění na jinou frekvenci,
- dálkový test funkčnosti. [21]

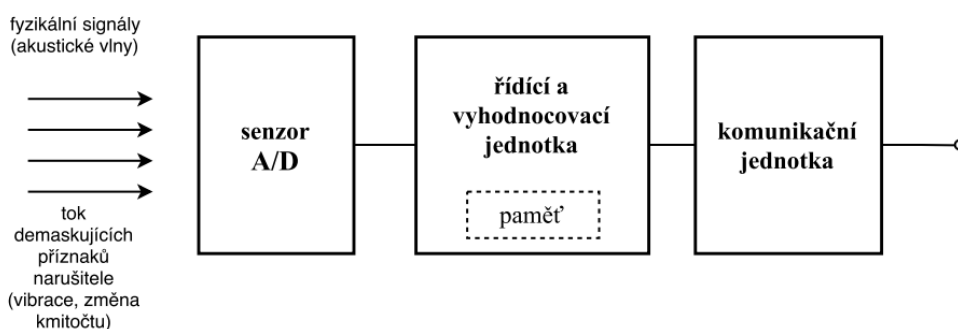
Mezi velké výhody bezdrátových systémů patří především rychlost a jednoduchost instalace. Vzhledem k absenci kabeláže, která by jinak musela být v hotovém objektu vysekána do zdi nebo jiným stavebním zásahem instalována, je velmi jednoduché bezdrátové systémy již do hotových objektů. [21]

## 3.2 Detektory narušení

V této části kapitoly budou popsány funkční vlastnosti detektorů narušení. V publikaci Bezpečnostní technologie, systémy a management I. se detektory narušení popisují následovně:

Úkolem detektorů narušení je detekovat neoprávněné vniknutí narušitele do střeženého prostoru. Detektor je definován jako zařízení zkonstruované ke generování signálu nebo zprávy o vniknutí, jako reakci na nenormální stav detekující přítomnost nebezpečí. Detektor narušení (dříve označovaný také jako čidlo) představuje zařízení bezprostředně reagující na fyzikální jevy (změny), související s narušením střeženého prostoru narušitelem. Detekce stavu narušení vyvolává v detektoru vyslání poplachového signálu, zprávy. [22]

Na následujícím obrázku je uvedeno blokové schéma detektoru narušení:

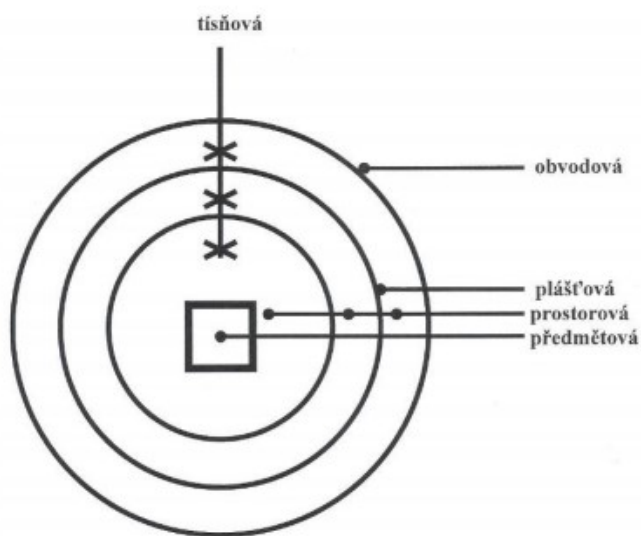


Obr. 19: Blokové schéma detektorů narušení [22]

Technická ochrana se člení do čtyř následujících částí:

- perimetrická,
- obvodová,
- plášťová,
- předmětová. [22]

Rozdělení lze vidět na Obr. 21, Jednotlivé části jsou ještě doplněny o tísňovou ochranu, která slouží k manuální aktivaci vyhlášení poplachu.



Obr. 20: Rozdělení technické ochrany [23]

### 3.2.1 Detektory obvodové ochrany

Detektory pro obvodovou neboli perimetrickou ochranu slouží k detekci narušení ve vnějších částech budov. Riziko planých poplachů ve vnějším prostředí je velké. Detektory musí být imunní vůči značnému množství podnětů, jako jsou především:

- proudění vzduchu,
- vítr,
- sníh,
- déšť,
- pohyb zvíře,
- pohyb rostlinstva,
- dopravní ruch. [22] [23]

Při návrhu je důležité vzít v úvahu všechny negativně ovlivňující faktory, které mohou ovlivnit funkci detektoru perimetrické ochrany. Základním znakem detektorů perimetrické ochrany je, že jejich detekční charakteristika dosahuje vzdálenost 100–500 m. [22] [23]

Z důvodu pravděpodobnosti planých poplachů se často prvky perimetrické ochrany kombinují s video-dohledovým systémem. [22] [23]

*„Ochrana důležitých objektů s vysokým rizikem nebo objektů, na které hrozí při útoku vysoká škoda – tzv. objekty zvláštní důležitosti, kterými jsou například sklady hmotných rezerv*

*státu, sklady zbraní a střeliva, mezi národní letiště a podobně, je charakteristická použitím perimetrické ochrany.“ [22]*

Jedná se o první překážku případným pachatelům, jehož hlavní funkcí je odhalení a odstranění narušitele.

### **Infračervené bariéry a závory**

Infračervené bariéry a závory jsou častým prvkem perimetrické ochrany. Skládají se z vysílací a přijímací částí, které mezi sebou vyzařují infračervené paprsky. Při přerušení paprsků dojde k vyvolání poplachového stavu. Efektivní maximální dosah infračervených paprsků se pohybuje mezi 150–200 m, proto tento systém perimetrické ochrany nalezne uplatnění zejména na rozsáhlých pozemcích. [22] [23]

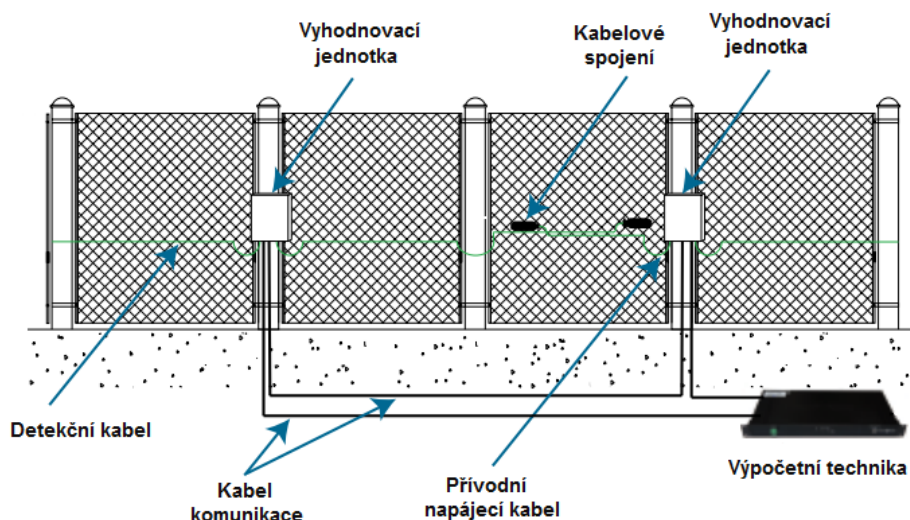
Podmínkou funkce je přímá viditelnost vysílací a přijímací části. Dále je důležité vhodně nastavit citlivost přijímací části, aby nedocházelo při horších povětrnostních podmínkách (děšť, sníh, mlha) k vyvolání planého poplachů. [22] [23]



Obr. 21: Zobrazení funkce infračervených bariér [22]

### **Mikrofonické kabely**

Mikrofonické kabely snímají namáhání a záchvěvy, které se převádějí na elektrický signál. K vyhodnocovací jednotce je možné připojit reproduktor pro akustický odposlech, čímž uživatel může snadněji určit charakter vlivu působící na mikrofonický kabel. Montují se přímo na oplocení a používají se pro detekci překonávání bariér obvodové ochrany. [22] [23]



Obr. 22: Zobrazení zapojení mikrofonických kabelů [24]

### Mikrovlnné bariéry

Mikrovlnné detektory využívají principu Dopplerova jevu. Vyzářují do prostředí vysoko-frekvenční signál, který se odrazí zpět a je vyhodnocován při změnách signálu. [22] [23]

Mikrovlnné detektory mají dosah až 300 m, a při použití více detektorů se mohou jejich pole překrývat, čímž se eliminují mrtvé zóny. [22] [23]

### Štěrbinové kabely

K vytvoření štěrbinových kabelů jsou použity koaxiální kabely, ve kterých je vytvořena vzduchová štěrбина. Vzduchovou štěrbinou je vyzářován vysokofrekvenční signál, který přijímací kabel vyhodnocuje. Při změně v signálu je vyhlášen poplach. Hlavní výhodou štěrbinových kabelů spočívá v jejich skryté montáži. [22] [23]

### Kapacitní kabely

Kapacitní kabely využívají ke své činnosti vlastností kondenzátoru. Mezi elektrodami vzniká elektrostatické pole, kde jako dielektrikum slouží vzduch. Pokud vnikne narušitel do prostoru mezi elektrodami (dielektrikum), dojde ke změně v elektrostatické pole, změní se tedy kapacita a dojde k vyhlášení poplachového stavu. [22] [23]

Kapacitní kabely bývají instalovány na ploty. Velkým problémem kapacitních kabelů jsou falešné poplavy, poněvadž jsou citlivé na pohyby pletiva při působení větru. [22] [23]

### Perimetrické pasivní infračervené detektory

Princip funkce je obdobný jako u PIR detektorů pro vnitřní použití, pouze jsou použity složitější vyhodnocovací obvody, jiná optika a odolná konstrukce proti povětrnostním vlivům. Často se používají jako doplněk k dohledovým videosystémům. [22]

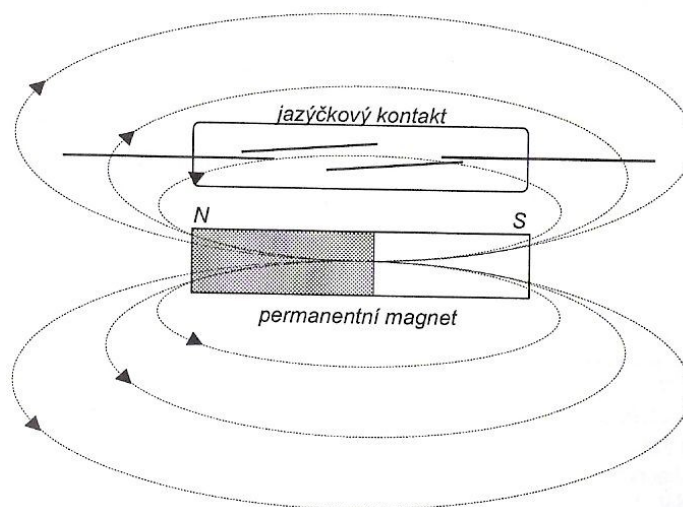
### 3.2.2 Detektory plášťové ochrany

Úkolem detektorů plášťové ochrany je signalizace narušení pláště chráněného objektu. Jedná se především o otvorové výplně (dveře, okna, balkonové dveře atd.), ale také o obvodové zdivo, střechy aj. [23]

*„Cílem plášťové ochrany je odstrašení, znemožnění průchodu, zpoždění a odhalení narušitele. Plášťová ochrana signalizuje narušení pláště budovy. Plášťovou ochranu tvoří stěny, okna, dveře, zámky a zámkové systémy, mříže, bezpečnostní fólie, kamerové systémy, detektory narušení atd. Detekční prvky plášťové ochrany se zpravidla umísťují zevnitř budovy.“*  
[22]

### Magnetické detektory

Magnetické detektory se označují jako pasivní, poněvadž nemají žádný vyhodnocovací obvod. Hlavním prvkem magnetického detektoru je jazýčkové relé, které je složeno z elektromagnetického materiálu. V klidovém stavu je jazýčkové relé drženo v sepnutém stavu přiloženým statickým magnetem, který je instalován na pohyblivé části – dveře, okenní křídla apod. Pokud dojde k otevření dveří, dojde k rozepnutí relé a k vyhlášení poplachového stavu. [22] [23]



Obr. 23: Zobrazení principu funkce magnetického detektoru [23]



Velkou výhodou magnetických detektorů je jejich vysoká spolehlivost, odolnost a jednoduchost montáže, ovšem je nutností instalace na každé okno nebo dveře. [22] [23]

### **Detektory na ochranu skleněných ploch**

Detektory na ochranu skleněných ploch se dělí na:

- kontaktní,
- bezkontaktní.

Kontaktní detektory tříštění skla využívají vlnění, které se při narušení šíří skleněnou plochou. Instalují se na okno, na plochu skla. Při narušení skleněné plochy je vlnění vyhodnoceno a je vyhlášen poplachový stav. [22]

Bezkontaktní detektory na ochranu skleněných ploch využívají charakteristického zvuku, který vydává tříštící se sklo. Zvuk je zaznamenáván elektretovým mikrofonem a o poplachovém stavu je rozhodnuto vyhodnocovacím obvodem. Obvykle doplňují magnetické kontakty, ale mohou pracovat i samostatně. [22]

Detektory destrukce skla se využívají k ochraně výkladních skříní, reklamních výloh, vitrín, a podobně.

### **Poplachové fólie, polepy, tapety**

Uvedené detektory se skládají s fólie ve které je umístěn jemný vodič. Při přerušení tohoto vodiče dojde k vyvolání poplachového stavu. [22]

### **3.2.3 Detektory prostorové ochrany**

Prostorová ochrana vhodně doplňuje velmi vhodnou formu střežení, kterou je plášt'ová ochrana. Prvky prostorové ochrany se umísťují do přístupů či vstupů, do hal, spojovacích chodeb a dalších propojovacích komunikačních uzlů budovy. [23]

Knižní publikace Bezpečnostní technologie, systémy a management I. popisuje detektory prostorové ochrany následovně:

*„Cílem prostorové ochrany je zpoždění a odhalení pohybu narušitele uvnitř střežené budovy. Opatření prostorové ochrany jsou realizována ve vnitřních prostorách budovy, zpravidla na chodbách, schodištích a místnostech. Prostorovou ochranu tvoří dveře, mříže, zámky a zámkové systémy, kamerové systémy, systémy kontroly vstupu a poplachové zabezpečovací systémy s detektory narušení. Detektory narušení by měly v rámci prostorové ochrany signalizovat vniknutí do vnitřních prostor budovy.“ [22]*

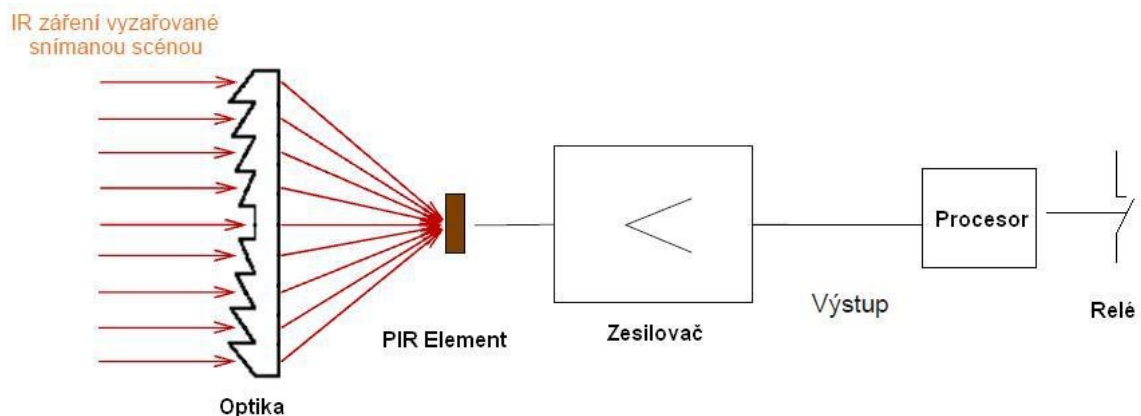
### Pasivní infračervené detektory

Pasivní infračervené detektory, označované jako PIR detektory (Passive Infra Red), jsou založeny na vyhodnocování změn vyzařování v infračerveném pásmu elektromagnetického vlnění. Základním prvkem je pyroelement, což je snímač se schopností detekce změny záření dopadající na detektor. Změny v záření jsou způsobeny pohybem osob v zorném poli detektoru. [22]

PIR detektory jsou nejrozšířenějším druhem detektorů, což je způsobeno především díky relativně nízkým pořizovacím nákladům. Detektory fungující na tomto principu se využívají nejen v oblasti prostorové ochrany, ale také v oblasti ochrany perimetrické. [22]

Při návrhu zabezpečení objektu je nutné dbát na následující vlivy, které mohou ovlivnit funkci PIR detektoru a vyvolat planý poplach:

- činnost ventilace,
- rychlé změny teploty,
- volně zavěšené předměty,
- poryvy větru,
- světla automobilů. [23]



Obr. 24: Blokové schéma funkce a zapojení PIR detektorů narušení [22]

### Ultrazvukové detektory

Ultrazvukové detektory patří do skupiny elektroakustických detektorů narušení. Fungují na principu Dopplerova jevu. Vysílají do prostoru ultrazvukové vlnění, které je nad pásmem

slyšitelných kmitočtů lidským uchem. Přijímací část detektoru snímá odražené vlnění, v případě narušení prostoru dojde ke změnám v přijímaném vlnění a dojde k vyvolání poplachového stavu. [22]

Při návrhu zabezpečení prostor je nutné dbát na následující vlivy, které mohou ovlivnit funkci ultrazvukového detektoru a vyvolat planý poplach: [22]

- častá změna interiéru,
- klimatizace,
- ventilace,
- teplotní poryvy,
- potrubí s proudící párou,
- předměty s možností pohybu,
- vibrace způsobující zvuky ve vysokém frekvenčním spektru,
- vzájemné rušení při instalaci více ultrazvukových detektorů. [22]

Dalšími faktory, které mohou způsobit snížení účinnosti detektorů, je použití materiálu absorbující zvuk, mezi které patří především koberce, pěnové materiály, textilní nábytek apod.), což může snížit dosah detektoru. [22]

Výše uvedené možnosti negativního ovlivnění funkce ultrazvukových detektorů způsobily, že se tyto detektory již téměř nepoužívají.

### **Mikrovlnné detektory**

Princip mikrovlnných detektorů je shodný s principem ultrazvukových detektorů, ale jejich kmitočtové pásmo se pohybuje v pásmu elektromagnetického vlnění, na frekvencích 2,5 GHz, 10 GHz nebo 24 GHz. [22]

Důležitou vlastností tohoto typu záření je jejich schopnost projít skrz pevné překážky, proto je nutné nastavení citlivosti a dosahu. [22]

Vlivy, které mohou mít vliv na mikrovlnné detektory jsou následující:

- voda v potrubí,
- kovové materiály
- pohybující se předměty,
- rušení zářivkami. [22]

### **Kombinované detektory**

Výše uvedené prostorové detektory narušení disponují určitými nevýhodami. Tyto nevýhody lze odstranit použitím kombinace dvou a více způsobů detekce pohybu v jednom detektoru. Nejčastěji se lze setkat s kombinací PIR a MW detektorů. [22]

Vyhlášení poplachu u tohoto typu detektorů probíhá až pokud obě vyhodnocovací jednotky v nastaveném časovém intervalu detekují změny v jejich zorném poli. [22]

Kombinované neboli duální detektory se instalují především v prostorech s teplotní nestabilitou. [22]

#### **3.2.4 Detektory předmětové ochrany**

Detektory předmětové ochrany slouží ke střežení cenných předmětů. Jsou určeny především ke střežení předmětů i v době, kdy jsou prostorové detektory pohybu z důvodu provozu v zájmovém prostoru vypnuta. [23]

Knižní publikace Bezpečnostní technologie systémy a management I. popisuje detektory předmětové ochrany následovně:

*„Předmětovou ochranu tvoří opatření vedoucí k zamezení zcizení a neoprávněné manipulaci s chráněnými aktivy. Chráněnými aktivy jsou obvykle cenné umělecké předměty, patentově chráněné vzory a další, z jakéhokoliv důvodu cenné, fyzické předměty (objekty). Předmětovou ochranu tvoří vitríny, skleněné tabule, kamerové systém a poplachové zabezpečovací systémy.“* [22]

#### **Otřesové detektory**

Snímají vlnění šířící se pevnými tělesy při jejich mechanickém namáhání. Využívají se pro střežení trezorů, trezorových místností atd. [23]

#### **Závěsové detektory**

Principem závěsových detektorů je zavěšení chráněného předmětu na drát, na jehož konci je vyhodnocovací jednotka. Při manipulaci se střeženým předmětem dojde k vyhlášení poplachu. [23]

### Váhové detektory

Váhové detektory slouží ke střežení nejčastěji uměleckých předmětů, jakými jsou hlavně obrazy a tapiserie. Detektor čítá hmotnost zavěšeného předmětu, a tím dokáže detekovat jeho manipulaci. [23]

### 3.3 Klávesnice

Klávesnice slouží jako ovládací zařízení I&HAS. Slouží k uvádění systému do stavu střežení nebo stavu klidu. Obsluha dále může klávesnici použít k servisním účelům, resetování poplachů nebo dalších základních i nadstandardních funkcí. Pomocí klávesnice lze ovládat jak poplachové, tak i nepoplachové aplikace (klimatizace, ventilace, osvětlení, a podobně). [22]

Klasické klávesnice skládající se z tlačítek a popřípadě malého displeje jsou v některých aplikacích často nahrazovány plně dotykovými panely. K ovládání systému lze využít uživatelský kód, který lze nahradit bezdrátovou klíčenkou nebo kartou a biometrickými funkcemi. [22]



Obr. 25: Ovládací panel od firmy Honeywell [25]

### 3.4 Signalizační zařízení

Signalizační zařízení slouží k upozornění na poplachový stav. Opticky a obvykle i akusticky informují obsluhu o vzniklé poplachu a obvykle fungují i jako odstrašovací činitel vůči narušiteli. [23]



Obr. 26: Prvky signalizačních zařízení [26]

### 3.5 Prvky tísňové ochrany

Prvky tísňové ochrany slouží k ochraně zaměstnanců a veřejnosti v případě přímého ohrožení. Hlášení může být vyvoláno manuální aktivací nebo zprostředkovaně předem nadefinovaným postupem. U těchto prvků riziko vyvolání planého poplachu je raritní. Většinou bývá vyvoláno v případě, že je nesprávně umístěno a dojde k nechtěné aktivaci, nebo neznalostí a zanedbáním. [23]

#### 3.5.1 Veřejné tísňové hlásiče

Veřejné tísňové hlásiče představují prvek, který slouží personálu i veřejnosti k vyvolání tísňového hlášení. Umísťují se na viditelných místech v objektu. Obvykle jsou chráněny sklíčkem, které zamezují náhodné použití nebo zneužití. [23]

#### 3.5.2 Skryté tísňové hlásiče

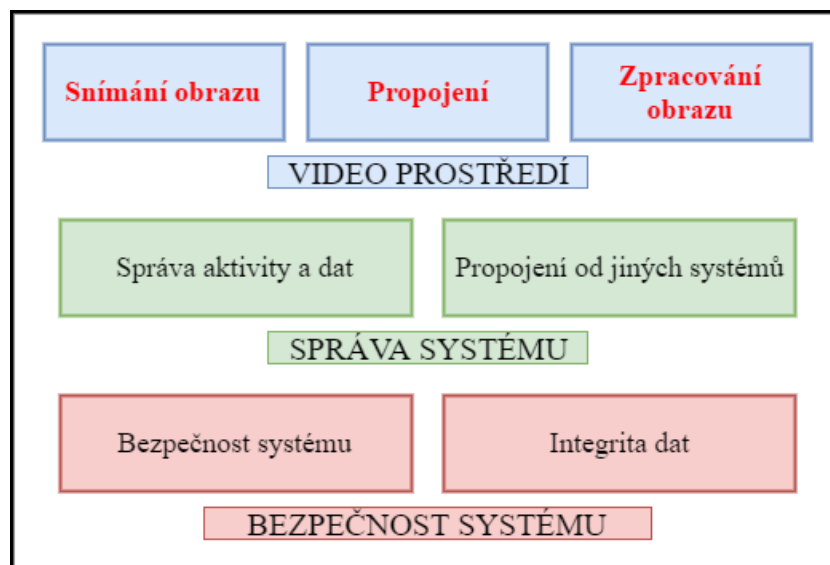
Skryté tísňové hlásiče, někdy označované i jako speciální tísňové hlásiče, slouží k nepozorovanému hlášení v případě přímého ohrožení. Je nutné dbát na správné umístění hlásiče, protože nedisponují ochranou před nechtěným vyhlášením poplachu. Hlásič tedy musí být neustále přístupný, ale nesmí být v dohledu cizích osob. [23]

## 4 VIDEODOHLEDOVÉ SYSTÉMY A JEJICH FUNKČNÍ VLASTNOSTI

Videodohledové systémy jsou v současnosti nepostradatelnou součástí komplexních zabezpečovacích systémů sloužící k ochraně osob a majetku. Systémy kontroly vstupu, požární signalizace, poplachový tísňový a zabezpečovací systém a dohledový videosystém často tvoří jeden sofistikovaný fungující celek. [11]

Technická norma ČSN EN 62676-1-1 (Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně) znázorňuje funkční bloky představující jednotlivé části systému a jejich funkce. Vzhledem k náplni a cíli diplomové práce jsou nejdůležitějšími bloky k vysvětlení podstaty problematiky části:

- snímání obrazu,
- vzájemná propojení,
- zpracování obrazu. [4]

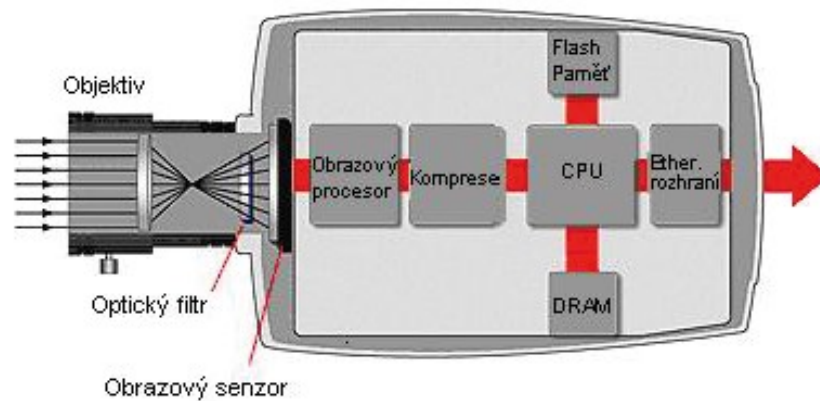


Obr. 27: Funkce VSS [4, vlastní zpracování]

### 4.1 Snímání obrazu

Cílem snímání obrazu je generovat data, který dodá informace o reálném světě.

