# Návrh zabezpečovacího systému firmy zaměřené na elektromontáže

Bc. Petr Kovář

Diplomová práce
2017



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Petr Kovář** |
| Osobní číslo: | **A15179** |
| Studijní program: | **N3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Forma studia: | **prezenční** |
| Téma práce: | **Návrh zabezpečovacího systému firmy zaměřené na elektromontáže** |
| Téma anglicky: | **The Design of a Security System for a Company Specialising in Electrical Installation Projects** |

Zásady pro vypracování:

1. **Proveďte obecný rozbor zabezpečovacích systémů a zařízení určených k ochraně průmyslových objektů.**
2. **Seznamte se s aktuálním stavem firmy, včetně celého areálu a popište jejich stávající zabezpečení.**
3. **Proveďte bezpečnostní analýzu rizik provozovny dané firmy.**
4. **Vyberte vhodné zabezpečovací systémy a zařízení s ohledem na kladené požadavky.**
5. **Navrhněte dva systémy zabezpečení firmy a to s ohledem na možná bezpečnostní rizika spojená s jeho specifickým provozem.**
6. **Porovnejte a zhodnoťte Vámi navržené systémy zabezpečení jako celek.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:


1. **VALOUCH, Jan. Projektovaní integrovaných systémů. Zlín. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2015. ISBN 978-80-7454-557-3.**
2. **UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8.**
3. **KINDL, Jiří. Projektování bezpečnostních systémů. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.**
4. **ČANDÍK, Marek. Objektová bezpečnost II. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 100 s. Učební texty vysokých škol / Univerzita Tomáše Bati ve Zlíně. ISBN 8073182173.**
5. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. [aktualiz. S.l.: Cricetus], 2006, 313 s. ISBN 80-902938-2-4.**
6. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. Zlín: VeRBuM, 2011 - 2015, 368 s. ISBN 978-80-87500-05-7.**
7. **ŠEFČÍK, Vladimír. Analýza rizik. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 98 s. ISBN 978-80-7318-696-8.**


Vedoucí diplomové práce: **Ing. Petr Skočík**
Ústav elektroniky a měření

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **24. května 2017**

Ve Zlíně dne 3. února 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
*děkan*

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

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové 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 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 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 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 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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 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 15.5.2017

.....
podpis diplomanta

## ABSTRAKT

Diplomová práce je koncipována na teoretickou a praktickou část. Teoretická část převážně pojednává o zabezpečovacích systémech a postupech bezpečnostního posouzení objektů. Praktická část je zaměřena na zabezpečení objektu firmy provádějící elektromontážní práce. Na základě bezpečnostního posouzení daného objektu a výstupů získaných z bezpečnostní analýzy rizik byly vytvořeny dva návrhy zabezpečovacího systému. První verze zabezpečení byla vypracována s ohledem na kladené požadavky uvedené firmy a druhá pouze na základě zkušeností a teoretických poznatků získaných během studia oboru Bezpečnostní technologie, systémy a management. Oba systémy byly následně porovnány a vyhodnoceny.



Klíčová slova: Detektor, ochrana, poplachový zabezpečovací systém, kamerový systém, bezpečnostní posouzení, analýza rizik



## ABSTRACT

The dissertation is conceived in the theoretical and practical part. The theoretical part deals predominantly with security system and safety assessment procedures of objects. The practical part is focused on securing the object of the company performing electrical work. Based on the safety assessment of the object and the results obtained from the security risk analysis, two proposals of the security system were created. The first version of the security was elaborated with respect to the requirements of the company and the second version was elaborated only based on the experience and the theoretical knowledge gained during the studies in the field of Security technologies, systems and management. Then both systems were compared and evaluated.



Keywords: Detector, protection, alarm security system, camera system, safety assessment, risk analysis

Chtěl bych poděkovat svému vedoucímu diplomové práce Ing. Petru Skočíkovi za jeho odborné vedení, pomoc při získávání informací a za ochotu a trpělivost při vedení mojí diplomové práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH


**ÚVOD** ..... **9**
**I TEORETICKÁ ČÁST** ..... **10**
**1 OBJEKTOVÁ OCHRANA** ..... **11**
1.1 KLASICKÁ OCHRANA ..... 11
1.2 FYZICKÁ OCHRANA ..... 12
1.3 REŽIMOVÁ OCHRANA ..... 12
1.4 TECHNICKÁ OCHRANA ..... 13
1.4.1 Poplachový zabezpečovací a tísňový systém ..... 15
1.4.2 Dohledové a poplachové přijímací centrum ..... 15
1.4.3 Ústředny ..... 18
1.4.4 Napájecí zdroje ..... 23
1.4.5 Elektronická požární signalizace ..... 23
1.4.6 Uzavřené televizní okruhy ..... 25
1.4.7 Systém kontroly vstupu ..... 27
**2 BEZPEČNOSTNÍ POSOUZENÍ** ..... **31**
2.1 ZABEZPEČOVANÉ HODNOTY ..... 32
2.2 BUDOVA ..... 33
2.3 VNITŘNÍ VLIVY ..... 34
2.4 VNĚJŠÍ VLIVY ..... 35
2.5 STUPEŇ ZABEZPEČENÍ A TŘÍDA PROSTŘEDÍ ..... 36
2.6 BEZPEČNOSTNÍ ANALÝZA ..... 38
2.6.1 Metody bezpečnostních analýz ..... 39
**II PRAKTICKÁ ČÁST** ..... **43**
**3 ÚVOD DO PRAKTICKÉ ČÁSTI** ..... **44**
**4 POPIS OBJEKTU** ..... **45**
**5 BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU** ..... **47**
5.1 BEZPEČNOSTNÍ POSOUZENÍ – ZABEZPEČOVANÉ HODNOTY ..... 47
5.2 BEZPEČNOSTNÍ POSOUZENÍ – BUDOVA ..... 48
5.3 BEZPEČNOSTNÍ POSOUZENÍ – VNITŘNÍ VLIVY NA PZTS ..... 53
5.4 BEZPEČNOSTNÍ POSOUZENÍ – VNĚJŠÍ VLIVY NA PZTS ..... 54
5.5 STUPEŇ ZABEZPEČENÍ, TŘÍDA PROSTŘEDÍ ..... 54
**6 ANALÝZA BEZPEČNOSTNÍCH RIZIK** ..... **55**
**7 NÁVRH ZABEZPEČENÍ OBJEKTU – VERZE I** ..... **59**
7.1 PŮDORYSY BUDOV ..... 59
7.2 POPLACHOVÝ ZABEZPEČOVACÍ A TÍSŇOVÝ SYSTÉM ..... 65
**8 NÁVRH ZABEZPEČENÍ OBJEKTU – VERZE II** ..... **79**
8.1 POPLACHOVÝ A ZABEZPEČOVACÍ SYSTÉM. ..... 82
8.2 POUŽITÉ ZAŘÍZENÍ ..... 88
**9 ZHODNOCENÍ NÁVRHŮ ZABEZPEČOVACÍCH SYSTÉMŮ** ..... **93**
**ZÁVĚR** ..... **95**
**SEZNAM POUŽITÉ LITERATURY** ..... **97**

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....100**
**SEZNAM OBRÁZKŮ.....102**
**SEZNAM TABULEK.....104**
**SEZNAM PŘÍLOH.....105**

# ÚVOD.

V dnešní době zasahuje kriminalita do všech oblastí naší společnosti, a tak je ochrana života a majetku jednou z hlavních priorit každého z nás. Jednou z možností ochrany našeho majetku jsou elektronické zabezpečovací systémy. Přítomnost elektronického zabezpečovacího systému v objektu působí na potencionálního pachatele ve většině případech odrazujícím dojmem. Na druhou stranu může objekt tímto prozrazovat zabezpečované hodnoty. Tyto systémy jsou finančně dostupnější než před několika lety a zájem o ně narůstá. Pachatelé, kteří se zaměří na tyto firmy, nemusí být zkušení. Majetek těchto firem lze snadno zpeněžit a ve většině případů nelze po odcizení dohledat. Dále se zde naskýtá riziko krádeže majetku zaměstnanci. Výše zmíněné elektronické zabezpečovací systémy umožnují vytvořit kompletní zabezpečení daného objektu dle specifických požadavků. Pokud chceme navrhnout zabezpečovací systém, který bude efektivní, je zapotřebí se s tímto objektem seznámit. Před samotným návrhem zabezpečení objektu je potřeba věnovat pozornost bezpečnostnímu posouzení, které bývá často opomíjeno. Nesmí být dále zapomínáno na normy, které jsou významným východiskem pro pojišťovny.

V teoretické částí jsou obecně rozebrány zabezpečovací systémy se zvýšenou pozorností na technickou ochranu a jednotlivé systémy. Dalším bodem jsou jednotlivé kroky bezpečnostního posouzení, které je potřeba provést vždy před návrhem systému. Praktická část diplomové práce obsahuje dvě verze zabezpečení objektu. Při vypracování první verze zabezpečení byl brán ohled na kladené požadavky uvedené firmy. Ve druhé verzi zabezpečení byly vybrány komponenty dle mých získaných zkušeností a znalostí během doby studia. Na závěr této práce jsou obě verze zabezpečení porovnány a vyhodnoceny.