VSS generuje obraz, který se později zpracovává. Vytváří se obrazová data, která jsou dále určena ke zpracování pomocí vzájemného propojení. [27]



Obr. 28: Princip snímání IP kamery [27]

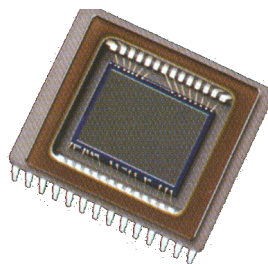
#### 4.1.1 Snímací čip

Základním prvkem každého IP dohledového videosystému je senzor, který společně s mnoha dalšími prvky určuje výslednou kvalitu obrazu. Na trhu se od různých výrobců lze setkat s různými označeními snímacích senzorů, ovšem všechny vychází ze dvou základních typů – CCD a CMOS. [28]

##### CCD

CCD (Charge Coupled Device) senzory se ke snímání obrazu se využívají již desítky let a jedná se tedy o propracovanou technologii. Čip z několika na světlo citlivých buněk (pixelů), na které dopadá světlo. Na základě množství dopadaného světla se produkuje odpovídající množství elektrické energie. Obsah senzoru se vyčítá sekvenčně a jelikož se jedná o analogová data, musí projít přes zesilovač do A/D převodníku, jehož výstupem jsou digitální data. [28]

Vzhledem k tomu, že zesilovač i A/D převodník není součástí samotného čipu, výkon a kvalita obrazu je vysoká, ovšem v porovnání s CMOS čipem, CCD čip vykazuje až 100x vyšší spotřebu energie. [28]



Obr. 29: Ukázka CCD čipu [28]



## CMOS

V čipu CMOS (Complementary Metal-Oxide Semiconductor) je veškerá elektronika integrována v samotném čipu. CMOS čipy mají na každém pixelu vlastní tranzistor (zesilovač), který zesiluje elektrický náboj. Daná technologie umožňuje vyrobit CMOS čip s vyšší hustotou pixelů, než je to možné u CCD čipů. CMOS senzory poskytují již digitalizovaný signál, což umožňuje jednodušší konstrukci kamery. Jejich spotřeba energie je také velmi nízká. [28]

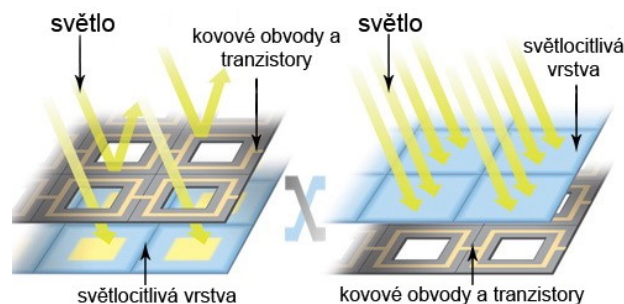


Obr. 30: Ukázka CMOS čipu [28]

## BSI CMOS

BSI CMOS je označován jako nový typ CMOS čipu. Konvenční CMOS snímače využívají tzv. čelního osvětlení, ve kterém jsou veškeré zesilovače a obvody umístěny nad světlo citlivou vrstvou, na které dopadá světlo. Tyto obvody zmenšují světlo citlivou plochu a část světla odráží zpět. Všechna tato negativa odstraňuje BSI (backside-illumination) CMOS. Zesilovače a obvody jsou u této technologie umístěny až pod světlo citlivou vrstvou, tedy světlo není zbytečně pohlcováno nebo odráženo zpět. [29]

Ovšem přemístění vrstvy citlivé na světlo a vrstvy se zesilovači a obvody zapříčinilo vyšší šum. Výhodou je vyšší rychlost, citlivost, menší rozměry čipu a nižší náklady na výrobu. [29]



Obr. 31: Ukázka uspořádání struktur CMOS (vlevo) a BSI CMOS (vpravo) [29]

## Shrnutí

V následující tabulce je uvedeno porovnání jednotlivé technologií čipů používané ve dohledových videosystémech.

	<b>CCD</b>	<b>CMOS</b>	<b>BSI CMOS</b>
<b>Světelná citlivost</b>	<b>vysoká</b>	nízká	<b>vysoká</b>
<b>Rychlost</b>	pomalá	<b>velmi vysoká</b>	<b>velmi vysoká</b>
<b>Rozměry</b>	velké	<b>malé</b>	<b>malé</b>
<b>Spotřeba</b>	100x vyšší	<b>nízká</b>	<b>nízká</b>
<b>Šum</b>	<b>nízký</b>	střední	vysoký
<b>Cena</b>	vysoká	<b>velmi nízká</b>	<b>nízká</b>

Tab. 11: Porovnání technologií čipů CCD, CMOS a BSI CMOS [29]

### 4.1.2 Objektiv

Objektiv je nedílnou součástí každého dohledového videosystému. Volí se na základě podmínek požadované aplikace. [30]

#### Formát objektivu

Formát objektivu se udává v palcích. Tato hodnota reprezentuje velikost snímacího čipu kamery, pro který je spočtena ohnisková vzdálenost objektivu. [30]

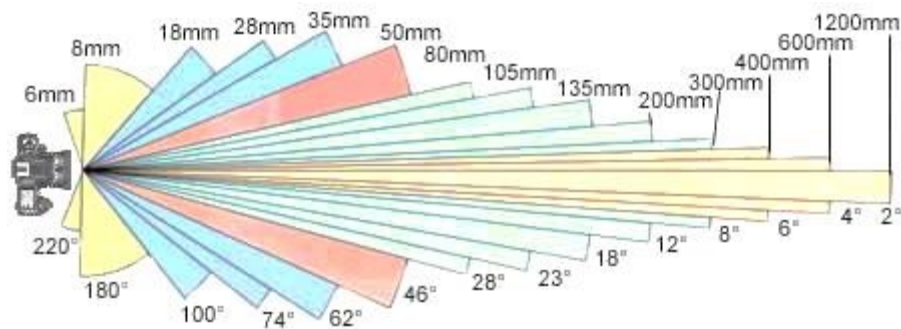
Nejčastěji se lze setkat s údaji:

- 1/3“,
- 1/2“,
- 2/3“,
- 1“. [30]

Formát objektivu by neměl být menší, než je formát snímacího čipu, poněvadž by okraje obrazu zůstaly nezobrazeny. Objektiv by nebyl schopen paprsky světla zaostřit na celou plochu snímacího čipu. [30]

#### Ohnisková vzdálenost

Ohnisková vzdálenost se udává v milimetrech. Je to pomyslná vzdálenost mezi středem objektivu a rovinou, na které objektiv dokáže zaostřit snímáný objekt.



Obr. 32: Ovlivnění šířky úhlu záběru změnou ohniskové vzdálenosti [30]

Platí tedy, že čím je ohnisková vzdálenost kratší, tím je širší úhel záběru objektivu.

### Světelnost objektivu a clona

Světelnost objektivu se udává poměrem ohniskové vzdálenosti k průměru vstupní pupily. Vyjadřuje kolik světla je maximálně objektiv schopen propustit. Je udávána bezrozměrným clonovým číslem. Platí pravidlo, že čím je clonové číslo menší, tím více světla dopadá na snímací čip. [30]

Clona slouží k regulaci světla procházejícího objektivem. Je to mechanické zařízení složené z kovových lamel tvořící prstenec, který lze otevírat nebo uzavírat a tím regulovat procházené světlo. Velikost clony také ovlivňuje kvalitu výsledného obrazu. [30]

U dohledových videosystémů se lze setkat s objektivy, které mají ručně nastavitelnou clonu nebo je automaticky řízená, popřípadě nemají žádnou. [30]

### Automaticky řízená clona P-Iris

P-Iris je typ objektivu, který má automaticky řízenou clonu. Díky této technologii lze precizně nastavit požadované clonové číslo, tedy optimalizovat kvalitu obrazu pro různé aplikace. V závislosti na světelných podmínkách je clona regulována tak, aby bylo dosaženo určité optimální středové pozici. [30]

Není doporučováno používat objektiv s automatickou regulací na dohledové videosystémy bez funkce P-Iris, jelikož jednotlivé funkce mezi sebou nejsou kompatibilní a mohlo by docházet k výraznému snížení kvality obrazu. Objektiv s funkcí P-Iris by se tedy měl používat výhradně s dohledovými videosystémy, které tuto technologii podporují. [30]

### **Hloubka ostrosti, optická ostrost**

Hloubka ostrosti je ovlivňována ohniskovou vzdáleností, clonou objektivu a vzdáleností snímaných objektů. Vyjadřuje rozdíl nejbližšího a nejvzdálenějšího objektu ve snímané scéně, které jsou vyobrazeny ostře. [30]

Obecně platí, že čím je clona objektivu více přivřena, tím je hloubka ostrosti vyšší.

Problémy mohou nastat u objektivů, které mají ručně nastavitelnou clonu, a to při snímání obrazu za použití infračervených reflektorů. Jelikož infračervené světlo je charakteristické jiným lomem světla, může při nočním snímání nastat rozostření světla. Proto by se měly používat objektivy, které jsou označovány IR (Infra Red), které mají na povrchu objektivu speciální vrstvu, která zamezuje pronikání infračerveného světla s odlišným lomem světla. [30]

### **Uchycení objektivu**

Objektivy dle typu uchycení se dělí na:

- C,
- CS.

U všech VSS se využívá stejného závitu uchycení objektivu (1“), rozdíl je pouze ve vzdálenosti roviny zadní čočky objektivu od snímacího čipu. [30]

Obecně platí, že objektivy s uchycením typu C, lze používat u VSS s typem uchycení C. Při instalaci objektivu s označením C na VSS s označením CS, je nutné použít redukci C/CS. Objektiv s uchycením typu CS lze použít pouze u VSS se shodným označením. [30]

## **4.2 Propojení**

Vzájemné propojení VSS vytváří přenos dat, obstarávající spojení a komunikaci.

Komunikace mezi jednotlivými zařízeními je obstaráváno kabely, např. koaxiální kabel, ethernetový kabel, optické vlákno, nebo pomocí bezdrátové sítě. Komunikaci VSS lze uskutečnit i prostřednictvím sítí, které nejsou vyhrazeny jen pro VSS, ale i pro jiné aplikace.

### **4.2.1 Přenosová cesta**

Přenos obrazu u IP VSS bývá standardně uskutečněn digitálně (koaxiálně kabel, ethernetový kabel, optické vlákno), ale použitím technologie hybridního dohledového videosystému lze pro přenos použít i koaxiální kabel. [4]

### Koaxiální vedení

Přenos videosignálu je uskutečněn metalickým koaxiálním vedením s impedancí  $75 \Omega$  ukončené BNC konektory. Maximální délka vedení závisí na kvalitě koaxiálního kabelu, obvykle dosahuje až 300 m a odvíjí se od kvality měděného jádra. Pro delší trasy je nutné použít zesilovač videosignálu. [31]

Základními částmi koaxiálního kabelu je:

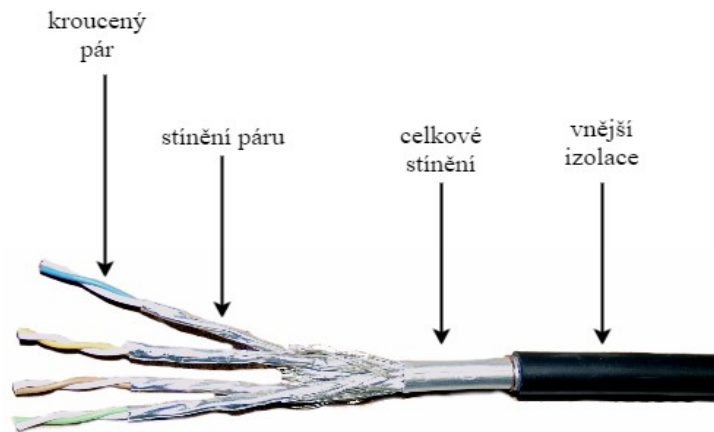
- vnitřní vodič (jádro z plného drátu nebo lanka),
- vnější vodič (hliníková nebo měděná fólie),
- izolační vrstva (nejčastěji polyethylen). [31]



Obr. 33: Vrstvy koaxiálního kabelu [31]

### Symetrické vedení

Symetrické vedení (krouceným párem) je další druh metalického vedení, kterým lze vést digitální signál. Využívají se kabely UTP (nestíněný kabel), FTP (každý pár je stíněný), STP (každý pár je stíněný a opletený drátem). Důvodem kroucení je zlepšení vlastností elektromagnetické kompatibility. Délka vedení se pohybuje mezi 100–200 m. [32]



Obr. 34: STP kabel [32]

Výhody symetrického vedení:

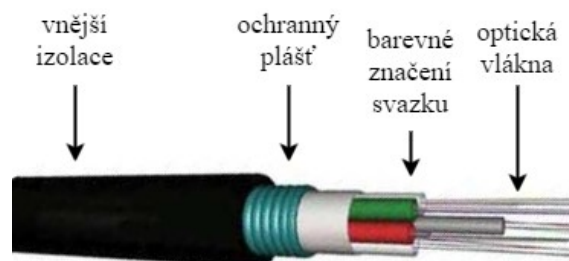
- možnost přenosu více signálu prostřednictvím jednoho kabelů,
- široké možnosti aplikace,
- odolnost vůči rušení.

Nevýhody:

- komplikace při přenosu signálu na větší vzdálenosti. [33]

### Optické vedení

Optické vedení je skleněné nebo plastové vlákno, ve kterém dochází k malým ztrátám. Důležitou vlastností je imunita vůči elektromagnetickému rušení. Používají se optické kabely jednovidové a mnohovidové. Maximální vzdálenost závisí na počtu optických vláken. U jednovidových kabelů lze dosáhnout vzdáleností v rámci jednotek kilometrů, u mnohovidových se pohybuje vzdálenost ve stovkách metrů. [33]



Obr. 35: Mnohovidový optický kabel [33]

Mezi výhody optických kabelů patří především:

- vysoká přenosová rychlost,
- nízké ztráty,
- absence bludných proudů
- absence tvorby elektromagnetického rušení,
- odolnost vůči elektromagnetickému rušení,
- dlouhá životnost. [33]

Nevýhody optických kabelů:

- vysoká cena,
- komplikovaná tvorba spojů,
- choulostivost na ohyb. [33]

### **Bezdrátový přenos**

Bezdrátový přenos nahrazuje signálový kabel mezi kamerou a záznamovým zařízením. Užívá se v případech složité realizace kabeláže. Přenos signálu je uskutečněn v rámci pásma 2,4 nebo 5 GHz. Výběr kamer se zabudovaným vysílačem je omezený. Používá se zřídka. Maximální vzdálenost při přímé viditelnosti se pohybuje ve stovkách metrů. Při přenášení bezdrátové signálu v rámci budov, je signál řádově snížen. [34]

### **4.2.2 Přenosové protokoly síťového videa**

#### **TCP/IP**

Protokol TCP/IP je nejpoužívanějším komunikačním protokolem. Využívá se pro širokou škálu aplikací. Je základním komunikačním protokolem pro přenos síťového videa. Má na starost přenos datových paketů přes případné mezilehlé uzly, až na místo jejich určení. [35]

IP část protokolu obstarává samotné proudění dat, zatímco TCP slouží k řízení toku dat. Každý IP VSS má svou vlastní IP adresu, která slouží k identifikaci zařízení v rámci sítě. [35]

#### **UDP**

Protokol UDP nenavazuje přímé spojení mezi komunikujícími počítači na rozdíl od TCP/IP. Výhodou tohoto protokolu je, že nepotřebuje jednoznačnou IP adresu k doručení dat. Umožňuje tedy streamovat video více účastníkům síťového provozu najednou. [35]

## RTSP

Protokol RTSP (Real Time Streaming Protocol) slouží k reálnému (v reálném čase) streamování audia i videa. RTSP využívá téměř každý výrobce VSS. [35]

## ONVIF

ONVIF (Open Network Video Interface Forum) je sdružení výrobců v oblasti VSS. V současné době sdružuje více než 500 společností poskytující zařízení, mezi kterými je zajištěna kompatibilita. [36]

Sdružení ONVIF sjednocuje kompresi, přenos audia i videa streamů, zpracování událostí, ovládání zařízení a mnoha dalších parametrů. Cílem je sjednotit jednotlivé platformy k zajištění kooperativní funkce. [36]

Byly vytvořeny jednotlivé profily, které slouží k jasné identifikaci zařízení, které jsou mezi sebou v rámci konkrétního profilu kompatibilní a zároveň jedno zařízení, může patřit do více profilů. [36]

V současnosti existuje několik profilů garantující parametry zařízení:

- profil S (audio a video streaming, ovládání PTZ a výstupů, konfigurace videa a multicast),
- profil G (konfigurace, požadavek a ovládání pořízení záznamu, zajištění přenosu audia a metadat),
- profil C (síťová konfigurace, ovládání událostí a poplachových stavů, řízení vstupu),
- profil Q (jednoduchost nastavení, konfigurace a ovládání zařízení),
- profil A – není oficiální (řízení privilegií, integrace systémů kontroly vstupu a IP VSS). [36]

### 4.2.3 Síťová zařízení

#### Router

Router je aktivní síťový prvek, který slouží pro vzájemné propojení sítí, mezi kterými uskutečňuje síťový provoz. Přeposílá pakety podle přiřazených IP adres, čímž zajišťuje doručení dat do korektního cíle. [37]



## Switch

Switch umožňuje komunikovat síťovým zařízením mezi sebou. Odděluje a zároveň propojuje provoz mezi jednotlivými zařízeními v rámci sítě. [37]

## Hub

Hub neboli rozbočovač, slouží jako opakovač, přeposílá přijatá data všem připojeným zařízením. Může způsobit zbytečné zatížení sítě. [37]

### 4.2.4 Zabezpečení sítě

Provoz sítě je nutné zabezpečit. Přístup, samotné posílání dat po síti a přístupnost sítě musí být zabezpečena a kontrolována. [5]

#### Přístupová práva

Přístupová práva slouží k ověření identity uživatele při přístupu k datům (autentizace) a zda uživatel má právo přístupu k danému zdroji (autorizace) [5]

##### *Autentizace*

Ověřuje identitu uživatele. Pomocí certifikátu nebo uživatelského účtu, například heslem, ověřuje, zda zařízení je tím, za koho se vydává. [5]

##### *Autorizace*

Autorizace poskytuje přístup ke zdrojům dat. Ověřuje se, zda uživatel má právo přístupu k tomuto zdroji dat. Uživatelé dále se rozdělují dle dalších práv, které udělují možnost data prohlížet nebo upravovat. [5]

## HTTPS

HTTPS je šifrovací protokol, který slouží k šifrování samotných dat. Pomocí nainstalovaného certifikátu klient ověřuje, zda certifikát je platný a rozhodne o přístupu k požadovaným datům. [38]

## VPN

VPN (Virtual Private Network) slouží k vytvoření zabezpečeného připojení mezi zařízeními uvnitř této soukromé sítě. Přístup k datům má pouze takové zařízení, které má k dispozici relevantní klíč. [38]

### 4.3 Zpracování obrazu

Mezi funkce zpracování obrazu patří analýza, uložení a zobrazení pořízených obrazových dat. [5]

#### 4.3.1 Analýza obrazu

Analýza obrazu je proces zkoumání snímaného obrazu nebo záznamu. Cílem je získat relevantní informace o detekci narušení, poškození kamery, identifikování objektu nebo osoby apod. Získávání informací může být skutečně obsluhou nebo výpočetní technikou.

Problematika videoanalýzy byla zpracována v kapitole 2.2.4.

#### 4.3.2 Záznamová zařízení

K uložení pořízených obrazových dat slouží záznamová zařízení. Uložený záznam lze dále zpracovávat, měnit rozlišení, snímkovou frekvenci, kompresi a použít k vyhledání relevantních informací. [39]

#### DVR

DVR (Digital Video Recorder) slouží k uložení zaznamenaných analogových (hybridní systémy) i digitálních dat na paměťové médium. DVR poskytuje funkce, které umožňují vyhledávat v záznamu dle data, času i události. Uložená data je možné dále komprimovat, měnit snímkovou frekvenci a rozlišení, čímž lze docílit optimalizace uskladněných dat. DVR bývá vybaveno síťovou kartou, lze tedy DVR připojit k síti, což umožňuje i vzdálené prohlížení záznamů. [39]

#### NVR

NVR (Network Video Recorder), na rozdíl od DVR, slouží především k samotnému uložení pořízeného obrazového záznamu z IP kamer, který je již zpracován k samotném kamerovém zařízení. Stejně jako DVR, je i NVR vybaveno síťovou kartou. [39]

#### 4.3.3 Zobrazovací prvky

K zobrazení snímané scény se používají monitory. Co se týče zobrazovacích prvků, bývá investice podceňována, což vede ke snížení kvality zobrazovaného obrazu. Mezi nejdůležitější parametry zobrazovacích zařízení patří rozlišení a velikost obrazovky. Technologie CRT monitorů je již historií, v současnosti se využívají LCD, plasma nebo LED monitory.

Na rozdíl od klasických monitorů, monitory pro VSS aplikace jsou navrženy pro nepřetržitý provoz. U klasických monitorů může docházet po určité době k degradaci obrazu z důvodu tzv. vypalování obrazu. Monitory pro VSS aplikace jsou také často vybaveny konektorem BNC k připojení analogových systémů. [5]

#### **4.3.4 Komprese obrazu**

Problematika komprese obrazu byla zpracována v kapitole 2.2.3

## 5 METODIKA TVORBY NÁVRHU BEZPEČNOSTNÍHO PROJEKTU

### 5.1 Požadavky zadavatele projektu

Před samotným bezpečnostním posouzením je nutné zjistit požadavky zadavatele projektu. Požadavky se mohou lišit vzhledem k typu a hodnotě chráněných aktiv, množství pohybujících se osob v objektu a v jeho okolí a umístění samotného okolí.

Norma doporučuje následující:

*„Návrh systému má být stanoven po konzultaci s klientem nebo zadavatelem I&HAS (případně jimi pověřeným zástupcem) a dalšími zainteresovanými stranami, například pojistiteli nebo policií.“ [3]*

### 5.2 Metodika návrhu I&HAS

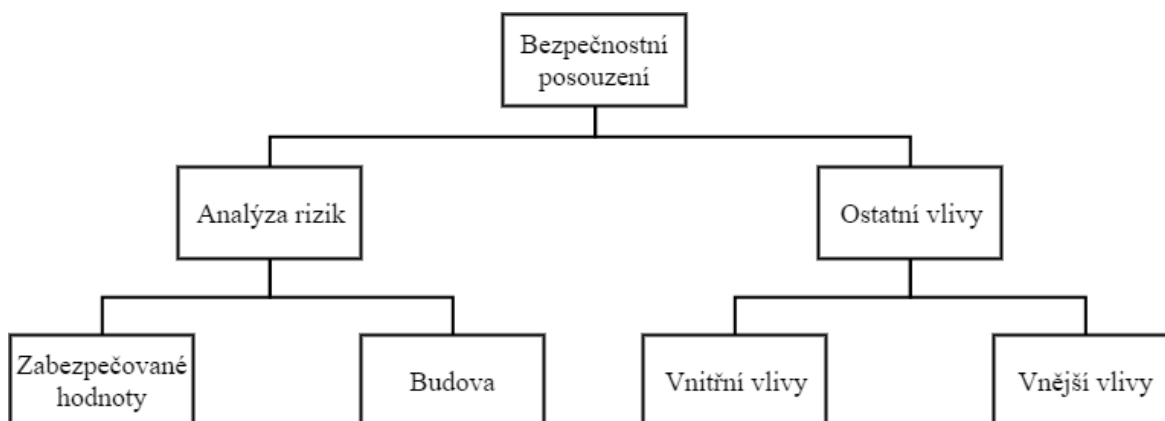
Prvotní etapou při zřizování I&HAS je nutné provést bezpečnostní posouzení, které je následováno posouzením ostatních vlivů v prostorách. Cílem návrhu I&HAS je stanovení rozsahu celého systému, volba vhodných komponentů splňující funkční kritéria a samotné zpracování návrhu řešení. Důležitou součástí je i volba vhodného počtu a typu detektorů a jejich umístění.

Metodika návrhu I&HAS vychází z technické normy ČSN CLC/TS 50131-7. [3]

#### 5.2.1 Bezpečnostní posouzení

Bezpečnostní posouzení představuje proces identifikace hrozeb a pravděpodobnosti jejich vzniku pro posuzovaný objekt. Cílem je určení stupně zabezpečení a návrh skladby systému při zachování bezproblémové nepřetržité funkce. [3]

Bezpečnostní posouzení se dělí na následující části:



Obr. 36: Rozdělení částí bezpečnostního posouzení [3]

### Zabezpečené hodnoty

Při návrhu je nutné dbát na charakter střeženého objektu. Návrh má odpovídat míře rizika vloupání do střežených prostor. V této souvislosti hrají roli následující faktory:

Tab. 12: Zabezpečené hodnoty [3]

<b>Druh majetku</b>	Zpeněžitelnost majetku, atraktivnost pro pachatele, zhodnocení nebezpečí vloupání.
<b>Hodnota majetku</b>	Maximální pravděpodobná hodnota jednotlivé ztráty, výdaje související se ztrátou.
<b>Množství nebo velikost</b>	Snadnost odejmutí a transportu, přístup do střežených prostor.
<b>Nebezpečí</b>	Nebezpečí hrozící pro osoby a okolní prostředí.
<b>Poškození</b>	Způsobené poškození zanedbáním, vandalismem nebo žhářstvím. na objektu

## Budova

Důležitým faktorem při návrhu systému je i stavební dispozice. Měly by se respektovat následující faktory:

Tab. 13: Budova [3]

<b>Otvory</b>	Okna, dveře
<b>Režim provozu objektu</b>	Přítomnost pracovníků ostrahy
<b>Lokalita</b>	Vliv lokality na budovu
<b>Bezpečnostní prostředí</b>	Umístění objektu vzhledem k okolí

## Vnitřní vlivy

Vlivů působících na I&HAS mající původ ve střežených prostorech může být mnoho. Měly by se respektovat především při volbě typů zařízení, jejich umístění a nastavení. Vlivy mohou být následující:

Tab. 14: Vnitřní vlivy [3]

<b>Vytápění, vzduchotechnika, klimatizace</b>	Vliv na ultrazvukové detektory
<b>Elektromagnetické rušení</b>	Vliv svařovacích souprav, výbojkových komponentů zařízení
<b>Uspořádání skladovaných předmětů</b>	Snížení nebo úplné zakrytí zorného pole detektorů
<b>Zvláštní pozornost</b>	Respektování specifických vlastností jednotlivých detektorů
<b>Riziko planých poplachů u tísňových systémů</b>	Minimalizace možnosti vyvolání nechtěné aktivace

## Vnější vlivy

Vnějších vlivů, které mohou působit na funkci I&HAS je několik, a jsou to následující:

Tab. 15: Vnější vlivy [3]

<b>Dlouhodobě působící faktory</b>	Faktory, které se nemění několik let, železnice, silnice apod.
<b>Krátkodobě působící faktory</b>	Vlivy výstavby objektů v těsné blízkosti zabezpečovaného objektu

### 5.2.2 Informace návrhu systému I&HAS

Návrh by měl obsahovat informace, které přesvědčí zadavatele projektu o tom, že je návrh proveden správně a je vhodný pro danou aplikaci. Návrh by měl obsahovat následující:

Tab. 16: Informace návrhu systému I&HAS [3]

<b>Údaje o střežených prostorech</b>	Účel prostor objektu a jejich popis
<b>Třída prostředí</b>	Uvedení třídy prostředí komponent systému
<b>Stupeň zabezpečení</b>	Uvedení stupně zabezpečení objektu
<b>Seznam vybavení</b>	Seznam použitého zařízení
<b>Konfigurace systému</b>	Informace o funkcích systému
<b>Hlášení poplachu</b>	Informace o umístění výstražných zařízení

### 5.2.3 Technické posouzení

Technické posouzení představuje proces, jehož cílem je potvrdit, zda požadavky uvedené v návrhu systému jsou realizovatelné. Také slouží k přesnému určení umístění jednotlivých komponent systému a propojení.

Tab. 17: Technické posouzení [3]

<b>Propojení</b>	Propojení systému I&HAS drátovým nebo bezdrátovým propojením
<b>Všeobecné požadavky pro detektory</b>	Správná volba zařízení v daném prostředí, výběr detektorů s vhodným umístěním

<b>Tísňová zařízení</b>	Snadná přístupnost, nemožnost náhodné aktivace
<b>Ústředny a napájecí zdroje</b>	Instalace do veřejně nepřístupných míst, do střeženého prostoru
<b>Výstražná zařízení</b>	Umístění na nápadném místě při zajištění slyšitelnosti

### 5.3 Metodika návrhu VSS

Metodika návrhu dohledového videosystému vychází z normy ČSN EN 62676-4.

#### 5.3.1 Posouzení rizik

Prvotním krokem před návrhem VSS je posouzení rizik a identifikace hrozeb představující riziko pro objekty, osoby nebo organizaci. Posuzují se následující faktory:

Tab. 18: Posouzení rizik [5]

<b>Zabezpečované hodnoty</b>	Finanční nebo intelektuální hodnota nacházející se v zabezpečovaných prostorách
<b>Prostředí</b>	Posouzení existujícího zabezpečení
<b>Osídlení</b>	Posouzení přístupu veřejnosti ke zabezpečovanému objektu, osídlení v okolí

#### 5.3.2 Specifikace provozních požadavků

Mělo by se vycházet z následujících částí:

Tab. 19: Specifikace provozních požadavků [5]

<b>Účel</b>	Stanovení účelu systému
<b>Definice sledovaného místa</b>	Stanovení sledovaného místa (budova, osoby, majetek)
<b>Definice aktivit</b>	Uvedení kategorie pozorování cílů
<b>Doba provozu</b>	Uvedení doby provozu
<b>Monitorování a ukládání obrazu</b>	Definice o u chovávaných záznamech



### 5.3.3 Volba zařízení a výkonnost

Obecně by se měly při výběru zařízení respektovat faktory životního prostředí. [5]

#### Kamerové zařízení

Musí být zvolena vhodná kombinace kamery a objektivu, která splňuje funkční a výkonové požadavky. Při výběru kamery by se měla brát v úvahu následující kritéria:

Tab. 20: Kamerové zařízení [5]

<b>Rozlišení</b>	Volba vhodného rozlišení
<b>Volba objektivu a krytu</b>	Clonové číslo, podmínky prostředí
<b>Pokrytí sledovaného místa</b>	Stanovení počtu kamer a jejich vhodného umístění
<b>Zorné pole</b>	Volba velikosti sledovaného cíle

### 5.3.4 Charakteristiky videa

Mezi funkční vlastnosti charakteristiky videa patří:

Tab. 21: Charakteristiky videa [5]

<b>Kompresce obrazu</b>	Vychází z provozních požadavků
<b>Snímkový počet</b>	Stanovení počtu, ale dané aplikace
<b>Rozlišovací schopnost</b>	Rozlišení dle účelu kamery

## DÍLČÍ ZÁVĚR

V kapitole byla popsána metodika bezpečnostního posuzování. Metodika pro bezpečnostní posuzování z hlediska I&HAS a VSS se liší. Pro poplachové zabezpečovací a tísňové systémy metodika vychází z normy ČSN CLC/TS 50131-7, zatímco metodika pro bezpečnostní posouzení VSS z technické normy ČSN EN 62676-4. Veškeré aspekty, zásady a faktory, které byly zmíněny v této kapitole, budou využity k navrhování bezpečnostního projektu rozsáhlé výrobní společnosti, která je vypracována v praktické části diplomové práce.

## **II. PRAKTICKÁ ČÁST**

## 6 BEZPEČNOSTNÍ POSOUZENÍ

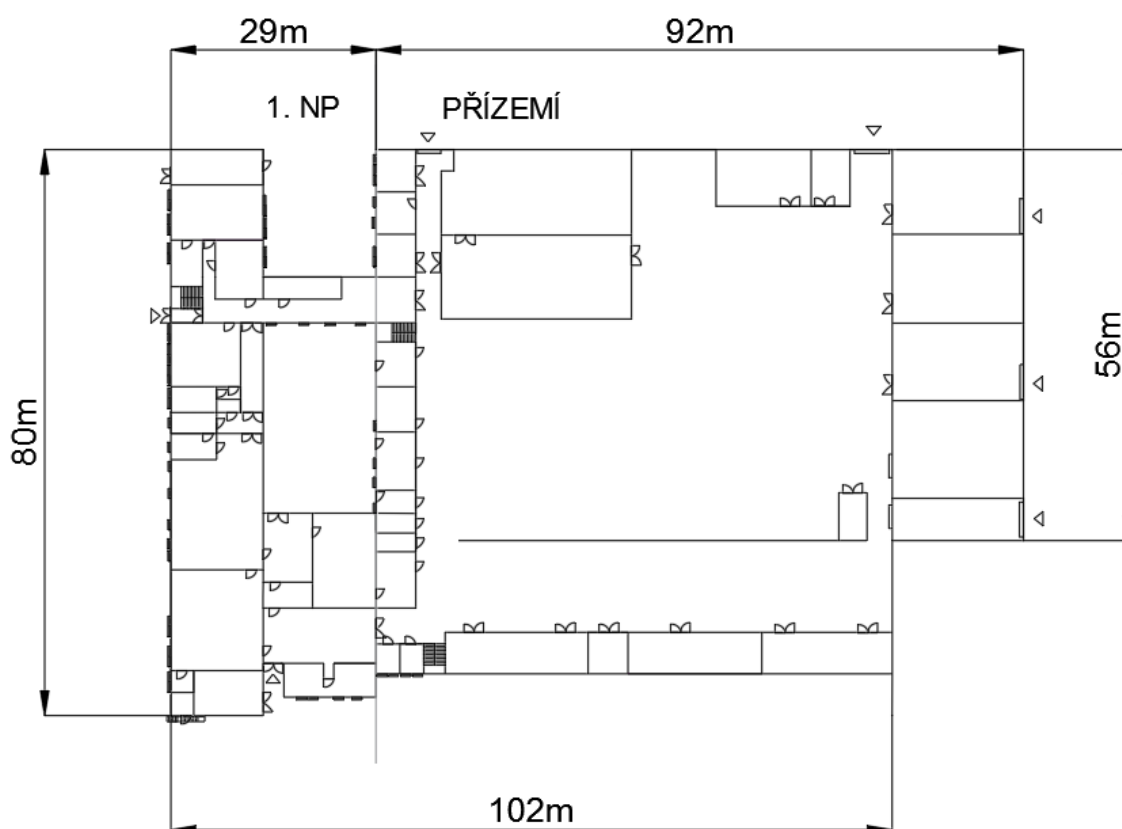
### 6.1 Informace o objektu

Objekt výrobní společnosti bude rekonstruován. Návrh bezpečnostního projektu vychází z projektové dokumentace návrhu na rekonstrukci.

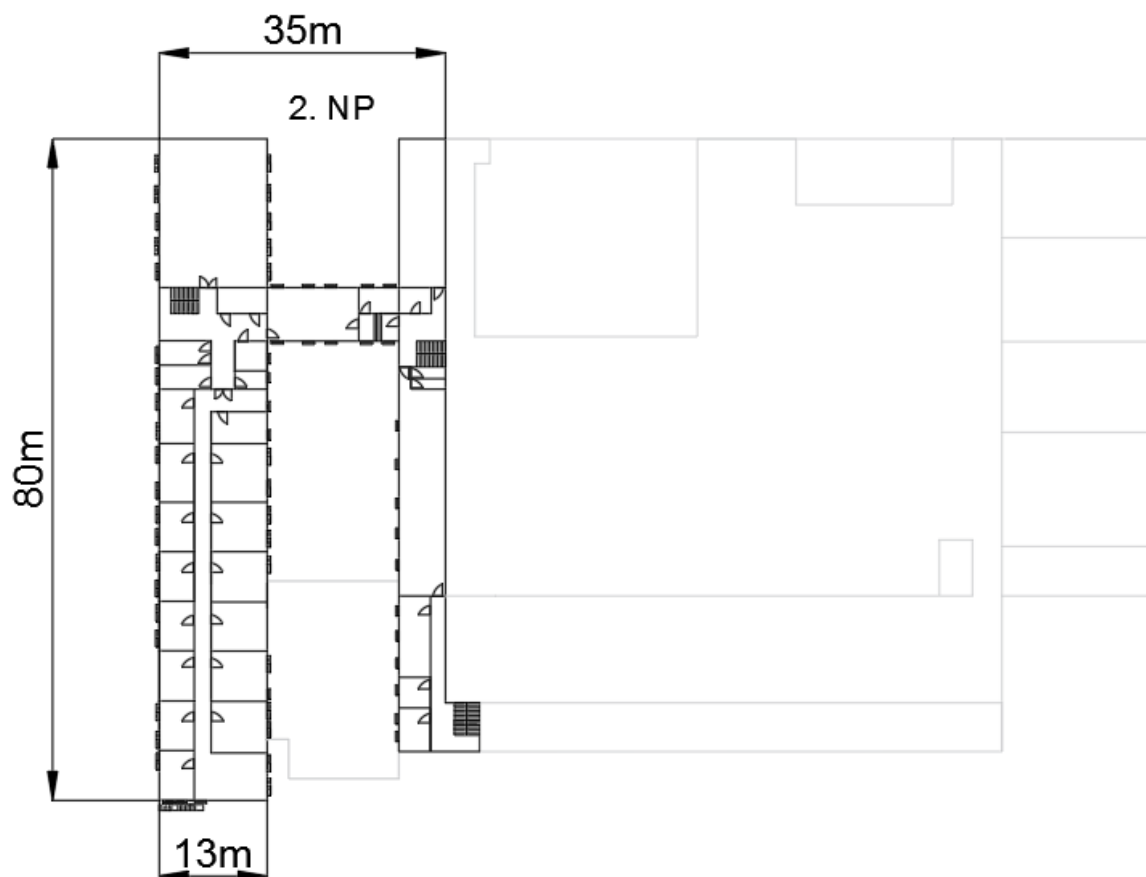
Vzhledem k rozsahu, objekt byl rozdělen na jednotlivé sektory. Každý sektor je rozdělen z hlediska účelu a využití daných prostor. Sektory jsou následující:

- výroba a sklady,
- administrativní část,
- vstupy, trafostanice a další klíčové prostory,
- perimetr,
- ostatní.

Samotný objekt se skládá z přízemí a 2 nadzemních podlaží. Následující schéma slouží ke zjednodušenému zobrazení a rozdělení objektu:



Obr. 37: Přízemí a 1. nadzemní podlaží

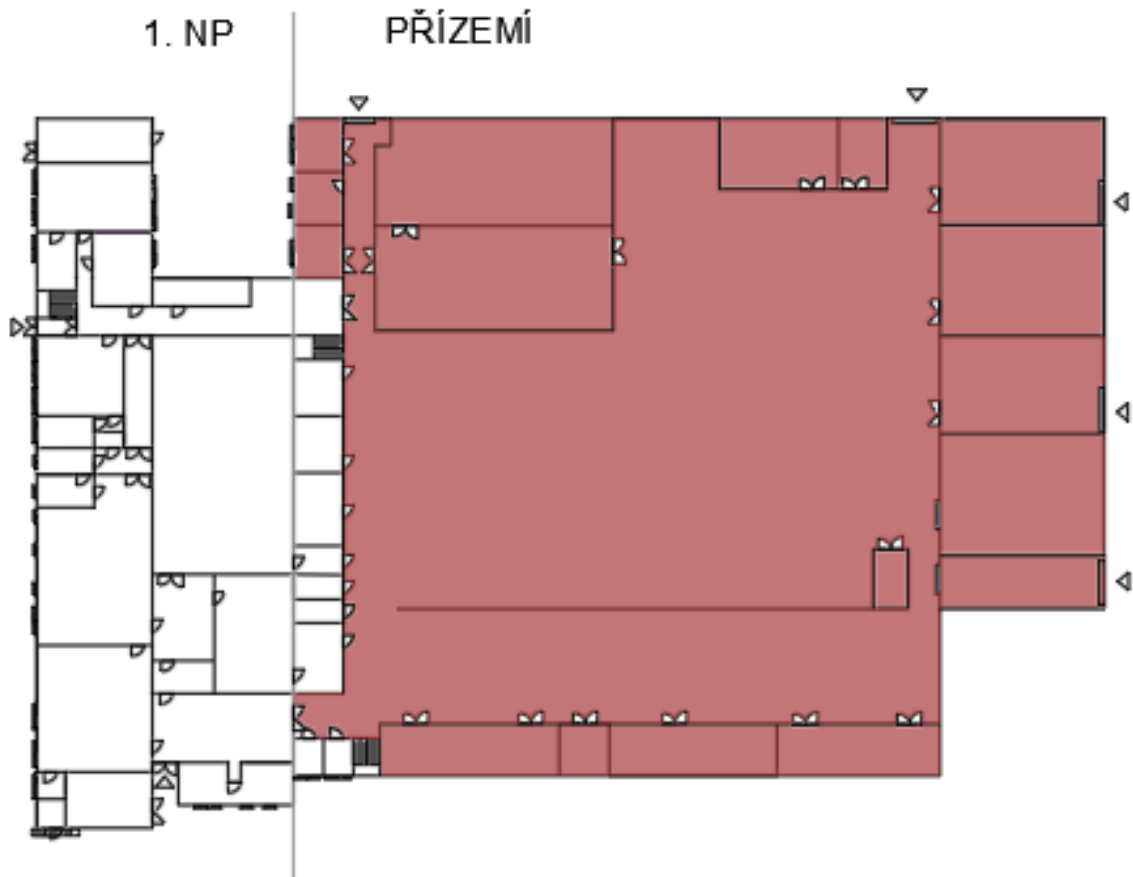


Obr. 38: 2. nadzemní podlaží

## 6.2 Bezpečnostní posouzení jednotlivých sektorů

### 6.2.1 Výroba a sklady

Prostory výroby a skladů představují následující prostory:



Obr. 39: Zjednodušené zobrazení prostor výroby a skladů

#### I&HAS

V prostorách výroby se bude nacházet několik technologických zařízení. Většinou se jedná o velké výrobní stroje, které jsou zcela neodcizitelné. Dále se v prostorách budou využívat vysokozdvižné vozíky, které jsou pro pachatele jednoduše zpeněžitelné a jejich hodnota a následná ztráta je vysoká. Materiál a produkty společnosti se nepovažují za finančně nákladné.

V prostorách vysoké riziko představují především formy sloužící k výrobě produktu. Jejich odcizení nebo poškození by mohlo způsobit značnou ztrátu výrobní společnosti.

Elektrická vrata představují riziko průniku skrz plášť.

V prostorách výroby a skladů se vyskytuje mnoho faktorů, které mohou ovlivnit funkce detektorů. Předpokládá se výskyt vodovodních potrubí a vzduchotechniky. Výrobní technologická zařízení představují velký zdroj tepla. Elektromagnetické rušení vlivem výrobních zařízení se nepředpokládá žádné. Pravděpodobnost vzniku planých poplachů je velmi vysoká. Skladované předměty mohou způsobit zastínění zorného pole detektorů. Vlivem svévolného pohybu skladovaných předmětů může dojít k vyvolání planého poplachu.

Tísňová tlačítka by měla být umístěna tak, aby nemohlo dojít při manipulaci s výrobními zařízeními nebo popřípadě jejich údržby, k nechtěné aktivaci poplachu.

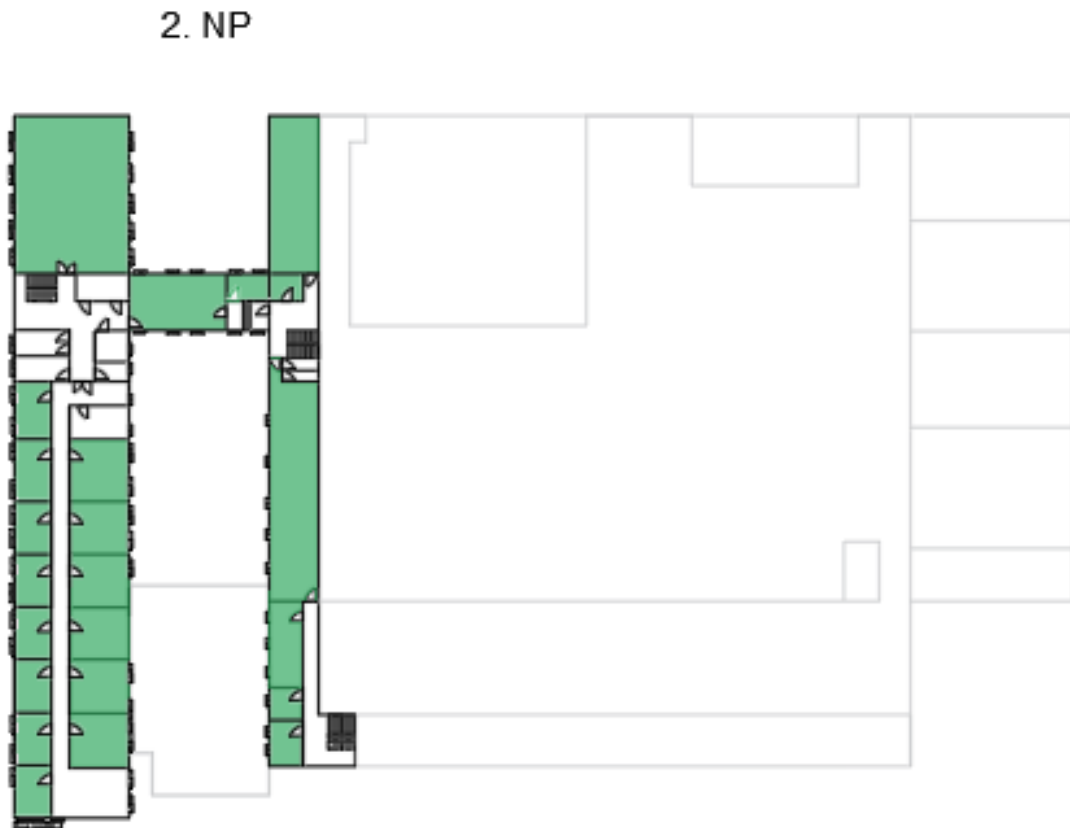
### VSS

Bude docházet k časté manipulaci s materiálem i produkty, čímž může vzniknout riziko vzniku nebezpečí osobám, produktům a technologickým zařízením. Vysokozdvížené vozíky představují nebezpečí, které mohou způsobit při manipulaci s materiálem a hotovými produkty. Měla by se také brát v úvahu možnost poškození samotných vysokozdvížných vozíků a možnost poškození ostatního vybavení a prostor. Pravděpodobnost vzniku hrozby nebezpečí pro zaměstnance a další osoby je vysoká. Je nutné brát na vědomí i riziko vandalismu způsobené nepovolanými osobami, ale také i samotným personálem.

Z hlediska vlivů, které mohou působit na VSS, je nutné brát na vědomí teplo, které budou produkovat výrobní zařízení. Kamerová zařízení tedy v žádném případě nesmí být umístována přímo nad tato výrobní zařízení.

### 6.2.2 Administrativa a kanceláře

Prostory administrativy a kanceláří představují následující části:



Obr. 40: Zjednodušené zobrazení prostor administrativy  
a kanceláří

#### I&HAS

Předpokládá se přítomnost velkého množství technického vybavení kanceláří (výpočetní technika, tiskárny, zobrazovací zařízení atd.), které je velmi atraktivní pro zloděje. Dále projektové dokumentace, technické výkresy a informace jejichž únik by mohl způsobit značné ztráty společnosti.

Část se nachází v 2.NP, což představuje snížení rizika průniku pachatele skrz okenní otvory, ovšem toto riziko není eliminováno.

Předpokládá se přítomnost klimatizačních a vzduchotechnických systémů, které mohou ovlivnit funkci detektorů pohybu.