# I. TEORETICKÁ ČÁST

# 1 OBJEKTOVÁ OCHRANA

Důvod, proč je realizována ochrana, je vytvoření bezpečného prostředí vzhledem k danému subjektu. Při návrhu konkrétní ochrany musíme vědět co chránit (popis subjektu) a proti čemu subjekt chránit (definice nebezpečí). Prostředky, které se využívají k ochraně, nazýváme bezpečnostní systém. Bezpečnostní systém můžeme brát jako integrovaný celek, který zajišťuje majetkovou bezpečnost, osobní bezpečnost, informační bezpečnost. V těchto bezpečnostních oblastech se využívá mechanické ochrany, elektronické ochrany a režimové ochrany. Při navrhování ochrany je důležité mít na paměti tří základní aspekty [2]:

- každá ochrana může být překonána,
- technické prostředky nedokáží plně nahradit člověka,
- jedna skupina ochrany nic neřeší.

Objektovou ochranu můžeme rozdělit do čtyř základních skupin [2]:

- klasická ochrana,
- fyzická ochrana,
- režimová ochrana,
- technická ochrana.

## 1.1 Klasická ochrana

Ochrana spočívá v použití takových mechanických zařízení, které znemožní pachateli poškodit nebo odcizit objekty a jejich části. Ochrana je zaměřena i na cenné předměty uvnitř objektu. V dnešní době se sní setkáme téměř na každém objektu. Klasická ochrana patří mezi nejstarší formu ochrany objektu a je stále hojně používaná. Jedná se o základní formu ochrany objektu, a dle současných zkušeností, není sama o sobě schopná zabezpečit chráněné objekty. V současné době se kombinuje s ostatními druhy ochrany. Mezi mechanické zábranné systémy patří [2;5]:

- systémy předmětové ochrany (příruční pokladničky, manipulační schránky, trezory, komerční úschovné objekty atd.),
- systémy plášťové ochrany (dveře, okna, ochranné a bezpečnostní fólie, bezpečnostní skla, rolety, mříže atd.),

- systémy obvodové ochrany (závory, bezpečnostní oplocení, brány atd.).

## 1.2 Fyzická ochrana

Fyzická ochrana objektu je zajišťována fyzickou ostrahou. Tuto ostrahu můžou tvořit hlídací služby, vrátní, hlídači nebo policisté. Ochranu aktiv pomáhají zajistit svojí dočasnou nebo trvalou přítomností v objektu. Zajišťování fyzické ochrany je finančně náročné z důvodu vysokých nákladů za režii. U ostatních typů ochrany jsou nízké režijní náklady, ale poměrně vysoké vstupní investice [1;7].

Mezi základní činnosti fyzické ostrahy patří [7]:

- kontrola osob,
- zamezení krádeže aktiv,
- odhalení a zadržení pachatele,
- kontrola motorových vozidel (doklady, náklad apod.),
- kontrola střeženého objektu a jeho perimetru,
- realizace havarijních a protipožárních opatření,
- podávání informací, udržování pořádku apod.

## 1.3 Režimová ochrana

Jedná se o administrativní opatření a postupy, jejíž cílem je stanovit pravidla, zásady, oprávnění při pohybu cizích osob a zaměstnanců v prostorách organizace. Je potřeba zavést účinné bezpečnostní směrnice, týkající se pohybu osob, vstupu a odchodu osob, způsobu nakládání s důležitými prvky a další. Je potřeba stanovit režimová opatření tak, aby bylo omezení pohybu osob co nejmenší a současně byla zajištěna požadovaná úroveň bezpečnosti [2;5]. Režimová opatření se lze rozlišit na:

- vnitřní opatření,
- vnější opatření.

**Vnitřní opatření**

Jsou opatření, které se tykají pohybu uvnitř chráněného objektu. Týká se to především osob a automobilů, které se mohou pohybovat ve vyhrazených prostorech, oblastech

nebo okruzích. Vnitřní opatření jsou dále zaměřena i na pohyb výrobku a materiálu v objektu, osvětlení potřebných částí objektu apod. [3;5].

**Vnější opatření**

Jsou zaměřena na vstupní a výstupní podmínky z chráněného objektu. Týká se to především kontroly vjezdů, vchodů a jiných prostorů, které využívají osoby a automobily při vstupu nebo výstupu z objektu [4;5].

## 1.4 Technická ochrana

Jde o monitorování objektu pomocí technických prostředků. Lze ji označit jako detekční systém, který nám podává informace o situaci v zabezpečeném objektu. Technická ochrana reaguje na změny, které vyvolá pachatel. Tyto změny jsou zaznamenány a následně můžou být předány bezpečnostní firmě, policii nebo majiteli. Díky technickým prvkům bezpečnosti lze tak pachatele dopadnout dříve, než je jeho protiprávní jednání dokonáno. Technická ochrana pachatele nedokáže zadržet, a z toho důvodu je vhodné tuto ochranu propojit s fyzickou ochranou [1;2;7].

Hlavními úkoly technické ochrany tedy je [1;2;7]:

- odhalení a zastrašení pachatele,
- monitorování útoku,
- prodloužení překonání ochrany k aktivům.