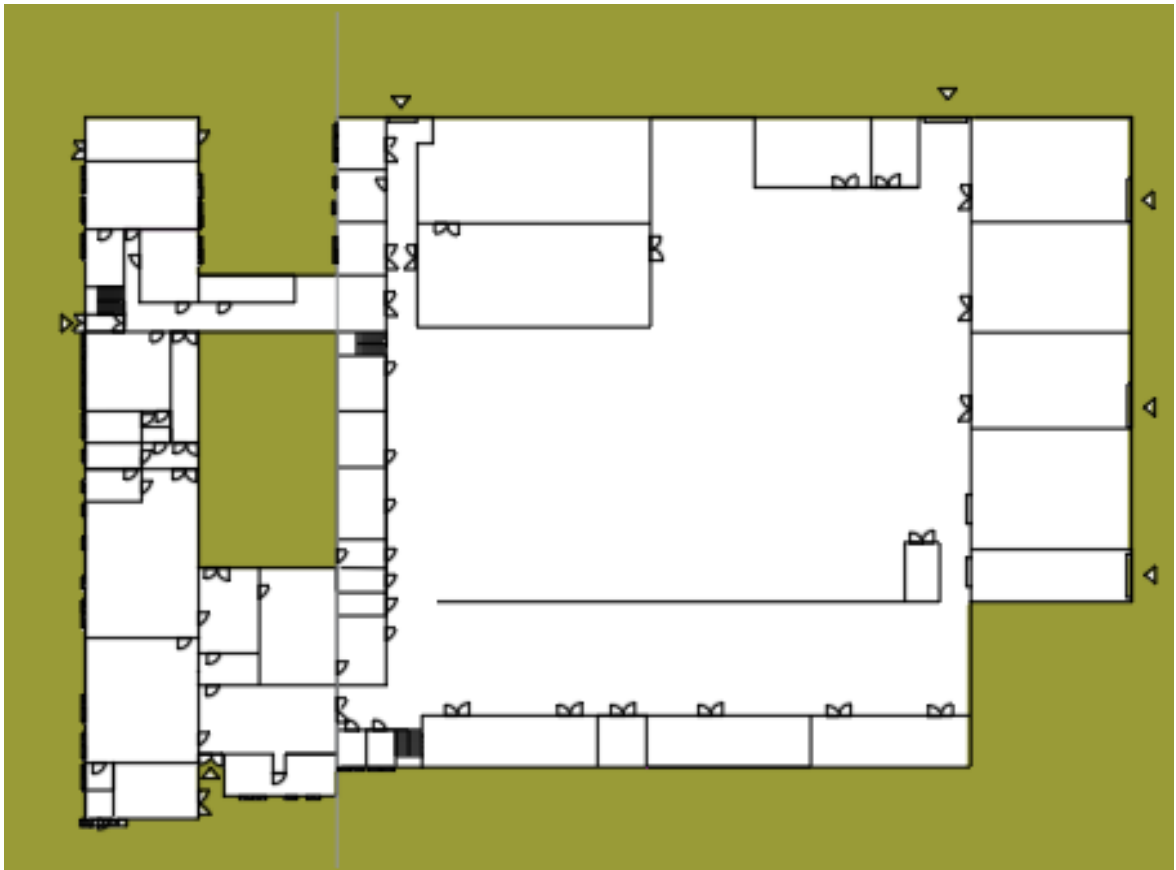


## VSS

Administrativní část tvoří mnoho kanceláří, které se budou nacházet v 2. NP. Veřejnost ani personál výroby a skladů běžně do těchto prostor nebude mít přístup.

### 6.2.3 Perimetr

Perimetr je zobrazen v následujícím schématu:



Obr. 41: Zjednodušené zobrazení perimetru objektu

## I&HAS

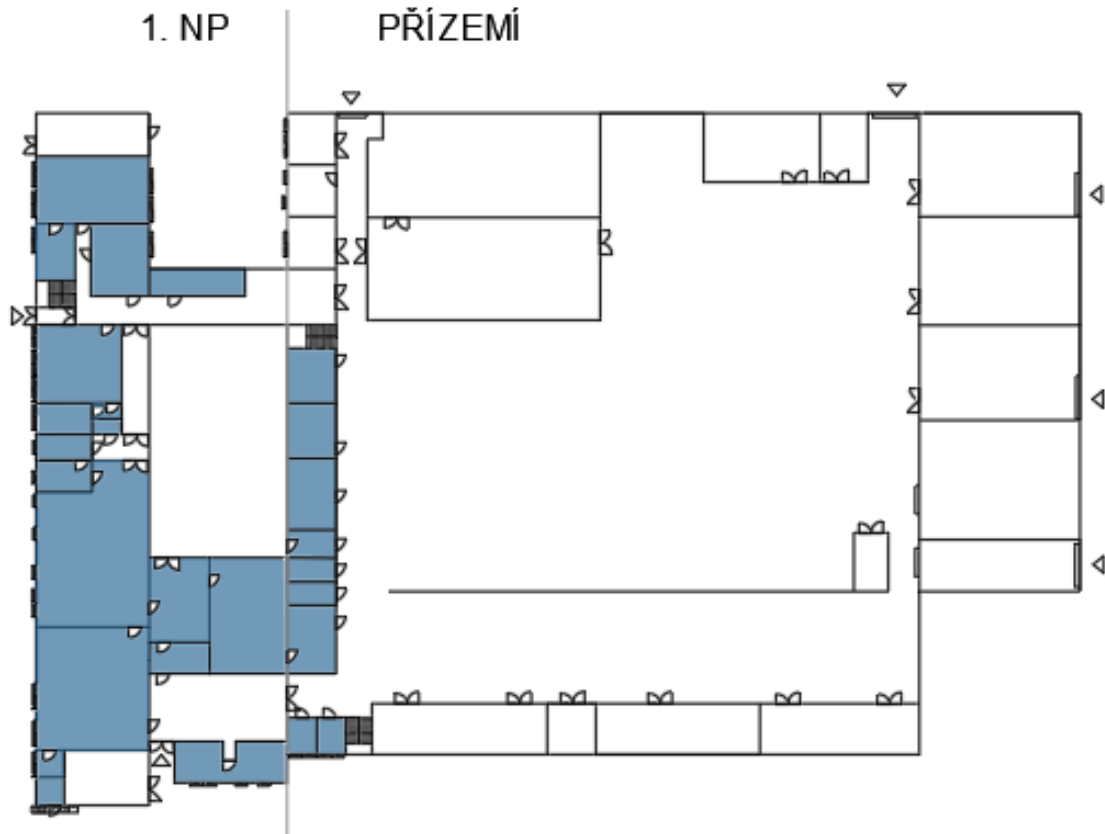
I&HAS nebude využit ke zabezpečení perimetru.

## VSS

Ze severní části budovy bude sluneční záření ovlivňovat snímací charakteristiky VSS, ty by měly mít schopnost potlačit tento negativní faktor. V těsné blízkosti objektu se nenachází žádné budovy, které by mohly omezit zorné pole nebo měly jiný vliv na výslednou kvalitu obrazu. Areál a objekt se nachází v oblasti s mírným podnebím bez žádných pozorovaných extrémů týkajících se klimatických podmínek.

#### 6.2.4 Ostatní

Ostatní prostory jsou zobrazeny na následujícím schématu:



Obr. 42: Zjednodušené zobrazení ostatních prostor

#### I&HAS

Mezi ostatní prostory patří jídelna, sociální zázemí, šatny, kuchyně a příslušné prostory.

Výskyt zabezpečovaných hodnot se předpokládá především v jídelně, v dalších prostorách nikoliv. V ostatních prostorech by se neměly nacházet aktiva, jejichž poškození či odcizení by mohly způsobit újmu společnosti.

Pokud se prostory nachází podél pláště budovy, měly by se brát v potaz okenní otvory. Dále se předpokládá využívání vzduchotechnických a klimatizačních systémů, které mohou ovlivnit funkce detektorů pohybu.

#### VSS

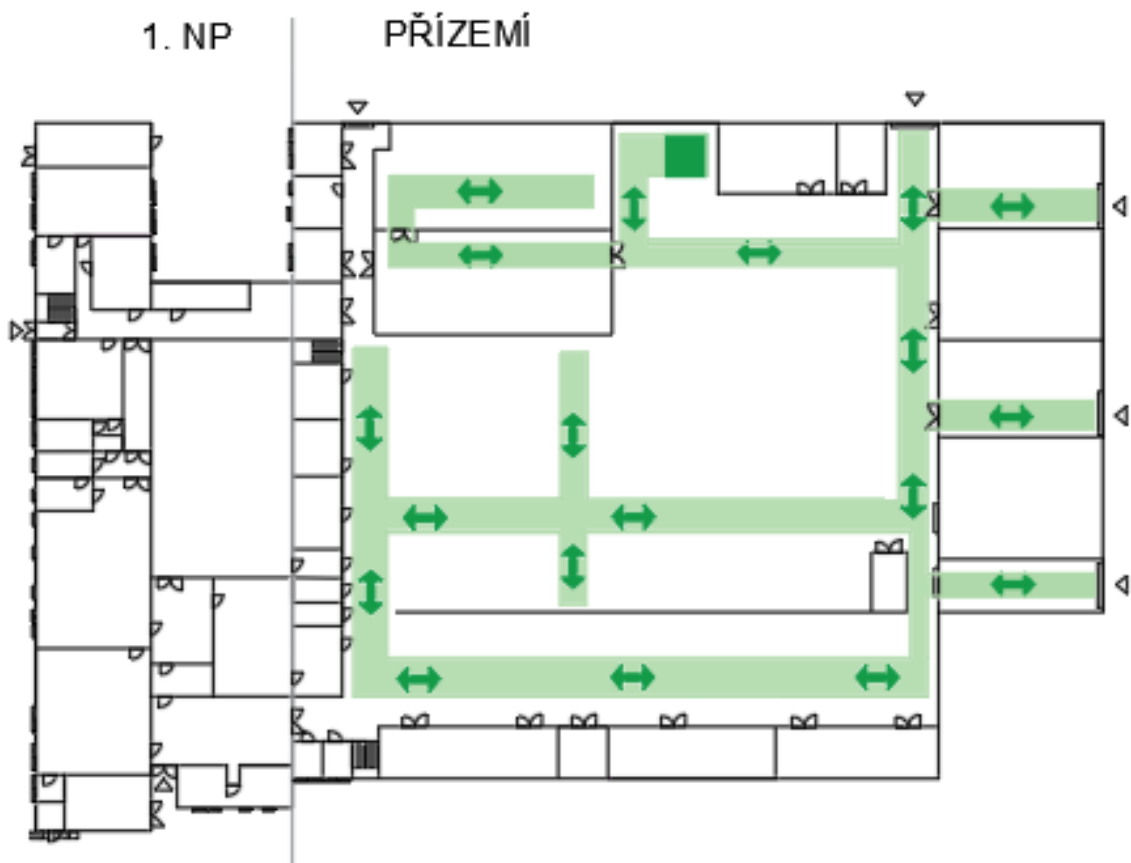
Nepředpokládá se umístění VSS.

## 6.3 Provoz v objektu

V předchozí kapitole bylo vypracováno bezpečnostní posouzení rizik v objektu. Následně je v následujících zjednodušených schématech zobrazen provoz v objektu z hlediska jednotlivých faktorů. Tato část bezpečnostního posouzení bude nápomocná zejména při posuzování rozmístění zařízení VSS

### 6.3.1 Častý pohyb vysokozdvížných vozíků

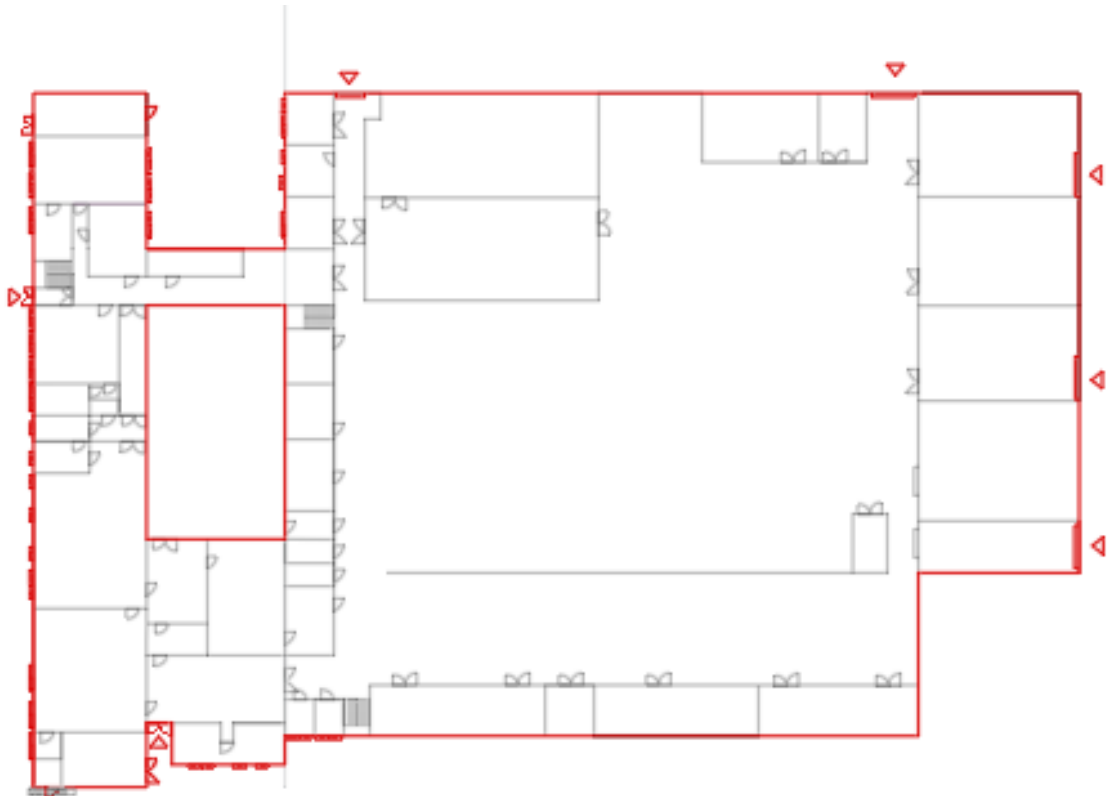
Vysokozdvížné vozíky, které budou použity k přepravě materiálu a produktů, představují riziko vzniku nehody. Může dojít k ohrožení výrobních zařízení, vybavení objektu i osob. Proto je nutné při návrhu zejména VSS brát na vědomí jejich pohyb. Předpokládaný pohyb vysokozdvížných vozíků a jejich stanoviště je zobrazeno na následujícím schématu:



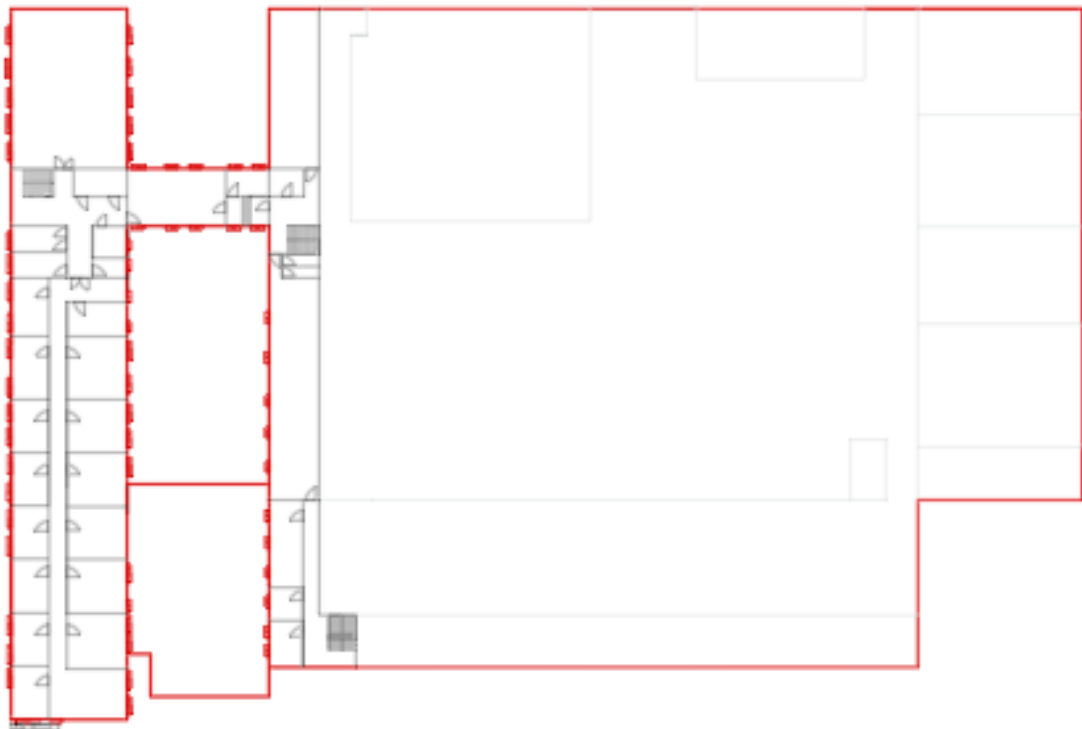
Obr. 43: Předpokládaný zvýšený pohyb vysokozdvížných vozíků.

### 6.3.2 Plášť

Při zabezpečování pláště budovy je nutné brát ohled na otvorové výplně (dveře, okna, balkonové dveře a jiné), ale také na obvodové zdivo. Zejména dveře a okna představují jednoduchý způsob proniknutí pachatelé do objektu. Především by se mělo brát zřetel na dveře a okna, kterými se pachatel do budovy dostane nejpravděpodobněji. Plášť a otvorové výplně jsou zobrazeny na následujícím zjednodušeném schématu:



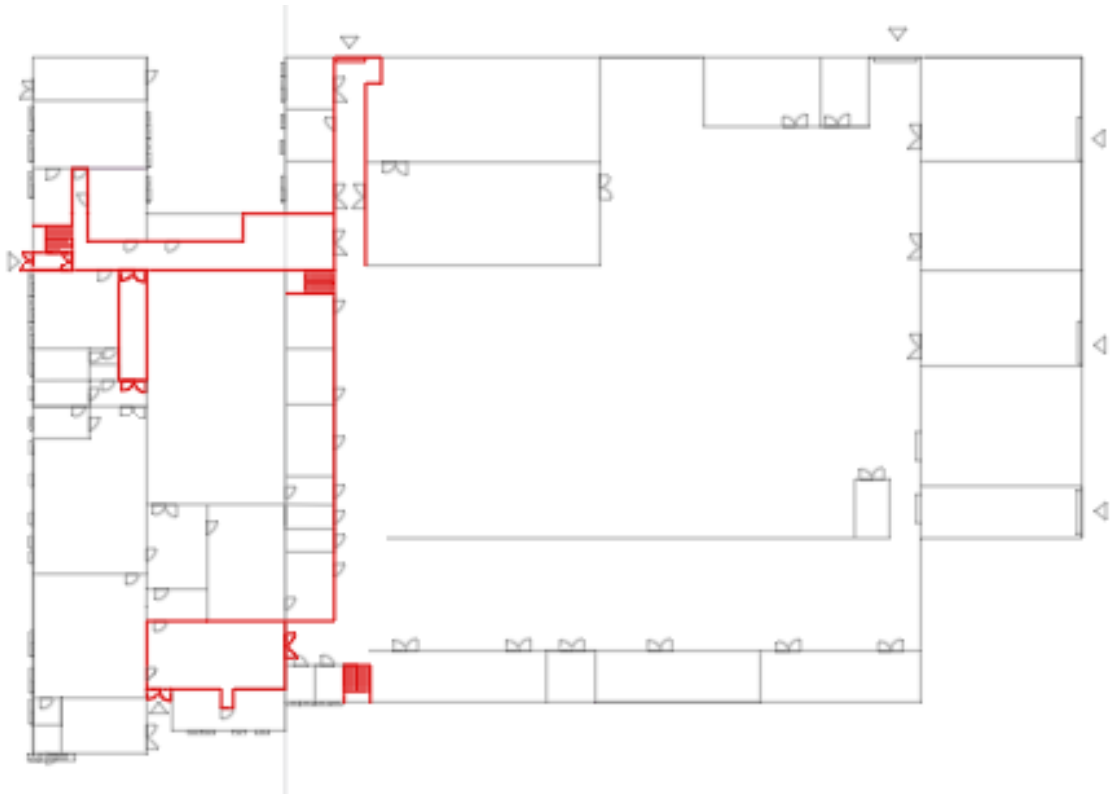
Obr. 44: Zobrazení pláště v přízemí a 1.NP



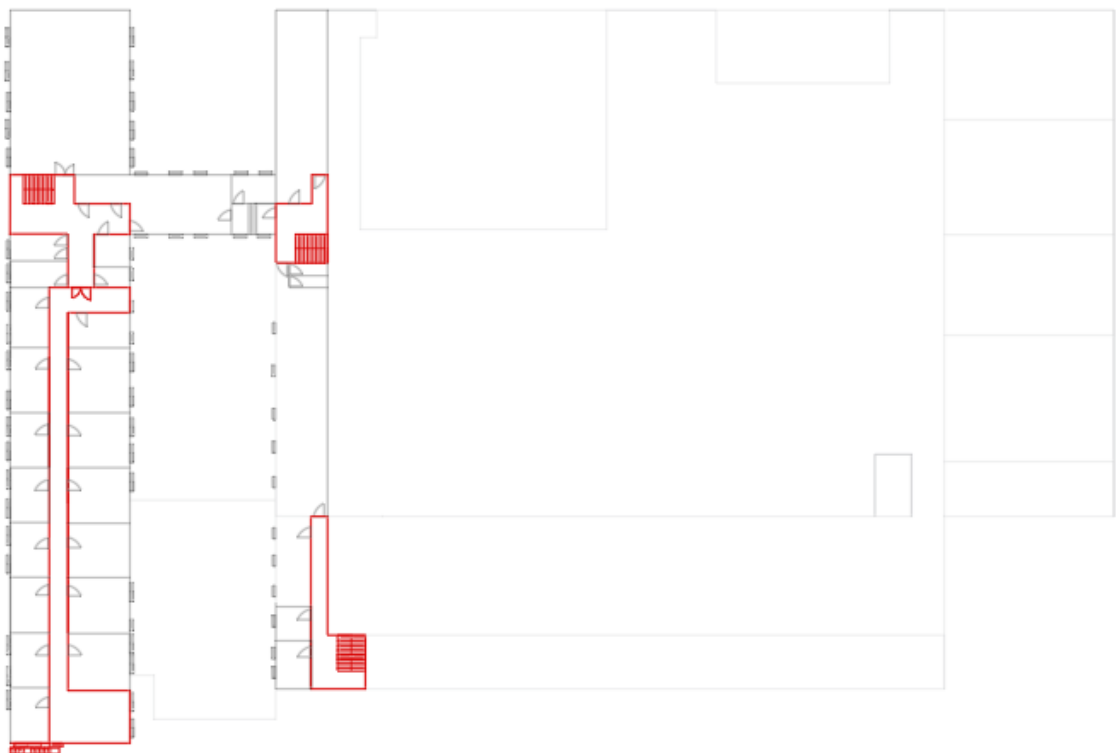
Obr. 45: Zobrazení pláště v 2.NP

### 6.3.3 Chodby, schodiště

Chodby a schodiště jsou prostory, kterým pachatel může proniknout do dalších částí budovy. Zabezpečení těchto prostor by nemělo být podceňováno. Zejména požární schodiště představuje vysoké riziko proniknutí pachatele do prostor administrativy. Nejčastěji se nacházejí u vstupů do budovy.



Obr. 46: Zobrazení chodeb a schodišť v přízemí a 1.NP



Obr. 47: Zobrazení chodeb a schodišť v 2.NP

## 7 BEZPEČNOSTNÍ ANALÝZA

Pro bezpečnostní analýzu byla zvolena mapová analýza rizik.

Posuzují se tyto dva faktory:

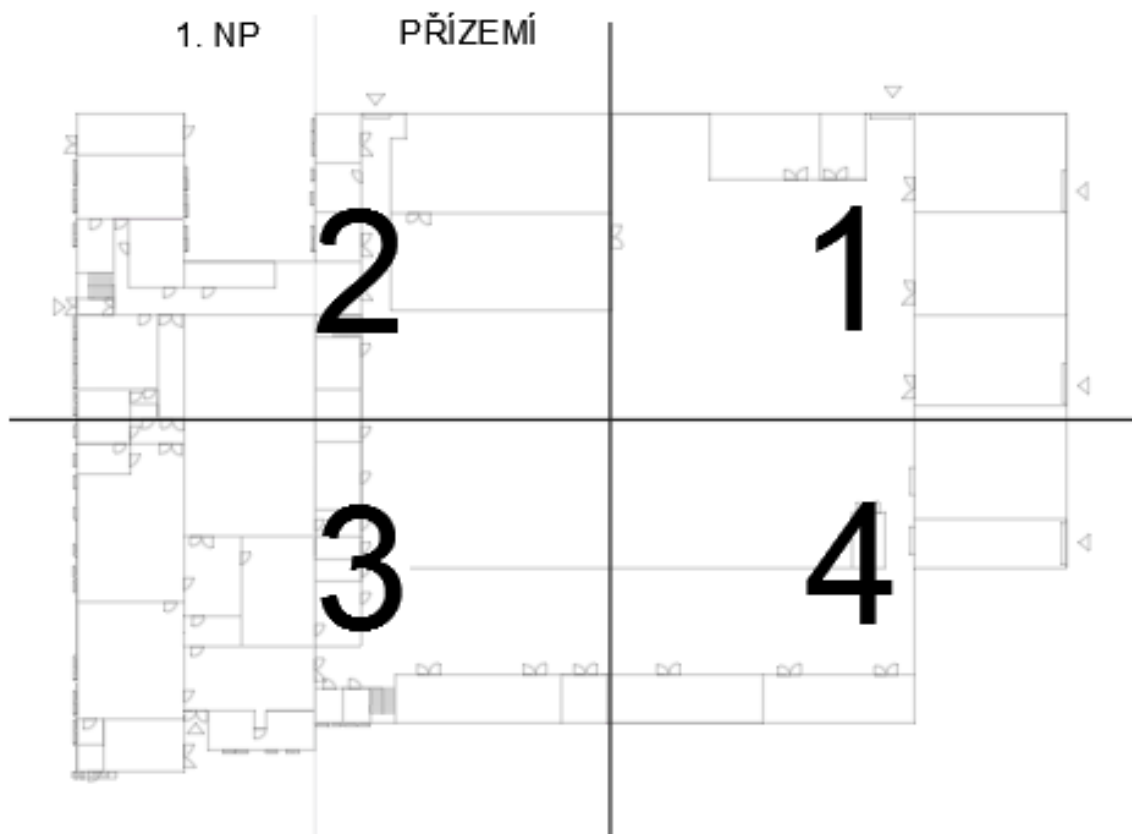
- osoby,
- aktiva.

Dále se vycházelo z následujících kritérií:

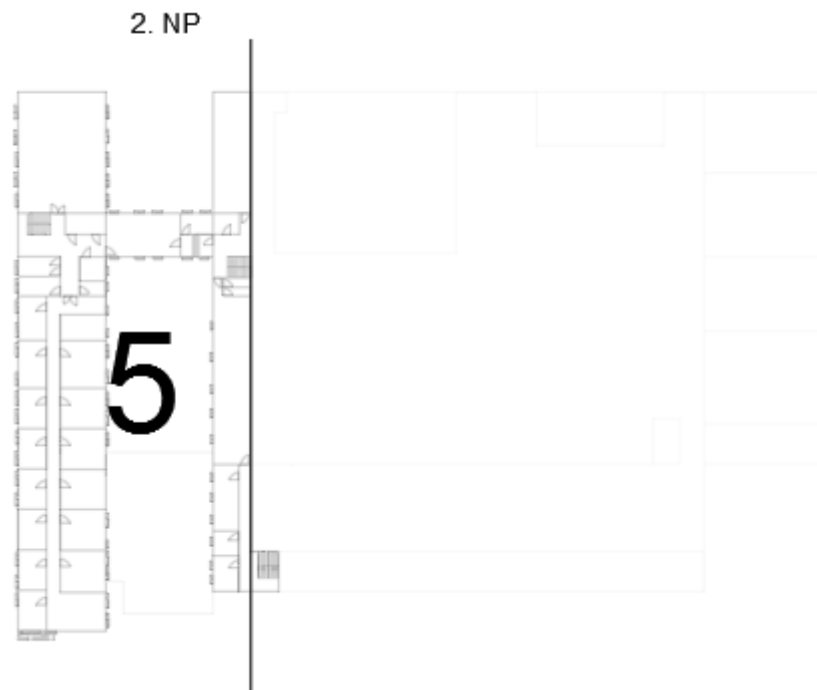
- hodnota,
- zranitelnost, pravděpodobnost,
- závažnost hrozby.

Vzhledem k rozsahu objektu a areálu, bylo schématické zobrazení rozděleno na 5 částí.

Jsou rozděleny následovně:



Obr. 48: Rozdělení zobrazení 1.NP a přízemí pro bezpečnostní analýzu



Obr. 49: Rozdělení zobrazení 2.NP pro bezpečnostní analýzu

Na jednotlivé části byla promítnuta mřížka, která rozdělila zobrazení na jednotlivé buňky, které byly následně ohodnoceny.

### **Hodnota**

Prvním kritériem je hodnota. Ta vychází z otázky – jaká velká hodnota se v prostoru nachází?

Byla zvolena škála 1-10, kde hodnota 1 představuje mizivý dopad, 10 závažný dopad.

Uvažovaly se především následující faktory:

- finanční hodnota majetku,
- poškození,
- nebezpečí pro osoby a okolní prostředí.

Jednotlivé části výpočtu lze najít v příloze P5.

### **Zranitelnost, pravděpodobnost**

Dalším kritériem je zranitelnost a pravděpodobnost. Jednotlivé hodnoty byly určeny na základě následující otázky: jaká je pravděpodobnost využití zranitelnosti prostoru?

Byla zvolena škála 1-10, kde hodnota 1 představuje prostor s nízkou pravděpodobností využití zranitelnosti a 10 vysoké riziko využití zranitelnosti.



Uvažovaly se především následující faktory:

- pravděpodobnost vzniku nebezpečí,
- množství pohybujících se osob, kterým hrozí nebezpečí;
- zpeněžitelnost majetku,
- odcizitelnost.

Jednotlivé části výpočtu lze najít v příloze P6.

### **Závažnost hrozby**

Posledním kritériem je závažnost hrozby. Byla určena položením následující otázky: Jak závažný bude mít dopad, pokud dojde k uskutečnění hrozby?

Byla zvolena škála 1-3, ve které jednotlivé číslice představují následující:

- **1 – zanedbatelný,**
- **2 – značný,**
- **3 – velmi závažný.**

Uvažovaly se především následující faktory:

- újma společnosti při uskutečnění hrozby,
- závažnost hrozby.

Jednotlivé části výpočtu lze najít v příloze P7.

## **7.1 Provedení analýzy**

Poté, co jednotlivá kritéria byla vyhodnocena, bylo vypočteno celkové vyhodnocení rizika v prostoru pomocí následujícího vzorce:

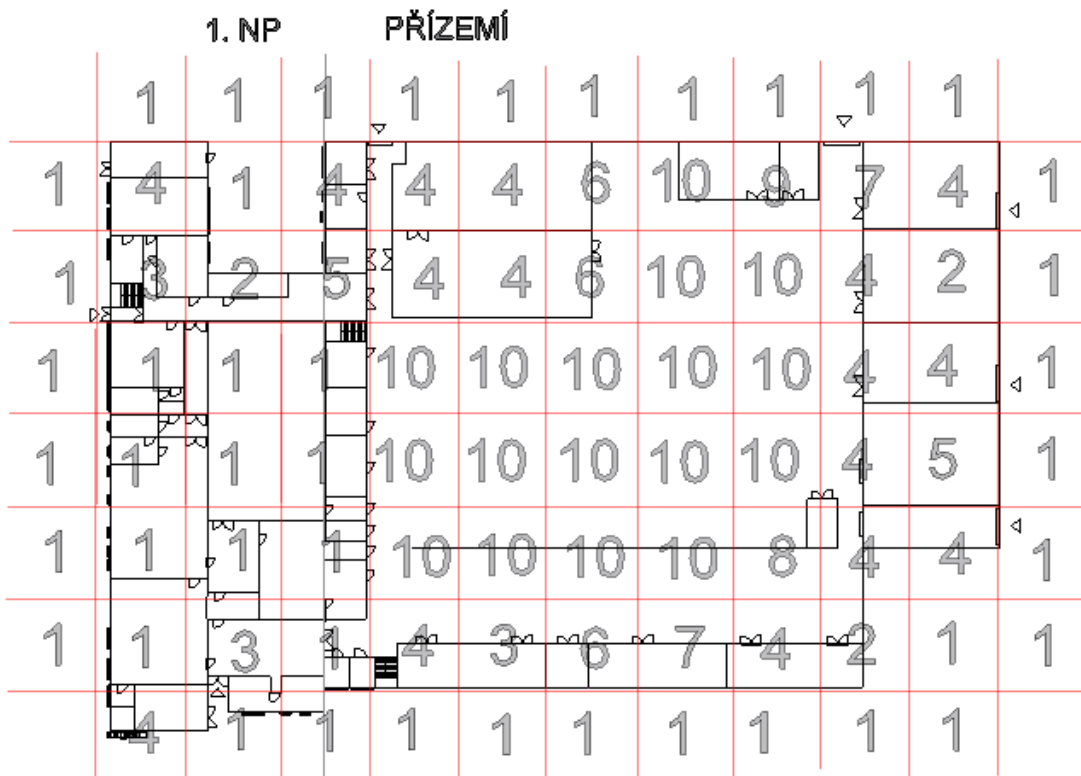
$$\text{Riziko} = \text{Hodnota} \times \text{Zranitelnost, pravděpodobnost} \times \text{Závažnost hrozby}$$

Pro vhodnější zobrazení byl proveden následující matematický krok, kterým bylo dosaženo ohodnocení jednotlivých polí škálou čísel 1-10:

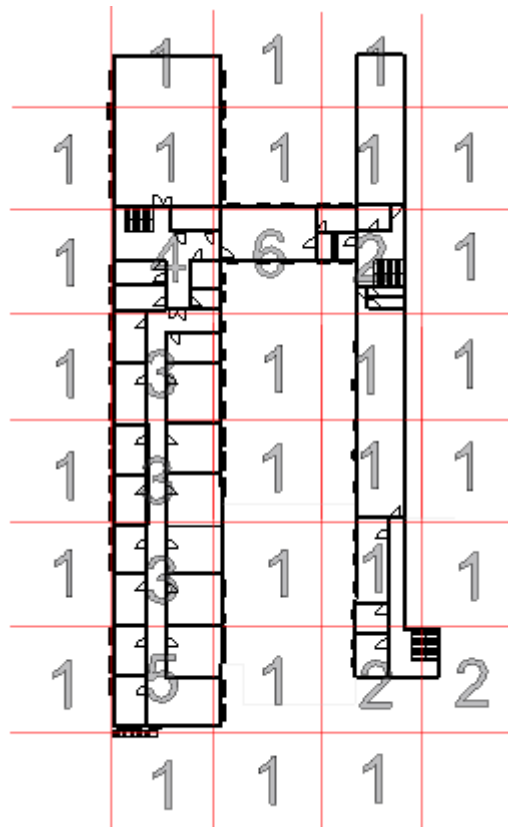
$$\text{Zobrazené riziko} = \text{Riziko} / 30$$

Byla zvolena mřížka o vhodné velikosti, která rozdělila objekt na jednotlivé části, které byly následně ohodnoceny dle zadaného kritéria.

Výsledkem je následující mapová analýza rizik:

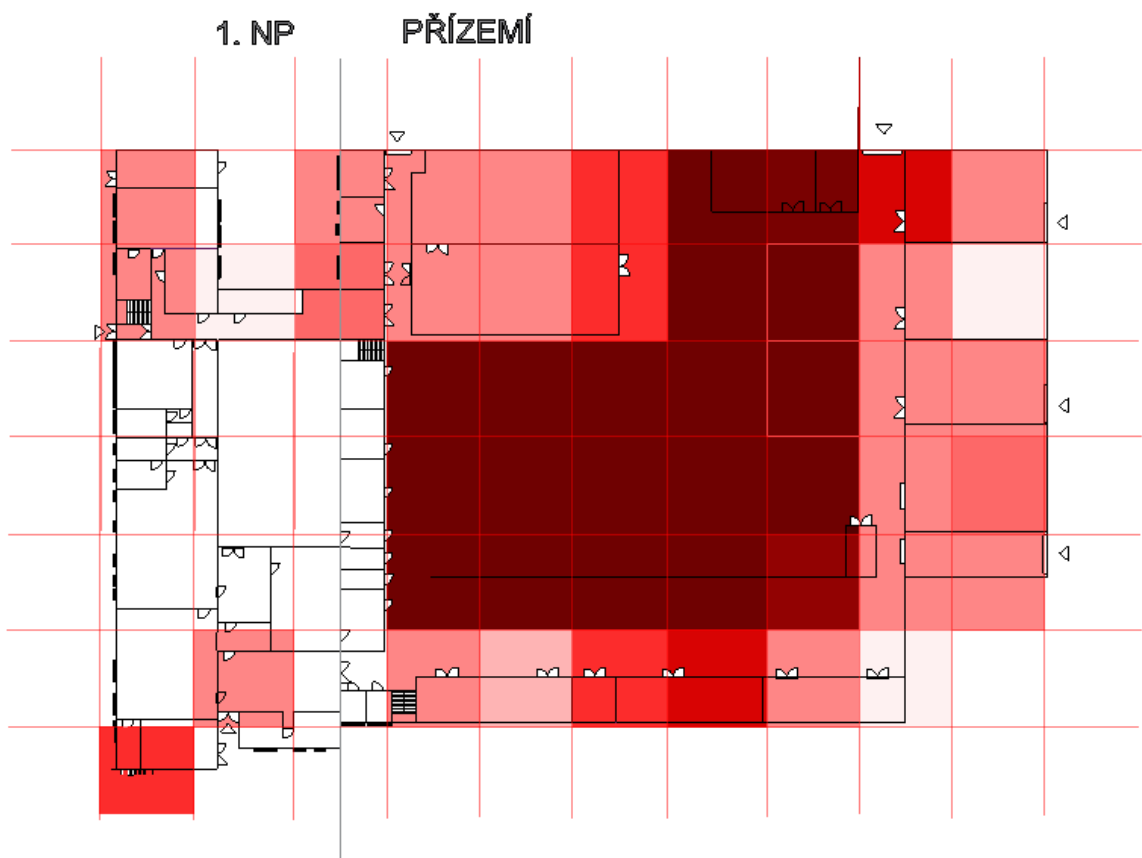


Obr. 50: Mapová analýza rizika přízemí a 1.NP

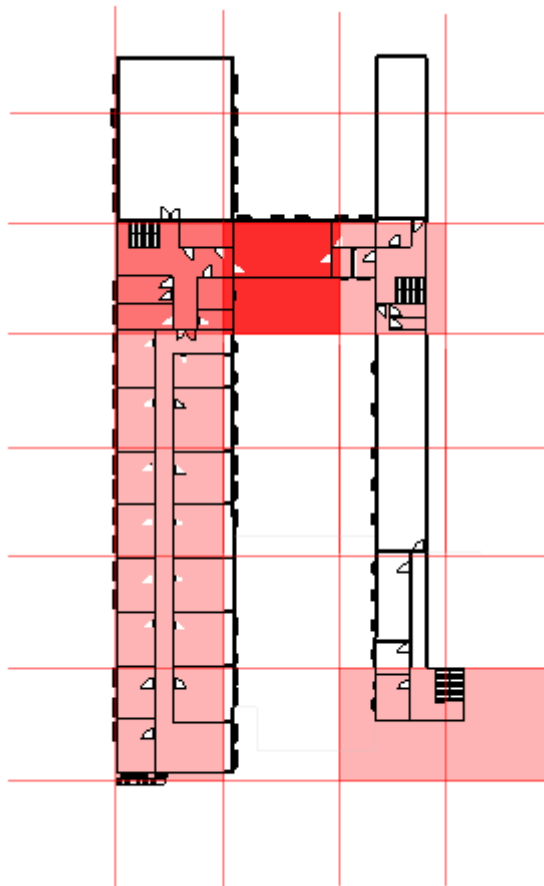


Obr. 51: Mapová analýza rizik 2.NP

Pro relevantnější přehled slouží následující barevné zobrazení pomocí gradientu:



Obr. 52: Barevné zobrazení rizik pomocí gradientu, přízemí a 1.NP



Obr. 53: Barevné zobrazení rizik pomocí gradientu, 2.NP

Škála barev vychází z následujícího obrázku:



Obr. 54: Škála barev

Platí pravidlo: s narůstající hodnotou je odstín červené barvy tmavší.

## 7.2 Vyhodnocení analýzy

Ze zobrazení rizik pomocí gradientu lze vypožorovat, že největší riziko se bude nacházet ve výrobních prostorech a skladech. Dalšími rizikovými prostory jsou vstupy do budovy a schodiště.

Z výsledků bezpečnostní analýzy je jasné, že je relevantnější pro VSS, než pro I&HAS, jelikož do bezpečnostní analýzy nebyly zahrnuty hrozby týkající se pláště budovy. Perimetr také nemá vypovídající hodnotu. Pro návrh zabezpečení perimetru bude využito výsledků bezpečnostního posouzení.

## 8 NÁVRH SYSTÉMU

System byl navržen na základě výsledků bezpečnostního posouzení, bezpečnostní analýzy a požadavků zákazníka. Bylo dodrženo zásad umístování jednotlivých zařízení získaných z technických norem.

### 8.1 I&HAS

#### 8.1.1 Stupeň zabezpečení

Na základě syntézy získaných informací z jednání se zákazníkem a bezpečnostního posouzení byl zvolen následující stupeň zabezpečení:

#### stupeň zabezpečení 2 – nízké až střední riziko

Důvod volby stupně zabezpečení je předpoklad, že narušitel má základní znalosti o systému a že použije základní sortiment nástrojů a přenosných přístrojů. Rozhodnutí o stupni zabezpečení vychází také ze samotného umístění posuzovaného objektu a účelu jeho využití.

Tab. 22: O – otevření, P – průnik, T – past, S – objekty vyžadující speciální pozornost

Střeží se	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Obvodové dveře	0	0	OP	OP
Okna		0	OP	OP
Ostatní otvory		0	OP	OP
Stěny			P	P
Stropy nebo střechy			P	P
Podlahy				P
Místnosti	T	T	T	T
Objekt (vysoké riziko)			S	S

#### 8.1.2 Typy napájení

Minimální doba napájení náhradním napájecím zdrojem v hod. na základě ČSN EN 50 131-1:

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Typ A	12	12	60	60
Typ B	24	24	120	120

### 8.1.3 Třída prostředí

Pro posuzovaný objekt byla zvolena následující třída prostředí:

#### II. třída prostředí

Je definována:

- vnitřní všeobecné prostředí,
- rozsah teplot – 10° C až + 40° C,
- vlivy prostředí vyskytující se obvykle ve vnitřních prostorech při nestálé teplotě, například chodby a schodiště, nevytápěné prostory.

Tato zvolená třída prostředí plně vyhovuje danému objektu.

### 8.1.4 Legenda místností

Tab. 23: Popis místnosti v přízemí

103	Otrýskání forem
104	Rezerva
105	Kontrola
107	Sklad
108	Chladný sklad
109	Omražování
110	Kompresorovna
111	Sklad hotových výrobků
112	Vstupní kontrola
118	Dovulkanizační pece
119	Nanášení spojovacích prostředků
121	Hala gumovýroba
122	Komunikační prostor
123a	Vstupní sklad
123b	Údržba, čištění a sklad forem

124	Kontrola a sklad hotových výrobků
126	Hala plastová výroba
135	Kuchyně
139	Údržba
140	Kancelář mistrů
146	WC

Tab. 24: Popis místnosti v 1.NP

106	Šatna muži
113	Šatna ženy
116	Sprchy ženy
121	Jídelna
124d	Příprava jídel
125	Trafostanice
126	Denní místnost
133a	Chodba
150	Atrium
154	Trafostanice
155	Chodba
156	Technická místnost

Tab. 25: Popis místností v 2.NP

106	Šatna muži
113	Šatna ženy
201	Zasedací místnost
204	Vedení společnosti
204	Místnost VZT
216	Kancelář
222	Volný prostor
231	Kancelář
232	Serverovna

### 8.1.5 Rozmístění prvků

Rozmístění jednotlivých prvků je uvedeno v příloze P1 a P2.

Rozmístění prvků vychází z rozdělení do 5 částí, které bylo použito v bezpečnostním posouzení.

Legenda:

	PIR detektor
	PIR detektor s dlouhým dosahem
	Magnetický detektor
	Magnetický vratový detektor
	Siréna
	Expandér
	Napájení 12V
	Klávesnice
	Tišňový hlásič
	Ústředna I&HAS

Obr. 55: Legenda prvků



### 8.1.6 Použité technické vybavení

#### Varianta 1 – Satel

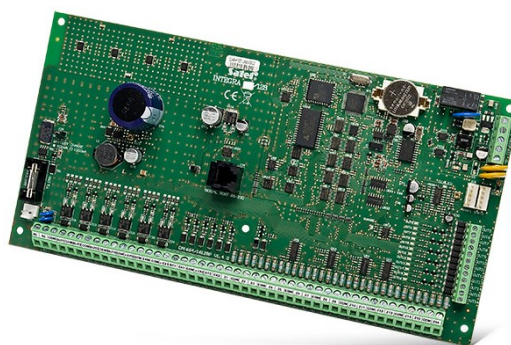
#### Ústředna

#### Integra 128

Zabezpečovací ústředna nabízí kromě funkce ohlašování poplachu i možnost realizace systémů automatizace a kontroly vstupu. Je rozšiřitelná o širokou nabídku externích modulů, které umožňují využít systém v rozsáhlých systémech.

Tab. 26: Specifikace ústředny Integra 128 [40]

Třída prostředí	II
Napětí zdroje ústředny ( $\pm 10\%$ )	13,8 V DC
Zatížení nízko zatížitelných programovatelných výstupů	50 mA
Zatížení vysoko zatížitelných programovatelných výstupů	3000 mA
Proudový výkon zdroje	2,5 A
Rozsah pracovních teplot	-10...+55 °C
Napájecí napětí základní desky ( $\pm 15\%$ )	20 V AC, 50-60 Hz
Proudová spotřeba v klidu	149 mA
Max. proudová spotřeba	337 mA



Obr. 56: Základní deska ústředny Integra 128 [40]

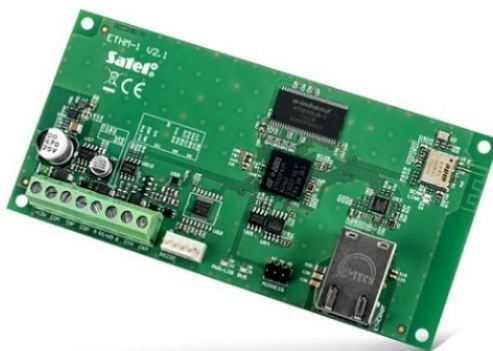
## Komunikační modul

### ETHM-1 Plus

Komunikační modul ETHM-1 Plus umožňuje využívat komunikaci po TCP/IP pro ústředny INTEGRA. Umožňuje připojení na PCO po TCP/IP a dálkové programování ústředěn. Ve spojení s ústřednami INTEGRA umožňuje modul ETHM-1 Plus dálkové ovládání systému přes síť INTERNET pomocí počítače, tabletu nebo chytrého telefonu. [40]

Tab. 27: Specifikace komunikačního modulu ETHM-1 Plus [40]

Proudová spotřeba v klidu	70 mA
Maximální proudová spotřeba	80 mA
Napájecí napětí	12 V DC



Obr. 57: ETHM-1 Plus TCP/IP komunikační modul [40]

### Zdroj napájení

#### APS-30

Pulzní zdroj určený pro napájení zařízení zabezpečovacích systémů napájecím napětím 12 V. Proudový výkon zdroje činí 3 A. [40]

### Expandér

#### INT-E

Model určený pro ústředny Integra. Umožňuje rozšíření o 8 drátových zón s dodatečným vstupem pro tamper usnadňující detekci otevření krytu. [40]

Tab. 28: Specifikace INT-E [40]

Napájecí napětí ( $\pm 15\%$ )	12 V DC
Proudová spotřeba v klidu	35 mA
Max. proudová spotřeba	80 mA



Obr. 58: INT-E expandér [40]

## Klávesnice

### INT-KLCD-GR

LCD klávesnice je určena pro systémy Integra. Díky LCD displeji, na kterém jsou zobrazována textová hlášení, je možné využívat i složité funkce zabezpečovací ústředny jednoduše a pohodlně. [40]

Tab. 29: Specifikace LCD klávesnice INT-KLCD-GR [40]

Napájecí napětí ( $\pm 15\%$ )	12 V DC
Proudová spotřeba v klidu	17 mA
Max. proudová spotřeba	101 mA



Obr. 59: LCD klávesnice INT-KLCD-GR [40]

## Magnetický detektor

### S-1

Detektor S-1 je určen pro povrchovou montáž přichycením šrouby na montážní povrch např. k rámu dveří nebo oken. S-1 se skládá ze dvou voděodolných částí: jazýčkového kontaktu (magnetický senzor) a magnetu. Dále je detektor vybaven tamper smyčkou. [40]

Tab. 30: Specifikace magnetického detektoru S-1 [40]

Maximální spínané napětí přes kontakt	20 V
Maximální spínaný proud	20 mA



Obr. 60: Magnetický detektor S-1 [40]

### Magnetický vratový detektor

#### B-4S

Kovová chránička vodičů slouží k jejich ochraně před poškozením, umožňuje tak ideální řešení v místech s možností sabotáže nebo většímu mechanickému namáhání. Magnety se připevňují na povrch pomocí šroubů a jsou určeny pro montáž na garážová vrata. [40]

Tab. 31: Specifikace magnetického vratového detektoru B-4S [40]

Maximální spínané napětí přes kontakt	100 V
Maximální spínaný proud	400 mA



Obr. 61: Magnetický vratový detektor B-4S [40]

### PIR detektor

#### Aqua Pro

AQUA Pro je digitální pasivní infračervený detektor osazený čtyřmi PIR senzory a algoritmem digitální detekce pohybu. Díky dvoucestné analýze signálu z PIR senzoru (hodnota a kvantita) a teplotní kompenzací je zařízení určené pro širokou škálu okolních teplot, s vysokou citlivostí a imunitou vůči falešným poplachům. [40]

Tab. 32: Specifikace PIR detektoru Aqua Pro [40]

Průměrná proudová spotřeba	10 mA
Maximální proudová spotřeba	12 mA
Detekovatelná rychlost pohybu	0,3...3 m/s
Třída prostředí	II



Obr. 62: PIR detektor Aqua Pro [40]

### PIR detektor s dlouhým dosahem

Pro PIR detektor s dlouhým dosahem byl použit detektor Aqua Pro s dodávanou výměnnou čočkou, určenou pro pokrytí dlouhých chodeb.