**Technická ochrana se z prostorového hlediska dělí na:**

- **Obvodová ochrana**

Signalizuje narušení obvodu (perimetru) objektu. Obvodem objektu se rozumí jeho katastrální hranice. Ta bývá často tvořena umělými nebo přírodními bariérami jako jsou ploty, zdi, vodní toky apod. Cílem obvodové ochrany je odhalit pachatele, zpomalit jeho postup k objektu anebo pachatele zastrašit. Na detektory, používané v rámci obvodové ochrany, jsou kladeny vyšší požadavky na klimatickou odolnost. Největší problematikou u těchto detektoru jsou plané poplachy, vyvolané různorodým venkovním prostředím a pohybujícími se objekty různého druhu. Mezi prvky obvodové ochrany patří infračervené závory a bariéry, mikrovlnné bariéry, štěrbinové kabely a další [5;7].

- **Plášťová ochrana**

Signalizuje narušení pláště objektu (budovy). Detektory reagují na překonávání mechanické překážky. Tato ochrana bývá realizována zevnitř, ale i z venku objektu. Mezi prvky plášťové ochrany patří magnetické kontakty, detektory pro ochranu skleněných ploch, mechanické kontakty, vibrační detektory, poplachové folie a poplachová skla a další [6].

- **Prostorová ochrana**

Signalizuje narušení chráněných míst v prostorách objektu. Plášť objektu byl pachatelem překonán a již se pohybuje uvnitř chráněného objektu. Detektory reagují na pohyb pachatele v klíčových místech objektu. Jedná se o místa předpokládaného pohybu pachatele (haly, chodby, schodiště apod.). Mezi prvky prostorové ochrany patří infračervené detektory, ultrazvukové detektory, mikrovlnné detektory a další [7;5].

Detektory prostorové ochrany se dělí na [8]:

  - **Aktivní**

    Okolní prostor je ovlivněn funkcí detektorů. Aktivní detektory nejčastěji produkují do svého okolí ultrazvukové vlnění nebo elektromagnetické záření. Kvůli ovlivňování okolního prostředí je možné lehce detekovat mrtvé a aktivní zóny.

  - **Pasivní**

    Okolní prostor není ovlivněn funkcí detektorů. Pasivní detektory pouze reagují na okolní fyzikální změny vyvolané pachatelem. Detekce těchto typu detektorů je běžnými technickými prostředky obtížná.

- **Předmětová ochrana**

Signalizována je neoprávněná manipulace s předmětem nebo i přiblížení pachatele k chráněnému předmětu. Pomocí těchto detektorů je možné střežit např. sošky, vázy, části nábytku, obrazy, tapiserie. Mezi prvky předmětové ochrany patří závěsný detektor, váhový detektor a další [9].

- **Tísňová ochrana**

Signalizuje zdravotní problémy osob nebo ohrožení života osob, které jsou ohroženy působením přírodních živlů (voda, plyn, požár) nebo jsou napadeny. Signalizace je vyvolaná např. stisknutím tlačítka, šlápnutím na tísňovou lištu atd. [10].

### 1.4.1 Poplachový zabezpečovací a tísňový systém

PZTS je určený k detekci poplachu vniknutí a tísňového poplachu. Hlavním úkolem PZTS je signalizovat nežádoucí narušení objektu majiteli nebo obsluze. Ti následně mohou reagovat na vzniklou událost. Systém může být využíván i k indikaci jiných nebezpečí, jako je vznik požáru, únik plynu, tísňové hlášení při zdravotních problémech, tísňové hlášení při napadení. Je velice důležité, aby informace ze systému byly spolehlivě a včas přeneseny určeným osobám [11;7].

PZTS musí obsahovat [2]:

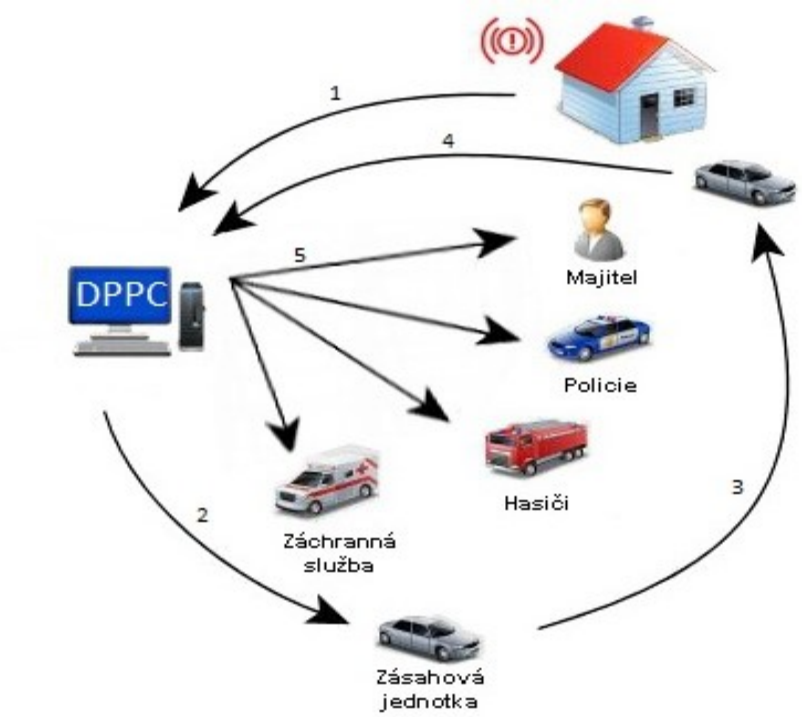
- ústřednu,
- vstupní prvky (např. detektory),
- výstupní prvky (přenosové a signalizační zařízení),
- napájecí zdroj,
- ovládací zařízení.