### Siréna

SP-4006 R [40]

SP-4006 R je akusticko-optická siréna, vybavená vysoce svítivými LED a piezo měničem. Dvě sady optické signalizace po obou stranách zajišťují zvýšení viditelnosti poplachu z větší dálky a za denního světla. Na výběr je jeden ze tří modulovaných signálů s intenzitou 120 dB, s možností omezení doby trvání akustické signalizace na 1, 5, 10 a 15 minut. Sirénu lze doplnit o akumulátor 1,2 Ah, 6 V, který je umístěn uvnitř krytu a zajišťuje tak záložní napájení.

Tab. 33: Specifikace sirény SP-4006 R [40]

Třída prostředí	III
Maximální proudová spotřeba	400 mA
Proudová spotřeba v klidu	40 mA
Napájecí napětí	12 V DC

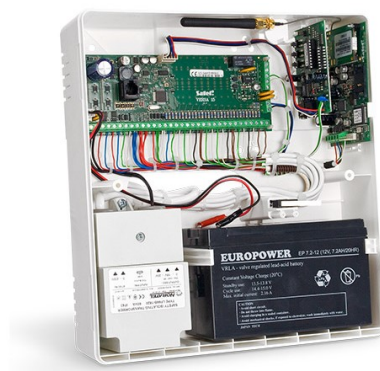


Obr. 63: Siréna SP-4006 R [40]

## Kryt

OPU-4

Kryt z bílého ABS plastu pro povrchovou montáž, s prostorem pro transformátor. [40]



Obr. 64: OPU-4 [40]

## Transformátor

TR 40 VA



Obr. 65: TR 40 VA [40]

## Prvky tísňové ochrany

### PNK-1

PNK-1 je tísňové tlačítko s pamětí pro spuštění okamžitého poplachu nebo spuštění přenosu tísňové události na PCO v případě ohrožení života nebo majetku. Zařízení se používá například v objektech, kde hrozí riziko napadení, včetně bank, směnárén, obchodů, skladů, kanceláří, atd. [40]

Tab. 34: Specifikace tísňového hlásiče PNK-1 [40]

Maximální proudová spotřeba	250 mA
-----------------------------	--------



Obr. 66: Tísňový hlásič PNK-1 [40]

### Záložní akumulátor

Byl zvolen akumulátor o kapacitě 24 Ah.

#### *Výpočet záložního napájení*

Pro určení vhodného akumulátoru bylo nutné provést výpočet proudového odběru jednotlivých komponentů v klidu:

Tab. 35: Výpočet kapacity záložního zdroje napájení

Komponent I&HAS	Modelové označení	Množství	Odběr [mA]	Odběr v zátěži [mA]
Ústředna	Integra 128	1	149	357
Komunikační modul	ETHM-1 Plus	1	70	80
Expandér	INT-E	11	11*35	11*80
Klávesnice	INT-KLCD-GR	1	17	101
Magnetický detektor	S-1	56	0	56*20

<b>Magnetický vratový det.</b>	B-4S	5	0	400*5
<b>PIR detektor</b>	Aqua Pro	19	19*12	19*12
<b>Celkem:</b>			836	4766

Celkový odběr teda činí 636 mA

Pro orientační určení kapacity záložního zdroje se odběr vynásobí počtem hodin na základě stupně zabezpečení.

**Celkový odběr v klidu x počet hodin = minimální požadovaná kapacita akumulátoru**

$$636 \times 24 = 20,064 \text{ Ah}$$

## Varianta 2 – Paradox

### Ústředna

#### EVO192PCB

EVO192 je největší ze zabezpečovacích ústředn Digiplex EVO. Jde o plně adresovatelný sběrniceový systém, do kterého lze zařadit až 254 sběrniceových modulů (klávesnice, bezdrátová nastavba, expandéry, PGM výstupy, doplňkové zdroje, posilovač sběrnice, hlasová nastavba) i samostatné sběrniceové detektory BUS. [41]

Tab. 36: Specifikace ústředny EVO192PCB [41]

Napětí zdroje ústředny ( $\pm 10\%$ )	16 V DC
Proudový odběr ústředny:	100 mA
Počet zón	16
Počet PGM	5
Počet podsystémů	8



Obr. 67: Ústředna EVO192PCB [41]



**Expandér**

ZX8

Sběrníkový modul rozšíření systému o 8 zón

Tab. 37: Specifikace expandéru ZX8 [41]

Napětí zdroje ústředny ( $\pm 10\%$ )	9-16 V DC
Proudový odběr	28 mA
Počet zón	8
Počet PGM	1



Obr. 68: Expandér ZX8 [41]

**Komunikační modul**

IP150SWAN

Ethernetový komunikační modul Paradox IP150SWAN umožňuje vzdálený přístup k ústřednám EVO192 [41]

Tab. 38: Specifikace komunikačního modulu EVO192 [41]

Třída prostředí	II
Proudový odběr	110 mA



Obr. 69: Komunikační modul IP150SWAN [41]

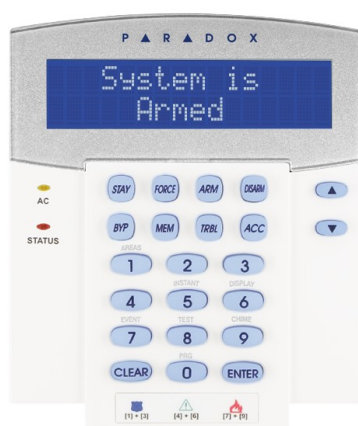
**Klávesnice**

K641

Pomocí této klávesnice lze systém jednoduše a rychle ovládat, přehledně zobrazovat informace o stavu systému a modifikovat parametry a funkce systému. Displej se 32 znaky zobrazuje všechny základní stavy a napovídá postupy ovládání systému. Pomocí této LCD klávesnice K641R, může být ovládán systém Digiplex 848/96NE i ústředny EVO48/96/192/HD [41].

Tab. 39: Specifikace klávesnice K641R [41]

Napětí zdroje ústředny ( $\pm 10\%$ )	9-16 V DC
Proudový odběr	120 mA



Obr. 70: Klávesnice K641 [41]

### Magnetický detektor

USP1000

Magnetický kontakt se svorkovnicí, přípojovací kabel je umístěn pod krytkou. Tento magnetický detektor je určen pro plošnou montáž na nevodivé i vodivé materiály. [41]

Tab. 40: Specifikace magnetického detektoru USP1000 [41]

Pracovní vzdálenost	25 mm
Typ kontaktu	NC



Obr. 71: USP1000 [41]

### Magnetický vratový detektor

#### USP3000SP

Kovový magnetický kontakt USP-3000 je masivní kontakt určený pro velké dveřní systémy a vrata. Kabel tohoto magnetu je ochráněn pancéřovým krkem, který je tak chráněn před porušením. [41]

Tab. 41: Specifikace magnetického vratového detektoru [41]

Pracovní vzdálenost	57 mm
Typ kontaktu	NC



Obr. 72: USP3000SP [41]

### PIR detektor

#### DG65+

Pohybový detektor s čtyřnásobným prvkem. Toto čidlo má patentovanou technologii digitálního zpracování. Princip digitální technologie je založen na eliminaci analogových komponentů (zesilovačů) mezi senzorem a procesorem určeným pro další digitální zpracování informace. [41]

Tab. 42: Specifikace PIR detektoru DG65+ [41]

Třída prostředí	II
Napájení	11-16 V DC
Proudový odběr	15 mA



Obr. 73: DG65+ [41]

**PIR s dlouhým dosahem**

LR1 čočka s dosahem 35 m.

**Siréna**

PS128

PARADOX PS 128 je zálohovaná siréna...Obsahuje výstup REPORT, který umožňuje předávat do ústředny informace o stavu baterie, reproduktoru a světla. Další inovací je servisní vstup sirény, který přepíná sirénu do servisního módu, ve kterém lze sirénu bezpečně otevřít a jakkoliv s ní manipulovat. Mód úspory energie zabraňuje úbytku na zvukové a světelné intenzitě a prodlužuje životnost baterie. [41]

Tab. 43: Specifikace sirény PS128 [41]

Třída prostředí	III
Napájení	13,6 – 14,8 V DC
Proudový odběr v klidu	5 mA



Obr. 74: PS128 [41]

**Tísňový hlásič**

DMN700L

DMN700R je červený tlačítkový požární hlásič pro zapuštěnou montáž. V sérii se spínacím kontaktem má vestavěný odpor 680 Ohm, a navíc obsahuje druhý spínací kontakt. [41]

Tab. 44: Specifikace tísňového hlásiče DMN700L

Proudový odběr v klidu	0 mA
------------------------	------



Obr. 75: DMN700L [41]

**Transformátor, zdroj napájení**

Transformátor i zdroj napájení byl použit totožný s variantou 1.

**Záložní akumulátor**

AKU CJ-12/18Ah

Byl zvolen akumulátor o kapacitě 18 Ah.

*Výpočet záložního napájení*

Pro určení vhodného akumulátoru bylo nutné provést výpočet proudového odběru jednotlivých komponentů v klidu:

Tab. 45: Výpočet kapacity záložního zdroje napájení

Komponent I&HAS	Modelové označení	Množství	Odběr [mA]
Ústředna	EVO192PCB	1	100
Expandér	ZX8	11	11*28
Komunikační modul	IP150SWAN	1	110
Klávesnice	K641R	1	120
Magnetický detektor	USP1000	56	0

<b>Magnetický vratový detektor</b>	USP3000SP	5	0
<b>PIR detektor</b>	DG65+	20	15*20=300
<b>Siréna</b>	PS128	4	5*4=20
<b>Celkem:</b>			678

Celkový odběr teda činí 678 mA

Pro orientační určení kapacity záložního zdroje se odběr vynásobí počtem hodin na základě stupně zabezpečení.

**Celkový odběr v klidu x počet hodin = minimální požadovaná kapacita akumulátoru**

$$678 \times 24 = 16,272 \text{ Ah}$$

Vzhledem k tomu, že nebylo možné získat detailní informace o parametrech jednotlivých prvků, nelze spočítat proudový odběr systému v zátěži.

### 8.1.7 Kabeláž

Pro kabeláž propojení detektorů s expandéry a ústřednou byla napočítána délka 2160 m.

Byl zvolen typ kabelu s označením VD-06.

### 8.1.8 Zóny

Zákazník nspecifikoval požadavky na rozdělení zabezpečovacího systému na jednotlivé systémy, systém tedy nebyl rozdělen na podsystémy.

Rozdělení a popis zón je uveden v příloze P3.

## 8.2 VSS

Systém byl navržen na základě výsledků bezpečnostního posouzení, bezpečnostní analýzy a požadavků zákazníka. Bylo dodrženo zásad umístování jednotlivých zařízení získaných z technických norem.

Byly zvoleny 3 typy kamer, které jsou určené do odlišných prostor a prostředí:

- **Kamera typ 1** – venkovní prostředí,
- **Kamera typ 2** – vnitřní prostředí, malé prostory,
- **Kamery typ 3** – vnitřní prostředí, velké prostory.

### 8.2.1 Zvolené komponenty

#### Varianta 1 – Samsung

Pro první variantu byl zvolen výrobce Samsung.

#### *Kamera typ 1*

Venkovní IP bullet kamera Wisenet Samsung XNO-8080R

Tab. 46: Parametry XNO-8080R [42]

Snímací prvek	1/1.8" 6M CMOS
Maximální rozlišení	2560 x 1920
Maximální snímková rychlost	25 FPS
Video komprese	H.264, H.265
Ohnisková vzdálenost objektivu	3,7 – 9,4 mm
IR přísvit	50 m



Obr. 76: XNO-8080R [42]

#### *Kamera typ 2*

Vnitřní IP dome kamera Wisenet Samsung XND-6080R

Tab. 47: Parametry XND-6080R [42]

Snímací prvek	1/2.8" PS Exmor CMOS (IMX136)
Maximální rozlišení	1920 x 1080
Maximální snímková rychlost	60 FPS
Video komprese	H.264, H.265, MJPEG
Ohnisková vzdálenost objektivu	2,8 - 12 mm
IR přísvit	30 m



Obr. 77: XND-6080R [42]

**Kamera typ 3**

Vnitřní IP doma kamera Wisenet Samsung XNV-8080R

Tab. 48: Parametry XNV-8080R [42]

Snímací prvek	1/1.8" 6M CMOS
Maximální rozlišení	2560 x 1920
Maximální snímková rychlost	30 FPS
Video komprese	H.264, H.265, MJPEG
Ohnisková vzdálenost objektivu	3,9 - 9,4 mm
IR přísvit	50 m



Obr. 78: XNV-8080R [42]

**NVR**

Vnitřní IP dome kamera Samsung Wisenet XRN-3010

Síťový rekordér Wisenet Samsung pro střední a větší aplikace.

Tab. 49: Parametry NVR XRN-3010 [42]

Počet videovstupů	až 64 IP zařízení
-------------------	-------------------



Maximální rozlišení obrazů	12 MPx
Maximální záznamová rychlost	300 Mb/s
Formát komprese	H.265 / H.264 / MJPEG / Wisestream
Max počet HDD	celkem 8 x SATA interních



Obr. 79: XRN-3010 [42]

## HDD

Western Digital DR-HDD-4TB

Pevný disk vhodný pro NVR s kapacitou 4TB.



Obr. 80: DR-HDD-4TB [42]

## Varianta 2 – Axis

Pro druhou variantu byl zvolen výrobce Axis.

### Kamera typ 1

Axis P1405-LE

Tab. 50: Parametry P1405-LE [43]

Snímací prvek	1/2.8" CMOS
Maximální rozlišení	1920x1080
Maximální snímková rychlost	25 FPS
Video komprese	H.264, MJPEG
Ohnisková vzdálenost objektivu	2,8 – 10 mm
IR přísvit	30 m



Obr. 81: P1405-LE [43]

**Kamera typ 2**

Axis M3025-VE

Tab. 51: Parametry M3025-VE [43]

Snímací prvek	1/2,7" CMOS
Maximální rozlišení	1920x1080
Maximální snímková rychlost	25 FPS
Video komprese	H.264, MJPEG
Ohnisková vzdálenost objektivu	3,6 mm
IR přísvit	ne



Obr. 82: M3025-VE [43]

**Kamera typ 3**

Axis P3367-V

Tab. 52: Parametry P3367-V [43]

Snímací prvek	1/3.2" CMOS
Maximální rozlišení	2592x1944
Maximální snímková rychlost	12 FPS
Video komprese	H.264, MJPEG

Ohnisková vzdálenost objektivu	3-9 mm
IR přísvit	ne



Obr. 83: P3367-V [43]

### NVR a HDD

Vzhledem k tomu, že výrobce Axis nedisponuje vlastním zařízením NVR, bylo zvoleno zařízení shodné s prvkem ve variantě 1.

#### 8.2.2 Praktické řešení

Umístění jednotlivých kamerových zařízení lze nalézt v příloze P4.

#### Kamera typ 1


Provozní vlastnosti kamery typu 1 jsou uvedeny v následující tabulce:

Tab. 53: Provozní vlastnosti kamery typu 1

Provozní vlastnosti	Charakteristika
Účel a použití	Monitorování vnějšího prostředí
Snímaný prostor	Vnější prostory
Zachytitelné aktivity	Pohyb osob a automobilů
Provoz	24 h


**Kamera typ 2**

Tab. 54: Provozní vlastnosti kamery typu 2

<b>Provozní vlastnosti</b>	<b>Charakteristika</b>
Účel a použití	Rekognoskace/identifikace osob
Snímaný prostor	Vnitřní prostory
Zachytitelné aktivity	Pohyb osob
Provoz	24 h
	

**Kamera typ 3**

Tab. 55: Provozní vlastnosti kamery typu 3

<b>Provozní vlastnosti</b>	<b>Charakteristika</b>
Účel a použití	Rekognoskace prostor výroby
Snímaný prostor	Vnitřní prostory
Zachytitelné aktivity	Pohyb vysokozdvížných vozíků a osob, manipulace s materiálem a produkty
Provoz	24 h
	

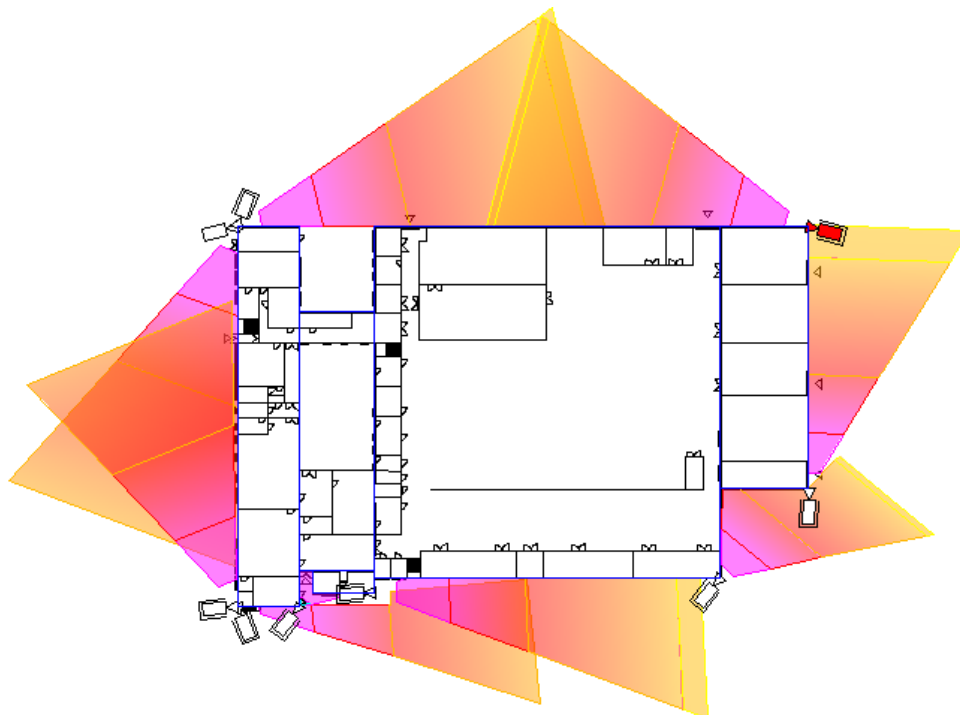
**Vizualizace**

K nevhodnějšímu rozmístění jednotlivých kamerových zařízení napomohla softwarová aplikace VideoCAD. Pomocí tohoto nástroje byly jednotlivé prvky vsazeny do půdorysu projektu, pro které byly nastaveny relevantní parametry. Výsledkem byla vizualizace, která umožnila celý systém optimalizovat a snížit tak finanční náklady spojené s realizací bezpečnostního projektu.

Vzhledem k rozsahu celého projektu, byly uvedeny pouze příklady.

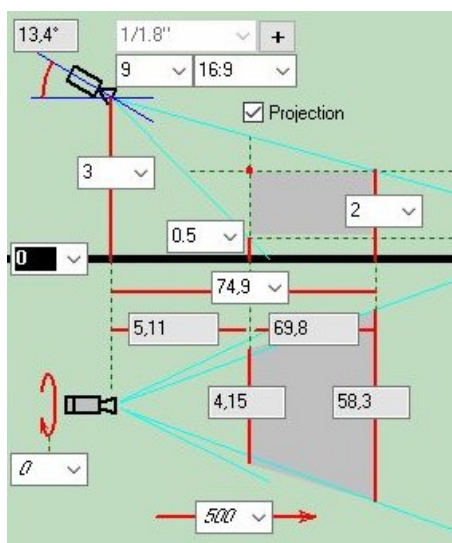
*Perimetr*

Na následujícím obrázku jsou zobrazeno zorná pole kamerových zařízení umístěných v perimetru objektu:



Obr. 84: Zorná pole kamerových zařízení v perimetru

Na následujícím obrázku je zobrazeno nastavení parametrů kamerového zařízení typ 1 (zobrazena na předchozím obrázku červeně):

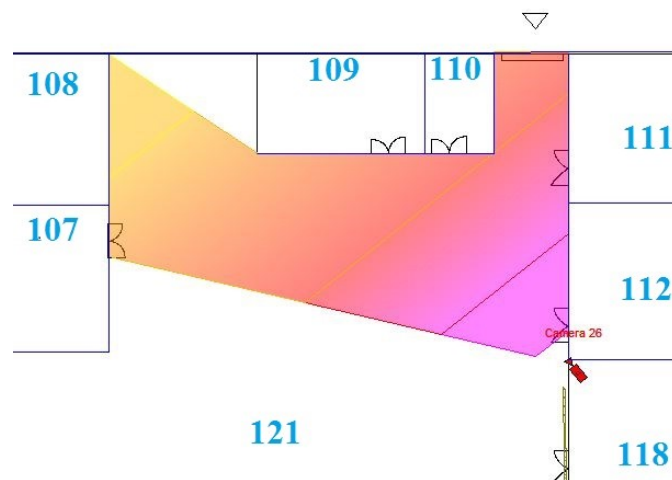


Obr. 85: Parametry kamery typ 1

Z obrázku lze vyčíst parametry jako je například výška instalované kamery – 3 m nebo nastavená ohnisková vzdálenost – 9 mm

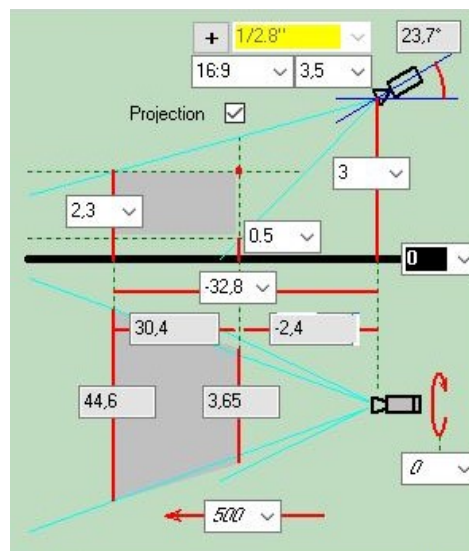
### *Výrobní hala*

Zorné pole kamerového zařízení zasahuje do částí, kde jsou nabíjeny vysokozdvizné vozíky a také na přístup do haly, které slouží k zásobování haly materiálem. Pomocí tohoto kamerového zařízení a inteligentních analytických funkcí lze ukládat státní poznávací značku kamionu, který bude sloužit ke zmíněnému zásobování výrobní haly.



Obr. 86: Zorné pole kamery typ 2

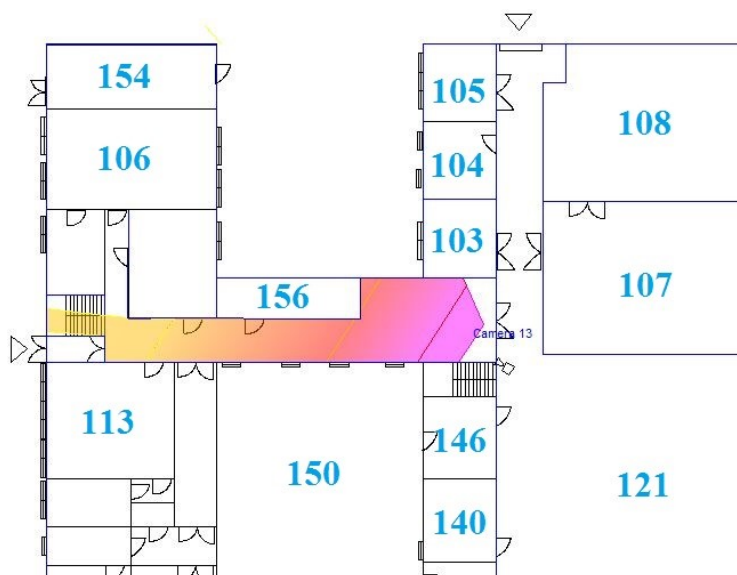
Z následujícího obrázku lze vyčíst nastavení kamerového zařízení.



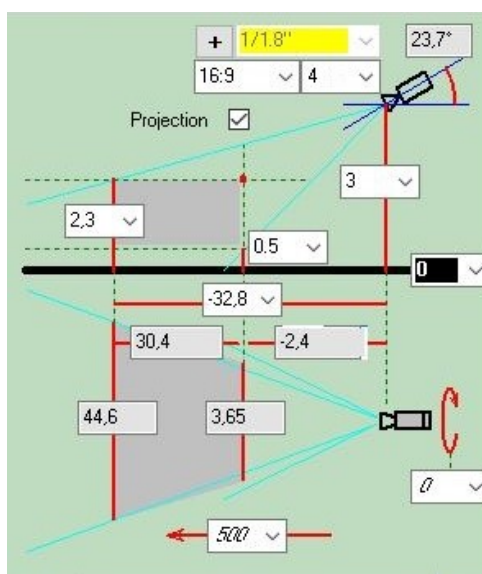
Obr. 87: Parametry kamery typ 2

### Chodba

Pomocí kamerového zařízení typ 3 byl zabezpečen prostor mezi hlavním vstupním vchodem a výrobní halou (121). Chodba slouží jako hlavní přístup do výrobní haly.



Obr. 88: Zorné pole kamery typ 3



Obr. 89: Parametry kamery typ 3

### 8.2.3 Úložný prostor

V následující části je vypočítán požadavek na úložný prostor.

Vzhledem k tomu, že v 1. variantě byly použity kamery, které disponují kompresním standardem H.265 a ve 2. variantě je použit kompresní standard H.264, je nutné vypočíst požadavek na úložný prostor jednotlivě.

Doba, po kterou bude uchováván záznam je stanoven na 2 dny.

Rozlišení bylo zvoleno nejvyšší, jaké konkrétní zařízení umožňuje.

#### Varianta 1

Tab. 56: Parametry výpočtu kapacity uložště Varianta 1

Model	Počet	sn/s.	Aktivita na scéně	Množství uložených dat
XNO-8080R	10	20	malá	954 GB
XND-6080R	8	20	střední	374 GB
XND-8080R	13	30	vysoká	1,9 TB
<b>Celkem:</b>				3,3 TB

Kalkulace byla provedena pomocí programu Bandwith Calculator společnosti Wisenet.

#### Varianta 2

Tab. 57: Parametry výpočtu kapacity uložště Varianta 2

Model	Počet	sn/s.	Aktivita na scéně	Množství uložených dat
P1405-LE	10	20	malá	538 GB
M3025-VE	8	20	střední	444 GB
P3367-V	13	12	vysoká	2,4 TB
<b>Celkem:</b>				3,4 TB



Kalkulace byla provedena pomocí programu Design Tool společnosti Axis.

Vzhledem k požadované kapacitě uložště je nutné zvolit pevný disk s dostatečnou velikostí i s ohledem na kapacitní rezervu. Pro obě varianty byly zvoleny 2 pevné disky s celkovou kapacitou 8TB.

### 8.3 Finanční náklady

V následující části je provedena kalkulační jednotlivých variant systémů.

Tab. 58: Finanční náklady, I&HAS – Varianta 1 - Satel

Varianta 1 Komponent I&HAS	Model	Počet	Cena za kus bez DPH	Cena za kus včetně DPH	Cena celkem bez DPH	Cena celkem s DPH
Ústředna	Integra 128	1	4811	5821	4811	5821
Komunikační modul	ETHM-1	1	3158	3821	3158	3821
Expandér	INT-E	11	932	1127	10252	12404
Klávesnice	KLCD-GR	1	2437	2949	2437	2949
Mag. detektor	S-1	56	115	146	6776	8198
Mag. vrat. detektor	B-4S	5	568	687	2840	3435
PIR detektor	Aqua Pro	20	626	757	12520	15150
Tísňový hlásič	PNK-1	12	230	278	2760	3400
Siréna	SP-4006R	4	1435	1736	5740	5945
Transformátor	TR VA 40	1	554	670	554	670
Kryt expandéru	OPU-1	11	274	332	3014	3647
Kryt ústředny	OPU-4	1	638	772	638	772
Kabeláž	VD-06 100 m	22	625	792	13750	17424
<b>Celkem [CZK]:</b>					<b>69250</b>	<b>83636</b>

Tab. 59: Finanční náklady, I&HAS – Varianta 2 - Paradox

Varianta 2 Komponent I&HAS	Model	Počet	Cena za kus bez DPH	Cena za kus včetně DPH	Cena celkem bez DPH	Cena celkem s DPH
Ústředna	EVO192PCB	1	4811	5773	4811	5773
Komunikační modul	IP150SWAN	1	3158	3790	3158	3790
Expandér	ZX8	11	1321	1585	14531	17437
Klávesnice	K641R	1	2437	2924	2437	2924
Mag. detektor	USP1000	56	115	138	6440	7728
Mag. vrat. detektor	USP3000SP	5	568	682	2840	3408
PIR detektor	DG65+	20	750	900	15000	18000
Tísňový hlásič	DMNL700L	12	342	410	4104	4925

Siréna	PS128	4	1350	1620	5400	6480
Transformátor	TR VA 40	1	554	670	554	670
Kryt expandéru	Box M-20	11	430	516	4730	5676
Kryt ústředny	Box M-40	1	890	1068	890	1068
Kabeláž	VD-06 100 m	22	625	750	13750	16500
<b>Celkem [CZK]:</b>					<b>78645</b>	<b>94379</b>

Tab. 60: Finanční náklady, VSS – Varianta 1 – Samsung

<b>Varianta 1 Komponent VSS</b>	<b>Model</b>	<b>Počet</b>	<b>Cena za kus bez DPH</b>	<b>Cena za kus včetně DPH</b>	<b>Cena celkem bez DPH</b>	<b>Cena celkem s DPH</b>
Vnější kamera typ 1	XNO-8080R	10	19570	23680	195700	236797
Vnitřní kamera typ 2	XND-6080R	8	13370	16178	106960	129422
Vnitřní kamera typ 3	XNV-8080R	13	19570	23680	254410	307836
NVR	XRN-3010	1	79286	95936	79286	95936
HDD	DR-4TB	2	4273	5170	8546	10340
<b>Celkem [CZK]:</b>					<b>644902</b>	<b>780331</b>

Tab. 61: Finanční náklady, VSS – Varianta 2 - Axis

<b>Varianta 2 Komponent VSS</b>	<b>Model</b>	<b>Počet</b>	<b>Cena za kus bez DPH</b>	<b>Cena za kus včetně DPH</b>	<b>Cena celkem bez DPH</b>	<b>Cena celkem s DPH</b>
Vnější kamera typ 1	P1405-LE	10	14707	17795	147070	177950
Vnitřní kamera typ 2	M3025-VE	8	12452	15067	99616	120536
Vnitřní kamera typ 3	P3367-V	13	22647	27405	294411	356265
NVR	XRN-3010	1	79286	95936	79286	95936
HDD	DR-4TB	2	4273	5170	8546	10340
<b>Celkem [CZK]:</b>					<b>628929</b>	<b>761027</b>

## ZÁVĚR

Cílem diplomové práce bylo vypracování návrhu bezpečnostního projektu areálu a objektu výrobní společnosti skládající se z I&HAS a VSS. V teoretické části byl zpracován a analyzován legislativní rámec těchto dvou systémů. Obecně se poplachovým zabezpečovacím a tísňovým systémům věnuje skupina norem ČSN EN 50131, videodohledové systémy upravuje skupina ČSN EN 62676. Provoz VSS upravuje zákon č. 101/2000 Sb., ve kterém jsou definovány podmínky provádění záznamu pořizovaných záběrů a využívání pořizovaných záběrů k identifikaci osob. Druhou zpracovanou kapitolou jsou technicko-technologické trendy, kde jsou popsány soudobé technologie. V dalších dvou kapitolách je čtenář seznámen s problematikou funkčních vlastností I&HAS a VSS, kde jsou dopodrobna rozepsány jednotlivé části těchto systémů, je popsán jejich princip funkce, jejich využití a další funkční parametry. V poslední kapitole teoretické části byl popsán postup tvorby návrhu bezpečnostního projektu, který vychází z technické normy ČSN EN 50131-7 pro I&HAS a z ČSN EN 62676-4 popisující VSS.

Praktická část se zabývala samotným návrhem bezpečnostního projektu. Nejprve bylo zapotřebí vypracovat bezpečnostní posouzení areálu a objektu, a poté provést analýzu. V bezpečnostním posouzení byla budova a areál rozdělena do několika funkčních částí, které byly dopodrobna popsány a posouzeny. Bezpečnostní analýza vycházela ze 3 základních faktorů. Těmi byla hodnota, zranitelnost a pravděpodobnost, a nakonec závažnost hrozby. Pomocí zvolené mřížky byl objekt rozdělen na jednotlivé segmenty, které byly následně ohodnoceny. Pomocí uvedeného vzorce bylo vypočteno riziko v jednotlivých segmentech, které mělo sloužit k návrhu zabezpečení. Z výsledků analýzy vyplynulo, že ji zcela nelze použít pro návrh I&HAS, ale pouze pro VSS. Veškeré komponenty a zařízení byly voleny na základě požadavků zákazníka a soudobých trendů při dodržení technických norem. Pro I&HAS i VSS byly jednotlivě zpracovány 2 varianty lišící se ve zvolených komponentech. První variantou zvolených komponentů v I&HAS byl systém od polské společnosti Satel, druhou byla česká společnost Paradox. Ve VSS byly uvedeny taktéž 2 varianty, jejíž první byly komponenty od společnosti Samsung, druhou variantou byla firma Axis. Celkem tedy byly zpracovány 4 varianty. Vzhledem k rozsahu zabezpečovaného podniku, finanční náklady jednotlivých variant se lišily pouze částečně. Při výpočtu minimálního požadovaného úložného prostoru k uchování záznamů pořízených VSS byla ověřena účinnost kompresního

standardu H.265 ve srovnání s H.264, výsledky ovšem zkreslilo použité nižší rozlišení komponentů od společnosti Axis. K vytvoření návrhu, vizualizací a jednotlivých zobrazení byly použity softwarové aplikace AutoCAD a VideoCAD.

**SEZNAM POUŽITÉ LITERATURY**

- [1] *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví* [online]. Praha [cit. 2017-04-24]. Dostupné z: [www.unmz.cz](http://www.unmz.cz)
- [2] ČSN EN 50131-1 ed. 2: *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007. Třídící znak 33 4591.
- [3] ČSN CLC/TS 50131-7: *Poplachové systémy - Elektrické zabezpečovací systémy - Část 7: Pokyny pro aplikace*. 2011. Třídící znak 33 4591
- [4] ČSN EN 62676-1-1: *Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky – Obecně*. 2014. Třídící znak 33 4592.
- [5] ČSN EN 62676-4: *Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 4: Pokyny pro aplikace*. 2016. Třídící znak 33 4592
- [6] ČR. *Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů*. Sbírka zákonů, Česká republika. 2000
- [7] *Detektory Bosch: Recenze a technika* [online]. [cit. 2017-05-01]. Dostupné z: <http://www.abbas.cz/clanky/aktuality/detektory-bosch-zkrati-cas-instalace-az-o-25/>
- [8] ENTWISTLE, Martha. *Qolsys to debut IQ Panel 2 at ISC West* [online]. 2016 [cit. 2017-05-01]. Dostupné z: <http://www.securitysystemsnews.com/article/qolsys-debut-iq-panel-2-isc-west>
- [9] RANDA, Michal. *Integrace poplachových systémů (2. část)* [online]. 2016 [cit. 2017-05-01]. Dostupné z: <http://elektro.tzb-info.cz/poplachove-a-zabezpe-covaci-systemy/14440-integrace-poplachovych-systemu-1-cast>
- [10] RANDA, Michal. *Integrace poplachových systémů (2. část)* [online]. 2016 [cit. 2017-05-01]. Dostupné z: <http://elektro.tzb-info.cz/poplachove-a-zabezpe-covaci-systemy/14460-integrace-poplachovych-systemu-2-cast>
- [11] VALOUCH, Jan. *Projektování integrovaných systémů*. [skriptum]. Zlín: UTB, 2013. ISBN 978-80-7454-296-1 152 s.
- [12] *Jablotron: Creative Alarms* [online]. [cit. 2017-05-01]. Dostupné z: <https://www.jablotron.com/cz/>

- [13] SVOBODA, Štěpán. *Měření teploty: Bezkontaktní teploměry a termovizní kamery* [online]. 2005 [cit. 2017-05-01]. Dostupné z: <http://www.odbornecasopisy.cz/elektro/casopis/tema/mereni-teploty-bezkontaktni-teplomery-a-termovizni-kamery--13376>
- [14] *Termokamera.cz* [online]. [cit. 2017-05-01]. Dostupné z: <http://www.termokamera.cz/princip-a-funkce/>
- [15] Nové termokamery FLIR FC-Series ID. *Abbas* [online]. 2016 [cit. 2017-05-01]. Dostupné z: <http://www.abbas.cz/clanky/aktuality/nove-termokamery-flir-fc-series-id/>
- [16] *Přisvícení kamer* [online]. [cit. 2017-05-01]. Dostupné z: <https://www.kamerove-systemy-cpplus.cz/prisviceni-kamer>
- [15] *Solid Light* [online]. [cit. 2017-05-01]. Dostupné z: <http://www.avtech.cz/technologie/Solid-Light-Prisvit>
- [16] *WHAT'S LASER INFRARED SECURITY CAMERA?* [online]. 2016 [cit. 2017-05-01]. Dostupné z: <http://www.hkvstar.com/technology-news/what-s-laser-infrared-security-camera.html>
- [17] *Komprimační formáty a přenosová rychlost* [online]. [cit. 2017-05-05]. Dostupné z: <https://www.stasanet.cz/Komprimacni-formaty-a-prenosova-rychlost/>
- [18] *Kompresa H.265 / H.265+: Výhody komprese H.265 / H.265+ jsou důležitým krokem kupředu* [online]. [cit. 2017-05-05]. Dostupné z: [https://www.abso-lon.cz/aktuality/\\_zobraz=kompresa-h.265--h.265--jiz-brzy](https://www.abso-lon.cz/aktuality/_zobraz=kompresa-h.265--h.265--jiz-brzy)
- [19] SULEK, Martin. *Pokročilá videoanalýza obrazu* [online]. **2015** [cit. 2017-05-05]. Dostupné z: <http://www.abbas.cz/clanky/recenze-technika/pokrocila-videoanalyza-obrazu/>
- [20] *CCTV objektivy a příslušenství* [online]. [cit. 2017-05-05]. Dostupné z: <http://www.escadtrade.cz/cctv-objektivy-a-prislusenstvi.html>

- [21] UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8
- [22] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeR-BuM, 2011, 316 s. ISBN 978-80-87500-05-7
- [23] KINDL, Jiří. *Projektování bezpečnostních systémů*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1
- [24] *Microphonic cable intrusion detection sensor: FLEX-PS* [online]. [cit. 2017-05-05]. Dostupné z: <http://senstar.com/wp-content/uploads/2013/06/FlexPS-US-Letter-English-R6-LR.pdf>
- [25] [online]. [cit. 2017-05-05]. Dostupné z: <http://www.globalhomeautomation.com/wp-content/uploads/2013/06/Touch-center-app-by-Honeywell-trusted-Globally.jpg>
- [26] [online]. [cit. 2017-05-05]. Dostupné z: <http://elektro.tzb-info.cz/docu/clanky/0123/012364o7.jpg>
- [27] Lukáš, Luděk: *Bezpečnostní technologie, systémy a management II*. - 1. vyd. - - Zlín: VeR-BuM, 2012. -- 387 s. ISBN 978-80-87500-19-4
- [28] *Which is better? It's complicated..* [online]. [cit. 2017-05-05]. Dostupné z: <http://www.teledynedalsa.com/imaging/knowledge-center/appnotes/ccd-vs-cmos/>
- [29] *BSI CMOS snímač: popis technologie* [online]. 2011 [cit. 2017-05-05]. Dostupné z: <http://www.digimanie.cz/bsi-cmos-snimac-popis-technologie/3650-2>
- [30] *CCTV objektivy a příslušenství* [online]. [cit. 2017-05-13]. Dostupné z: <http://www.escadtrade.cz/cctv-objektivy-a-prislusenstvi.html>
- [31] HOTÁREK, Lukáš. *KOAXIÁLNÍ KABELY V KOMUNIKAČNÍCH SÍTÍCH* [online]. Vysoké učení technické v Brně, 2013 [cit. 2017-05-13]. Dostupné z: [https://www.vutbr.cz/www\\_base/zav\\_prace\\_soubor\\_ve-rejne.php?file\\_id=69129](https://www.vutbr.cz/www_base/zav_prace_soubor_ve-rejne.php?file_id=69129)

- [32] ODVÁRKA, Petr. *Principy komunikace, média, rozsah* [online]. [cit. 2017-05-13]. Dostupné z: <http://www.svetsiti.cz/clanek.asp?cid=Principy-komunikace-media-rozsah-792000>
- [33] DUŠEK, Ing. Martin a Ing. Michal MAZANEC. *Fyzikální principy optických a optovláknových snímačů: Učební texty k semináři* [online]. [cit. 2017-05-13]. Dostupné z: [http://www.crr.vutbr.cz/system/files/brozura\\_06\\_1206.pdf](http://www.crr.vutbr.cz/system/files/brozura_06_1206.pdf)
- [34] *Základní rozdělení kamerových systémů* [online]. [cit. 2017-05-13]. Dostupné z: <http://kamerovatechnika.cz/druhy-kamerovych-systemu.html>
- [35] *Metody přenosu dat* [online]. [cit. 2017-05-13]. Dostupné z: <http://www.netcam.cz/encyklopedie-ip-zabezpeceni/metody-prenosu-dat.php>
- [36] *ONVIF* [online]. [cit. 2017-05-13]. Dostupné z: <https://www.onvif.org/>
- [37] *Síťová zařízení* [online]. [cit. 2017-05-13]. Dostupné z: <http://sites.cgymkh.cz/stryhal/kvarta/pocitacove-site/sitova-zarizeni>
- [38] *VPN, SSL, and HTTPS* [online]. 2010 [cit. 2017-05-13]. Dostupné z: <https://www.welivesecurity.com/2010/11/10/vpn-ssl-and-https/>
- [39] *DVR záznamové zařízení* [online]. [cit. 2017-05-13]. Dostupné z: <http://www.systemy-kamerove.com/dvr-zaznamove-zarizeni/>
- [40] *Satel* [online]. [cit. 2017-05-20]. Dostupné z: <https://www.satel.pl/>
- [41] *Paradox* [online]. [cit. 2017-05-20]. Dostupné z: <http://www.paradox.cz/>
- [42] Hanwha: Techwin Europe. [online]. [cit. 2017-05-20]. Dostupné z: <https://www.hanwha-security.eu/>
- [43] *Axis* [online]. [cit. 2017-05-20]. Dostupné z: <https://www.axis.com/cz/cs/>



**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

VSS	Video Surveillance System
I&HAS	Intruder and Hold-up Alarm System
CCTV	Closed Circuit Television
ČSN	Česká Státní Norma
BSI	Backside Illuminated
CMOS	Complementary Metal Oxide Semiconductor
CCD	Charge Coupled Device
GSM	Group Spécial Mobile
DPPC	Dohledové a poplachové přijímací centrum
NP	Nadzemní Podlaží

**SEZNAM OBRÁZKŮ**

Obr. 1: Vývojový diagram činností při zřizování I&HAS [3] .....	18
Obr. 2: Funkce VSS [4, upraveno Malaník] .....	20
Obr. 3: Více-senzorový detektor pohybu [7] .....	26
Obr. 4: Dotykový ovládací panel [8] .....	27
Obr. 5: Náhled do mobilní aplikace Můj Jablotron [12].....	28
Obr. 6: Blokové schéma VSS [vlastní zdroj].....	29
Obr. 7: Elektromagnetické spektrum vlnových délek [14].....	30
Obr. 8: Schématické zobrazení snímání termovizní kamerou [14] .....	30
Obr. 9: Snímek z termovizní kamery [15] .....	31
Obr. 10: Kamera s termovizí [15].....	31
Obr. 11: Rozdíl ve snímání scéně při použití technologie Solid Light (vpravo) [17]32	
Obr. 12: IR přísvit s technologií Solid Light [17].....	32
Obr. 13: Rozdíly mezi IR LED (vlevo) a laserovým (vpravo) přísvitem [16] .....	33
Obr. 14: Pořízený záběr z kamery s objektivem fish-eye [20] .....	36
Obr. 15: Blokové schéma I&HAS [vlastní zdroj].....	39
Obr. 16: Blokové schéma smyčkové ústředny [21] .....	40
Obr. 17: Blokové schéma ústředny s přímou adresací detektorů [21].....	41
Obr. 18: Blokové schéma smíšeného typu ústředny [21] .....	41
Obr. 19: Blokové schéma detektorů narušení [22] .....	43
Obr. 20: Rozdělení technické ochrany [23] .....	44
Obr. 21: Zobrazení funkce infračervených bariér [22] .....	45
Obr. 22: Zobrazení zapojení mikrofonických kabelů [24] .....	46
Obr. 23: Zobrazení principu funkce magnetického detektoru [23] .....	47
Obr. 24: Blokové schéma funkce a zapojení PIR detektorů narušení [22].....	49
Obr. 25: Ovládací panel od firmy Honeywell [25] .....	52
Obr. 26: Prvky signalizačních zařízení [26] .....	53
Obr. 27: Funkce VSS [4, vlastní zpracování] .....	54
Obr. 28: Princip snímání IP kamery [27].....	55
Obr. 29: Ukázka CCD čipu [28] .....	55
Obr. 30: Ukázka CMOS čipu [28] .....	56
Obr. 31: Ukázka uspořádání struktur CMOS (vlevo) a BSI CMOS (vpravo) [29] ....	56
Obr. 32: Ovlivnění šířky úhlu záběru změnou ohniskové vzdálenosti [30] .....	58

Obr. 33: Vrstvy koaxiálního kabelu [31] .....	60
Obr. 34: STP kabel [32] .....	61
Obr. 35: Mnohovidový optický kabel [33] .....	61
Obr. 36: Rozdělení částí bezpečnostního posouzení [3] .....	68
Obr. 37: Přízemí a 1. nadzemní podlaží .....	75
Obr. 38: 2. nadzemní podlaží .....	76
Obr. 39: Zjednodušené zobrazení prostor výroby a skladů .....	77
Obr. 40: Zjednodušené zobrazení prostor administrativy .....	79
Obr. 41: Zjednodušené zobrazení perimetru objektu .....	80
Obr. 42: Zjednodušené zobrazení ostatních prostor .....	81
Obr. 43: Předpokládaný zvýšený pohyb vysokozdvihných vozíků .....	82
Obr. 44: Zobrazení pláště v přízemí a 1.NP .....	83
Obr. 45: Zobrazení pláště v 2.NP .....	84
Obr. 46: Zobrazení chodeb a schodišť v přízemí a 1.NP .....	85
Obr. 47: Zobrazení chodeb a schodišť v 2.NP .....	85
Obr. 48: Rozdělení zobrazení 1.NP a přízemí pro bezpečnostní analýzu .....	86
Obr. 49: Rozdělení zobrazení 2.NP pro bezpečnostní analýzu .....	87
Obr. 50: Mapová analýza rizika přízemí a 1.NP .....	89
Obr. 51: Mapová analýza rizik 2.NP .....	89
Obr. 52: Barevné zobrazení rizik pomocí gradientu, přízemí a 1.NP .....	90
Obr. 53: Barevné zobrazení rizik pomocí gradientu, 2.NP .....	91
Obr. 54: Škála barev .....	91
Obr. 55: Legenda prvků .....	95
Obr. 56: Základní deska ústředny Integra 128 [40] .....	96
Obr. 57: ETHM-1 Plus TCP/IP komunikační modul [40] .....	97
Obr. 58: INT-E expandér [40] .....	98
Obr. 59: LCD klávesnice INT-KLCD-GR [40] .....	98
Obr. 60: Magnetický detektor S-1 [40] .....	99
Obr. 61: Magnetický vratový detektor B-4S [40] .....	99
Obr. 62: PIR detektor Aqua Pro [40] .....	100
Obr. 63: Siréna SP-4006 R [40] .....	101
Obr. 64: OPU-4 [40] .....	101
Obr. 65: TR 40 VA [40] .....	101