### 1.4.2 Dohledové a poplachové přijímací centrum

DPPC slouží k monitorování, příjmu a zpracování signálů přicházejících z lokálních zabezpečovacích systémů. DPPC jsou využívána soukromími bezpečnostními službami, Policií ČR, Hasičskými záchrannými sbory apod.

Základní princip činnosti DPPC (viz. Obr. 1) [11]:

- příjem poplachových a nepoplachových signálů,
- vyhodnocení stavu,
- vyslání zásahové jednotky na místo,
- koordinace zásahové jednotky,
- kontaktování majitele, policie, HZS atd.




Obr. 1. Princip činnosti DPPC [11]

Dohledová a poplachová přijímací centra se řídí normou ČSN EN 50518. Tato norma se skládá ze tří částí [9].

**Norma ČSN EN 50518–1 ed. 2** nám definuje umístění a konstrukční požadavky dohledových a poplachových přijímacích center.

V normě jsou uvedeny např. [9]:

- požadavky na umístění DPPC, ohodnocení rizik,
- konstrukční požadavky na DPPC,
- požadavky na elektrické zdroje a zálohování,
- požadavky na elektronickou detekci nebezpečí (útok, tíseň, požár, plyn atd.).

**ČSN EN 50518–2 ed. 2** nám definuje požadavky na technické řešení dohledových a poplachových přijímacích center.

V normě jsou uvedeny např. [9]:

- výkonnostní kritéria,
- požadavky na komunikaci,
- testování funkce všech zařízení DPPC,

- postupy při řešení závad a podání zpráv,
- požadavky na vypracovaní nouzového plánu.

**ČSN EN 50518–3 ed. 2** nám definuje Pracovní postupy a požadavky na provoz dohledových a poplachových přijímacích center.

V normě jsou uvedeny např. [9]:

- požadavky na obsluhu DPPC,
- evakuační plány,
- provozní postupy,
- provozní dokumentace.

**Způsoby připojení DPPC:**

**Telefonní linka** – zprávy z objektu na DPPC jsou přenášeny přes telefonní linku. Telefonní linky se začaly využívat pro přenos jako první, ale postupem času s rozvojem komunikačních technologii se od ní upouští. Čas přenosu zprávy na DPPC je pomalejší a kontrola spojení se provádí většinou jednou za 24 hodin. Nevýhodu je pak potřeba rozvodů telefonní linky v objektu. Přerušení telefonní linky pachatelem, může obsluha DPPC zjistit i až po několika hodinách. Nevýhodou jsou i telefonní poplatky v závislosti na hustotě provozu (vypínání, zapínání apod.) [5;10].

**GSM** – pro komunikaci s DPPC se využívá sít GSM. Lze využít například v případě, že objekt nemá rozvody telefonní sítě anebo je objekt mimo radiový dosah. Pří výpadku sítového napětí jsou GSM moduly zálohovány z akumulátoru ústředny a díky tomu nedojde k jejich výpadku. Jsou obtížně napadnutelné z důvodů použití bezdrátové technologie (nehrozí sabotáž vedení), šifrování, trvalé kontroly funkčnosti. Spolehlivost je odvozena

od aktuálního zatížení sítě [5;10].

**Radiová síť –** pro přenos zprávy se využívá soukromá radiová síť a je považována za nejbezpečnější. Přenos zprávy není tedy závislý na třetí straně. Tyto radiové sítě jsou budovány výhradně pro přenos zpráv z PZTS na DPPC a nejsou zde žádné poplatky za přenos zpráv. Přenos zpráv a kontrola funkčností je pak velmi rychlá. Je zde třeba počítat s poplatky za provoz a údržbu radiové sítě. Nevýhodou je vyšší pořizovací cena vysokofrekvenčního vysílače, který je potřeba zakoupit [5;10].

**Internet –** pro přenos zpráv lze využít i internetovou síť. Tento typ přenosu je poměrně levný. Zde je důležité si uvědomit, že tato sít není určena primárně k přenosu zpráv z PZTS na DPPC, a může tedy dojít k přetížení sítě nebo výpadku. Aktivní prvky sítě (switche, routery) nemají záložní zdroj a při výpadku napětí, je přenos zpráv na DPPC degradován [5;10].

### 1.4.3 Ústředny

Ústředna je centrální část poplachového systémů. Informace o pohybu osob a jiné informace z objektu jsou ústředně zasílány z připojených detektorů. Dle definovaných postupu se vyhlašuje poplach. Poplach může být signalizován místními výstupními prvky (optická signalizace, akustická signalizace) nebo dálkově přenesen na DPPC [6].

Mezi základní funkce ústředny patří [6]:

- přijímání a vyhodnocování elektrických signálu od detektorů,
- napájení detektoru a další zařízení PZTS,
- ovládání přenosových, signalizačních a jiných zařízení,
- diagnostika systému PZTS.

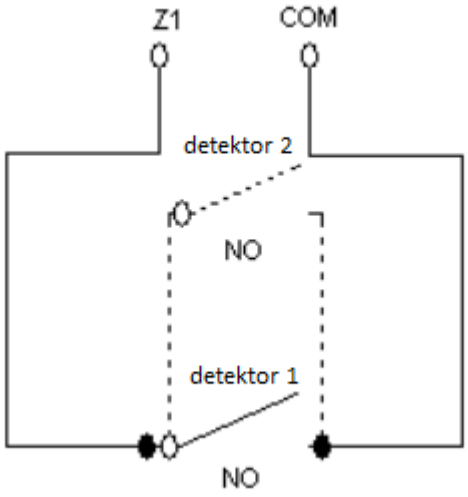
Ústředny PZTS se rozlišuji na [6]:

- ústředny smyčkové (analogové),
- ústředny sběrnicové (digitální),
- ústředny smíšené,
- ústředny s bezdrátovou komunikací.

**Smyčková ústředna** má samostatné vstupní vyhodnocovací obvody pro jednotlivé poplachové smyčky. Obvod je tvořen proudovou smyčkou o konkrétní hodnotě a toleranci. Každá smyčka je zakončena zakončovacím odporem o předepsané hodnotě odporu. Se změnou odporu smyčky dojde k vyhlášení poplachového stavu PZTS. Změna odporu je způsobena sabotáží smyčky nebo aktivací detektoru ve smyčce. Nevýhodou smyčkových ústředen je rozsáhlá kabeláž [6].

**Druhy zapojení smyček** [12]**:**

1. **Smyčka NO – spínaná**




Obr. 2. Smyčka NO [12]

V aktivaci – odpor se blíží nule

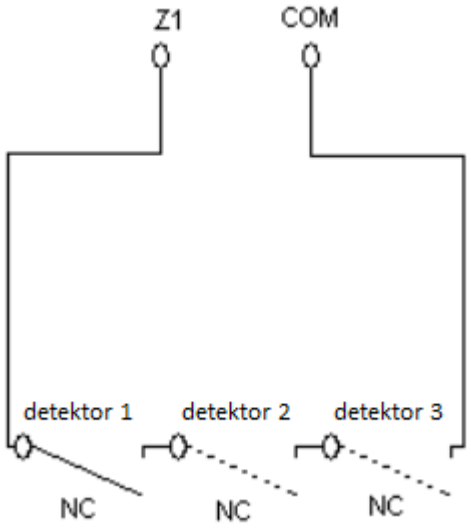
V klidu – odpor se blíží nekonečnu

Výhoda – ve stavu klidu není odebírán proud

Nevýhoda – přerušení vedení není nijak signalizováno

Pokud je potřeba zapojit více NO kontaktu do smyčky, zapojí se paralelně.

2. **Smyčka NC – rozpínaná**




Obr. 3. Smyčka NC [12]

V aktivaci – odpor se blíží nekonečnu

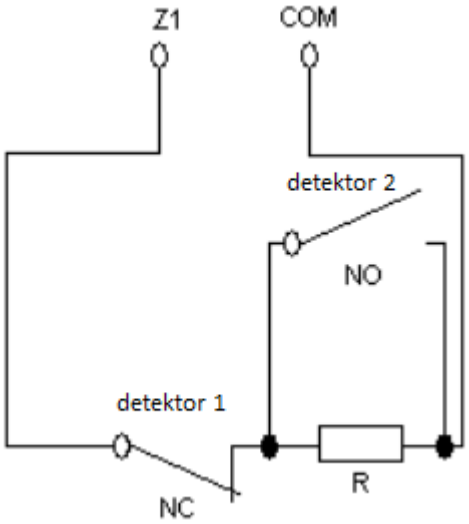
V klidu – odpor se blíží nule

Výhoda – přerušení vedení je signalizováno

Nevýhoda – ve stavu klidu je neustále odebírán proud (zkrat smyčky není signalizovaný)

Pokud je potřeba zapojit více NC kontaktu do smyčky, zapojí se sériově.