Obr. 66: Tísňový hlásič PNK-1 [40].....	102
Obr. 67: Ústředna EVO192PCB [41] .....	103
Obr. 68: Expandér ZX8 [41].....	104
Obr. 69: Komunikační modul IP150SWAN [41] .....	104
Obr. 70: Klávesnice K641 [41].....	105
Obr. 71: USP1000 [41] .....	106
Obr. 72: USP3000SP [41].....	106
Obr. 73: DG65+ [41] .....	107
Obr. 74: PS128 [41].....	107
Obr. 75: DMN700L [41].....	108
Obr. 76: XNO-8080R [42].....	110
Obr. 77: XND-6080R [42].....	111
Obr. 78: XNV-8080R [42].....	111
Obr. 79: XRN-3010 [42].....	112
Obr. 80: DR-HDD-4TB [42] .....	112
Obr. 81: P1405-LE [43] .....	113
Obr. 82: M3025-VE [43] .....	113
Obr. 83: P3367-V [43].....	114
Obr. 84: Zorná pole kamerových zařízení v perimetru.....	116
Obr. 85: Parametry kamery typ 1.....	116
Obr. 86: Zorné pole kamery typ 2.....	117
Obr. 87: Parametry kamery typ 2.....	117
Obr. 88: Zorné pole kamery typ 3.....	118
Obr. 89: Parametry kamery typ 3.....	118

**SEZNAM TABULEK**

Tab. 1: Struktura souboru norem 50 13x [2] .....	11
Tab. 2: Obecné rozdělení skupiny norem 50 13x [2] .....	12
Tab. 3: Jednotlivé části normy EN 50131 [2] .....	12
Tab. 4: Stupně zabezpečení [2] .....	13
Tab. 5: Třídy prostředí [2] .....	14
Tab. 6: Soubor norem ČSN EN 62676 [4] .....	18
Tab. 7: Třídy prostředí VSS [5] .....	20
Tab. 8: Popis vzorce [5] .....	23
Tab. 9: Rozdíly mezi IR LED a laserovým přísvitem [vlastní zdroj] .....	33
Tab. 10: Porovnání klasických kompresních standardů s Hikvision 265+ [18] .....	34
Tab. 11: Porovnání technologií čipů CCD, CMOS a BSI CMOS [29] .....	57
Tab. 12: Zabezpečované hodnoty [3] .....	68
Tab. 13: Budova [3] .....	69
Tab. 14: Vnitřní vlivy [3] .....	69
Tab. 15: Vnější vlivy [3] .....	70
Tab. 16: Informace návrhu systému I&HAS [3] .....	70
Tab. 17: Technické posouzení [3] .....	70
Tab. 18: Posouzení rizik [5] .....	71
Tab. 19: Specifikace provozních požadavků [5] .....	71
Tab. 20: Kamerové zařízení [5] .....	72
Tab. 21: Charakteristiky videa [5] .....	72
Tab. 22: O – otevření, P – průnik, T – past, S – objekty vyžadující speciální pozornost .....	92
Tab. 23: Popis místnosti v přízemí .....	93
Tab. 24: Popis místnosti v 1.NP .....	94
Tab. 25: Popis místností v 2.NP .....	95
Tab. 26: Specifikace ústředny Integra 128 [40] .....	96
Tab. 27: Specifikace komunikačního modulu ETHM-1 Plus [40] .....	97
Tab. 28: Specifikace INT-E [40] .....	97
Tab. 29: Specifikace LCD klávesnice INT-KLCD-GR [40] .....	98
Tab. 30: Specifikace magnetického detektoru S-1 [40] .....	99
Tab. 31: Specifikace magnetického vratového detektoru B-4S [40] .....	99

Tab. 32: Specifikace PIR detektoru Aqua Pro [40] .....	100
Tab. 33: Specifikace sirény SP-4006 R [40].....	100
Tab. 34: Specifikace tísňového hlásiče PNK-1 [40].....	102
Tab. 35: Výpočet kapacity záložního zdroje napájení .....	102
Tab. 36: Specifikace ústředny EVO192PCB [41] .....	103
Tab. 37: Specifikace expandéru ZX8 [41].....	104
Tab. 38: Specifikace komunikačního modulu EVO192 [41] .....	104
Tab. 39: Specifikace klávesnice K641R [41] .....	105
Tab. 40: Specifikace magnetického detektoru USP1000 [41].....	105
Tab. 41: Specifikace magnetického vratového detektoru [41] .....	106
Tab. 42: Specifikace PIR detektoru DG65+ [41] .....	106
Tab. 43: Specifikace sirény PS128 [41].....	107
Tab. 44: Specifikace tísňového hlásiče DMN700L .....	108
Tab. 45: Výpočet kapacity záložního zdroje napájení .....	108
Tab. 46: Parametry XNO-8080R [42] .....	110
Tab. 47: Parametry XND-6080R [42] .....	110
Tab. 48: Parametry XNV-8080R [42] .....	111
Tab. 49: Parametry NVR XRN-3010 [42].....	111
Tab. 50: Parametry P1405-LE [43].....	112
Tab. 51: Parametry M3025-VE [43].....	113
Tab. 52: Parametry P3367-V [43].....	113
Tab. 53: Provozní vlastnosti kamery typu 1 .....	114
Tab. 54: Provozní vlastnosti kamery typu 2 .....	115
Tab. 55: Provozní vlastnosti kamery typu 3 .....	115
Tab. 56: Parametry výpočtu kapacity uložště Varianta 1 .....	119
Tab. 57: Parametry výpočtu kapacity uložště Varianta 2 .....	119
Tab. 58: Finanční náklady, I&HAS – Varianta 1 - Satel.....	120
Tab. 59: Finanční náklady, I&HAS – Varianta 2 - Paradox.....	120
Tab. 60: Finanční náklady, VSS – Varianta 1 – Samsung.....	121
Tab. 61: Finanční náklady, VSS – Varianta 2 - Axis .....	121

## **SEZNAM PŘÍLOH**

Příloha P1: Umístění a označení prvků I&HAS v přízemí a 1.NP

Příloha P2: Umístění a označení prvků I&HAS v 2.NP

Příloha P3: Popis zón

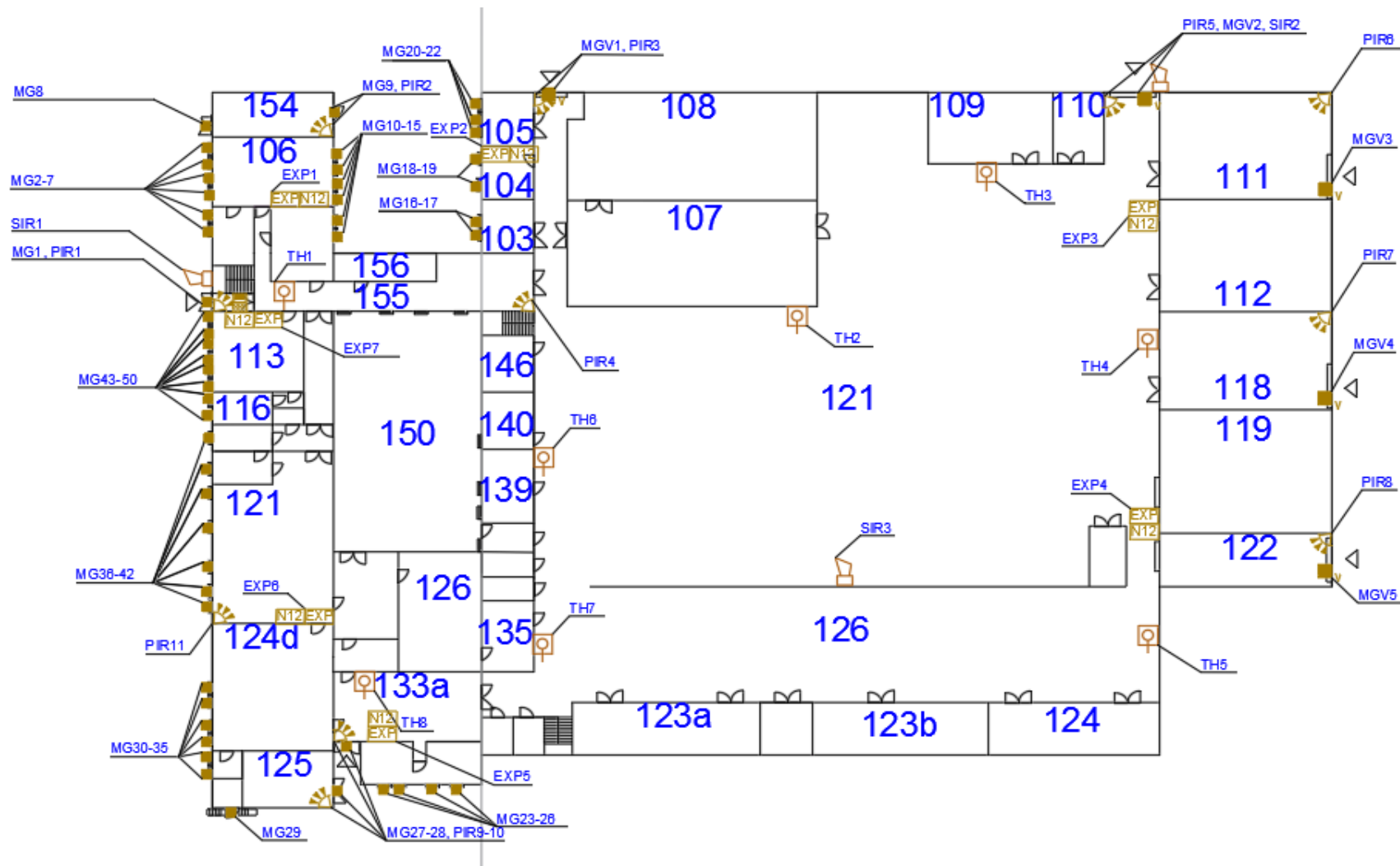
Příloha P4: Rozmístění prvků VSS

Příloha P5: Analýza – Hodnoty

Příloha P6: Analýza – Zranitelnost, pravděpodobnost

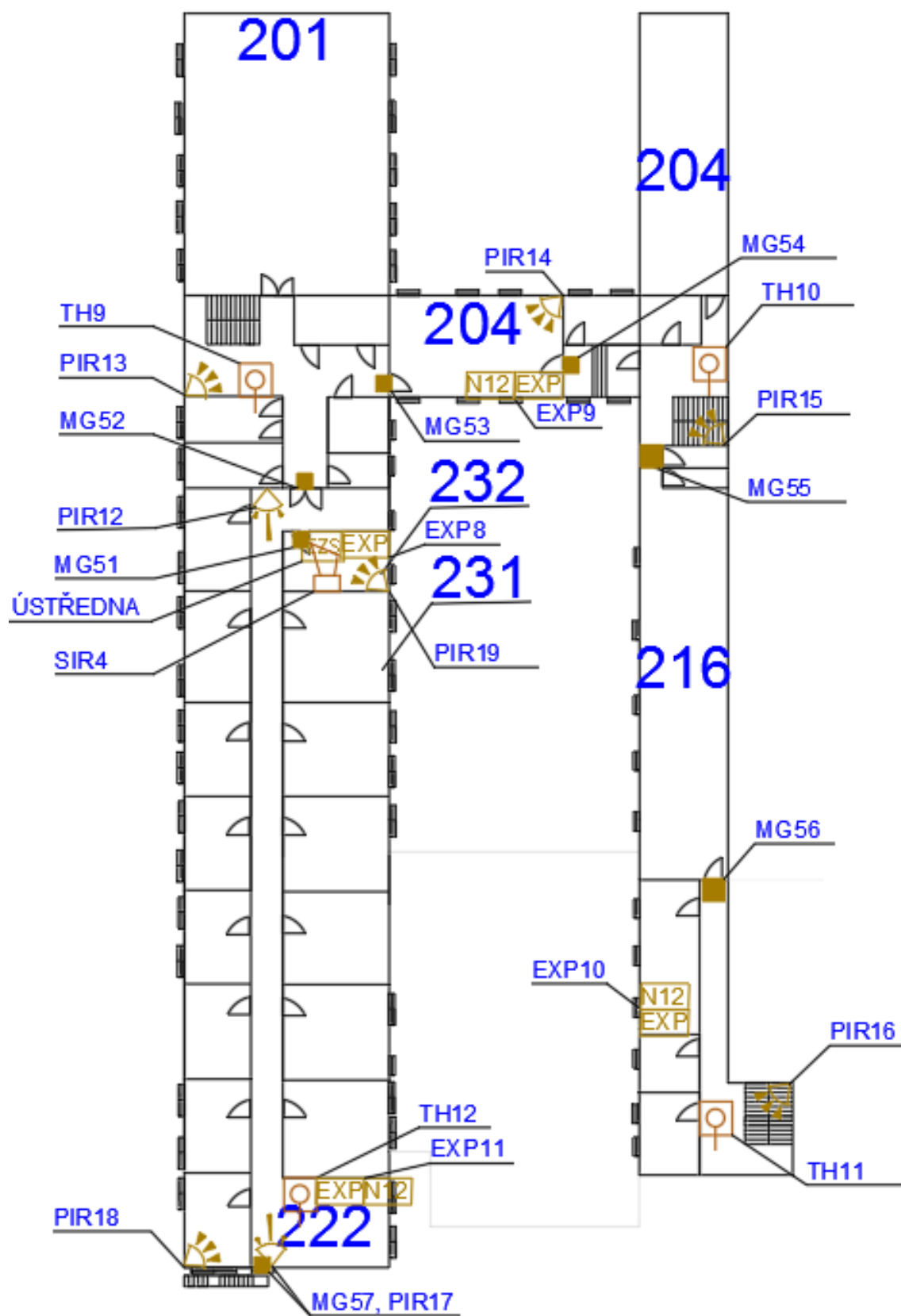
Příloha P7: Analýza – Závažnost hrozby

# PŘÍLOHA P1: UMÍSTĚNÍ A OZNAČENÍ PRVKŮ I&HAS V PŘÍZEMÍ A 1.NP





## PŘÍLOHA P2: UMÍSTĚNÍ A OZNAČENÍ PRVKŮ I&HAS V 2.NP



## PŘÍLOHA P3: POPIS ZÓN

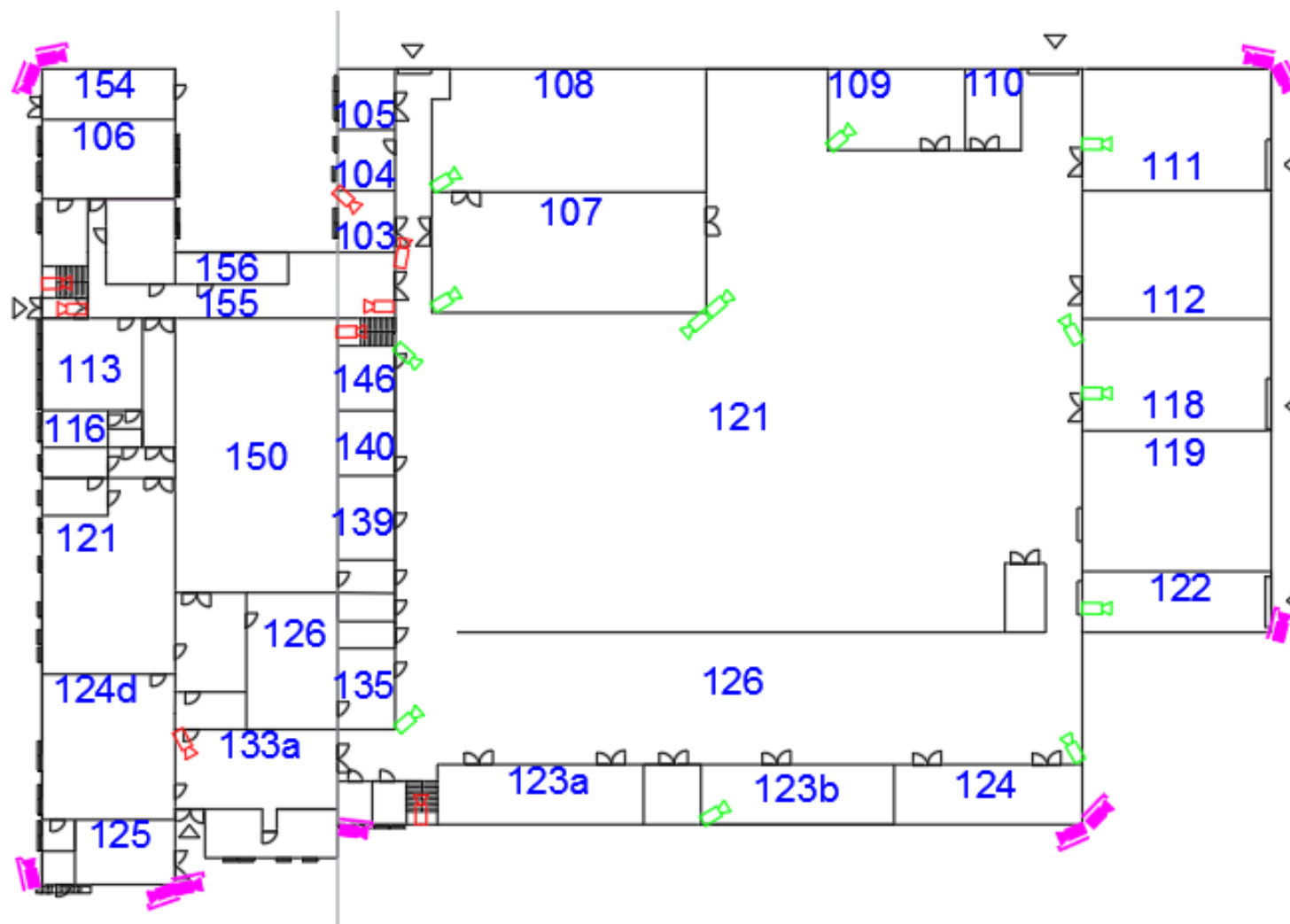
Zóna	Prvek	Typ zóny
1	MG1	Zpožděná
2	PIR1	Zpožděná
3	MG2-3	Okamžitá
4	MG4-7	Okamžitá
5	MG8-9	Okamžitá
6	MG10-13	Okamžitá
7	MG14-15	Okamžitá
8	PIR2	Okamžitá
9	EXP1 TAMPER	24 h
10	MG16-17	Okamžitá
11	MG18-19	Okamžitá
12	MG20-22	Okamžitá
13	MGV1	Okamžitá
14	PIR3	Okamžitá
15	TH2	Okamžitá
16	EXP2 TAMPER	24 h
17	TH3	Okamžitá
18	PIR5	Okamžitá
19	SIR2 TAMPER	24 h
20	PIR6	Okamžitá
21	MGV3	Okamžitá
22	PIR7	Okamžitá
23	TH4	Okamžitá
24	EXP3 TAMPER	24 h
25	SIR3 TAMPER	24 h
26	TH5	Okamžitá
27	MGV5	Okamžitá

28	PIR8	Okamžitá
29	MGV4	Okamžitá
30	EXP4 TAMPER	24 h
31	TH7	Okamžitá
32	MG23-26	Okamžitá
33	MG27	Okamžitá
34	PIR9	Okamžitá
35	PIR10	Okamžitá
36	MG28	Okamžitá
37	MG29	Okamžitá
38	EXP5 TAMPER	24 h
39	MG30-31	Okamžitá
40	MG32-35	Okamžitá
41	MG36-40	Okamžitá
42	PIR11	Okamžitá
43	MG41	Okamžitá
44	MG42	Okamžitá
45	EXP6 TAMPER	24 h
46	MG43-44	Okamžitá
47	MG45-50	Okamžitá
48	SIR1 TAMPER	2 4h
49	TH1	Okamžitá
50	TH6	Okamžitá
51	EXP7 TAMPER	24 h
52	PIR12	Okamžitá
53	SIR4 TAMPER	24 h
54	PIR18	Okamžitá
55	MG52	Okamžitá

<b>56</b>	PIR13	Okamžitá
<b>57</b>	TH9	Okamžitá
<b>58</b>	MG51	Okamžitá
<b>59</b>	EXP8 TAMPER	24 h
<b>60</b>	MG53	Okamžitá
<b>61</b>	MG54	Okamžitá
<b>62</b>	MG55	Okamžitá
<b>63</b>	PIR14	Okamžitá
<b>64</b>	PIR15	Okamžitá
<b>65</b>	TH10	Okamžitá
<b>66</b>	EXP9 TAMPER	24 h

<b>67</b>	MG56	Okamžitá
<b>68</b>	PIR16	Okamžitá
<b>69</b>	TH11	Okamžitá
<b>70</b>	EXP10 TAMPER	24 h
<b>71</b>	MG57	Okamžitá
<b>72</b>	PIR17	Okamžitá
<b>73</b>	PIR 18	Okamžitá
<b>74</b>	TH12	Okamžitá
<b>75</b>	EXP11 TAMPER	24 h
<b>76</b>	UST. TAMPER	24 h

# PŘÍLOHA P4: ROZMÍSTĚNÍ PRVKŮ VSS



## PŘÍLOHA P5: ANALÝZA – HODNOTY

1. část

	2	2	2	2	2	
9	7	10	10	7	7	2
9	7	10	10	7	7	2
9	10	10	10	7	7	2
	10	10	10	7	8	

2. část

	2	1	2	2	2	
2	7	2	6	9	9	7
2	3	4	10	9	9	7
2	3	2	4	10	10	10
	4	2	4	10	10	

3. část

	4	2	4	10	10	
2	4	2	4	10	10	10
2	4	4	4	10	10	10
2	4	5	4	6	7	9
	6	3	2	2	2	

4. část

	10	10	10	7	8	
10	10	10	10	7	8	2
10	10	10	9	6	7	2
7	10	10	7	5	1	1
	2	2	2	2	1	

5. část

	2	1	5	
1	3	1	4	1
1	3	9	3	1
1	10	1	4	1
1	10	1	4	1
1	10	1	3	1
1	6	1	5	3
	1	1	1	

## PŘÍLOHA P6: ANALÝZA – ZRANITELNOST, PRAVDĚPODOBNOST

1. část

	8	8	8	10	8	
7	9	10	9	10	9	10
7	8	10	10	8	5	8
10	10	10	10	8	9	10
10	10	10	8	9		

2. část

	8	8	10	8	8	
8	8	7	10	7	7	9
8	10	9	9	7	7	8
8	4	6	4	10	10	10
	4	6	4	10	10	

3. část

	4	6	4	10	10	
8	4	6	4	10	10	10
8	4	4	4	10	10	10
8	4	10	10	10	8	9
	10	10	8	7	7	

4. část

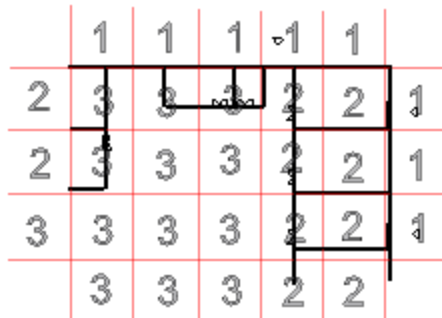
	10	10	10	9	9	
10	10	10	10	6	5	8
10	10	10	9	10	9	10
6	9	10	5	5	7	6
	7	7	7	7	7	

5. část

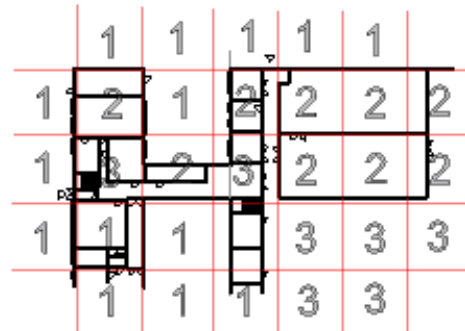
	5	4	4	
4	4	4	4	1
4	9	7	4	1
4	5	3	4	1
4	5	3	4	1
4	5	3	4	1
4	5	3	4	9
	9	4	4	

## PŘÍLOHA P7: ANALÝZA – ZÁVAŽNOST HROZBY

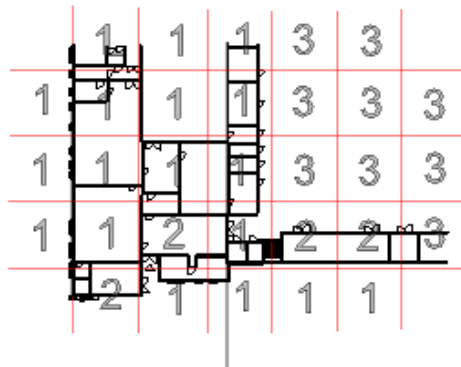
1. část



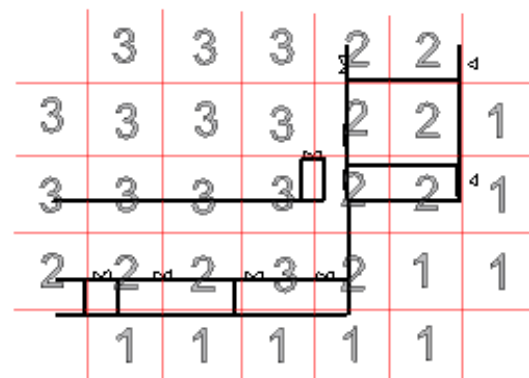
2. část



3. část



4. část



5. část