### 3. Smyčka EOL – odporově vyvažovaná



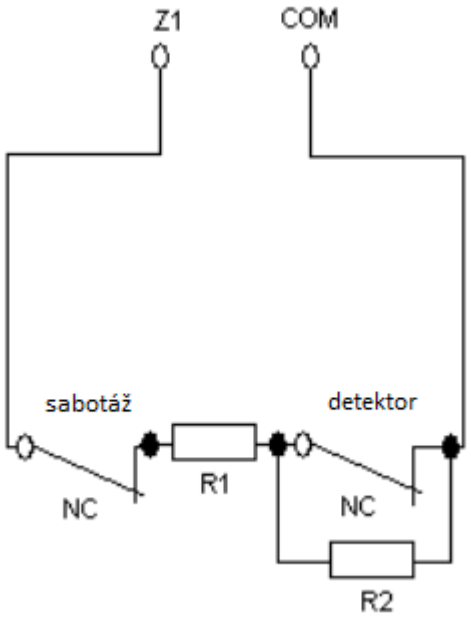

Obr. 4. Smyčka EOL [12]

V aktivaci – odpor se blíží nekonečnu nebo nule

V klidu – odpor se blíží hodnotě vyvažovacího rezistoru

Do smyčky lze zapojit NO i NC kontakty. NO kontakty se zapojují do smyčky paralelně. NC kontakty se zapojují do smyčky sériově.

### 4. Smyčka 2EOL – dvouodporově vyvažovaná




Obr. 5. Smyčka 2EOL [12]

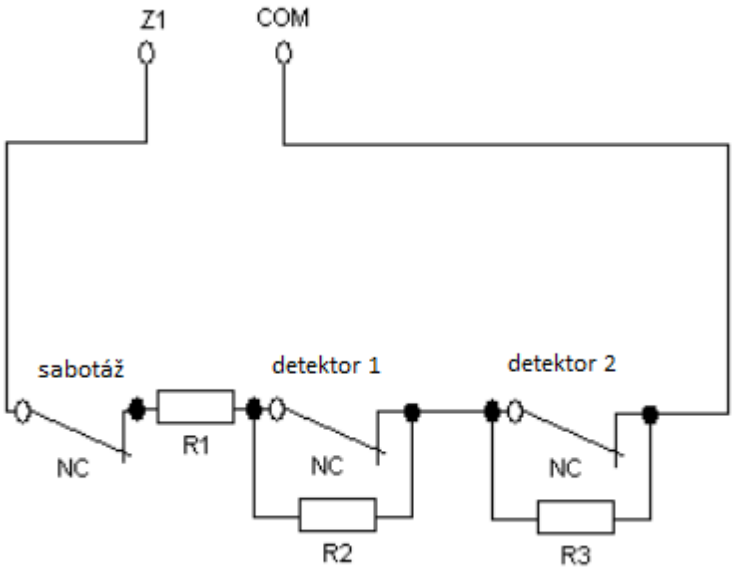
V aktivaci – detektor – Odpor se blíží součtu odporům rezistoru R1 + R2

V aktivaci – sabotážní kontakt – odpor se blíží nekonečnu

V klidu – odpor se blíží hodnotě vyvažovacího rezistoru R1

Výhoda – lze detekovat stav klidu, aktivace, sabotáž, přerušení, zkrat

### 5. Smyčka ATZ – odporově vyvažovaná dvojená




Obr. 6. Smyčka AZT [12]

V aktivaci – detektor 1 - Odpor se blíží součtu odporům rezistoru R1 + R2

V aktivaci – detektor 2 - Odpor se blíží součtu odporům rezistoru R1 + R3

V aktivaci – (detektor 1 + 2) - Odpor se blíží součtu odporům rezistoru R1 + R2 + R3

V aktivaci – sabotážní kontakt – odpor se blíží nekonečnu

V klidu – odpor se blíží hodnotě vyvažovacího rezistoru R1

Výhoda – lze detekovat stav klidu, aktivace detektoru 1, aktivace detektoru 2, aktivace současně obou detektorů, sabotáž, přerušení, zkrat

Nevýhoda – nelze určit, zda byl aktivován sabotážní kontakt detektoru 1 nebo detektoru 2

**Sběrnicová ústředna** umožnuje přímou adresaci čidel**.** Komunikace mezi ústřednou a detektory probíhá po datové sběrnici. Každý detektor obsahuje komunikační modul. Adresy detektorů jsou periodicky generovány ústřednou. Detektory mohou být připojeny v libovolném pořadí pomocí čtyřvodičového vedení. Dva vodiče jsou využívány pro datovou komunikaci a další dva vodiče jsou využívány pro napájení detektorů. Při vyhlášení poplachu je pak ústředna schopna určit, který konkrétní detektor byl aktivován a o jaký druh narušení se jedná. Výhodou těchto ústředen je použití menšího množství kabeláže [6].

U **smíšené ústředny** jsou detektory připojeny pomocí koncentrátorů. Koncentrátor je sběrnicový modul smyček. Detektory jsou ke koncentrátorům připojeny pomocí smyček a koncentrátory jsou připojeny k ústředně analogovou nebo datovou sběrnicí. Vyhodnocování pak probíhá různě, dle typu ústředny [6].

Pokud má ústředna dostatečnou kapacitu, je možné jednotlivé detektory napojit na vstupy koncentrátorů. Tím se ústředna změní na ústřednu s přímou adresací detektorů [6].

**Ústředna s bezdrátovou komunikací** se využívá například tam, kde není dovolené vedení kabelů nebo tam kde chceme minimalizovat stavební zásah (historické památky, novostavby atd.). Ústředny pracují v pásmu telemetrie 433 MHz nebo i 868 MHz. Detektory jsou napájeny lithiovou baterií nebo devíti voltovým destičkovým článkem. Napětí baterii je hlídáno a v případě poklesu napětí dojde k signalizaci. Signalizace nízkého napětí baterie může být realizována integrovaným bzučákem na místě nebo je tato informace přenesena do ústředny [6].

Výhody bezdrátových systému [6]:

- instalace je snadná a rychlá,
- možnost instalace systému s minimalizací stavebních zásahu do objektu,
- rozšíření systému o další prvky je snadné,
- změny v konfiguraci systému jsou snadné.

### 1.4.4 Napájecí zdroje

Napájecí zdroj slouží k napájení elektronických obvodů ústředny a všech prvků systému PZTS, které jsou k ústředně připojeny. Funkčnost systému musí být zachována i při výpadku napájecího napětí sítě. Jako záložní napájecí zdroj ústředny se používá bezúdržbový olověný akumulátor. U rozsáhlých systému je z důvodu úbytku napětí na dlouhých vedení nutné použít přídavný napájecí zdroj s vlastním náhradním zdrojem napětí. Základní napájecí zdroj musí být schopný dodávat potřebný proud ústředně a všem prvkům systému. Potřebný proud se rovná součtu proudového odběru ústředny a všech připojených prvků. Dále je nutné, aby základní napájecí zdroj byl schopný dobít záložní napájecí zdroj po výpadku, do doby stanovené dle normy ČSN EN 50131-1 ed.2 (viz. Tab. 1) [6].

Tab. 1. Požadované doby nabíjení [6]

| | Stupeň 1 | Stupeň 2 | Stupeň 3 | Stupeň 4 |
|---|---|---|---|---|
| Maximální doba dobíjení na min. 80% kapacity | 72 | 72 | 24 | 24 |

Norma ČSN EN 50131-1 ed.2 nám stanovuje i požadovanou dobu zálohování systému PZTS záložním zdrojem, při výpadku elektrické energie (viz. Tab. 2).

Tab. 2. Požadované doby zálohy [6]

| | Stupeň 1 | Stupeň 2 | Stupeň 3 | Stupeň 4 |
|---|---|---|---|---|
| Minimální doba pohotovosti (hod.) | 12 | 12 | 60 | 60 |

### 1.4.5 Elektronická požární signalizace

EPS je soubor zařízení sloužící k detekci požáru v době jeho vzniku, přivolání osoby schopné začít likvidovat vznikající požár, spuštění dalších požárních zařízení schopných likvidace požáru, usnadnění likvidace požáru nebo omezit šíření. EPS umožnuje [2;5]:

- rychle určit místo vzniku požáru,

- vyhlásit poplach,
- aktivovat a koordinovat evakuační systém,
- komunikovat automaticky s hasičským záchranným sborem (HZS).

Hlásiče požáru vždy detekují fyzikální projevy požáru. Dochází tedy k detekování vznikajícího tepla, detekování vyzařovaného plamene, detekování zplodin hoření a detekování přítomnosti plynů. Vyhodnocovací obvody hlásiče rozhodnou, jestli hodnota parametru nebo jeho změna nepřekonala přípustnou hodnotu [2;5].

Základní druhy hlásičů požáru [2;5]:

- **kouřové hlásiče**

Tyto hlásiče detekují požár v případě požárních aerosolů v ovzduší. K detekci se nejčastěji používá ionizační kouřový hlásič nebo opticko-kouřový hlásič. **Ionizační kouřový hlásič** funguje na principu změny protékajícího proudu ionizační komorou. Komora je tvořena dvěma elektrodami, mezi kterými je vzduch. Vzduch je ozařován radioaktivním materiálem a vznikají volné ionty. Pokud se kouř dostane mezi elektrody, volné ionty se začnou vázat na hmotnější částice kouře a dojde ke snížení vodivosti komory. **Opticko-kouřový hlásič** pracuje na principu rozptylu infračerveného záření na částečkách kouře. Rozptyl nebo absorpce infračerveného světla závisí na velikosti částic aerosolu, které se liší dle typů kouře (např. světlý, tmavý). Důležité je předpokládat druh hořícího materiálu.

- **teplotní hlásiče**

Teplotní hlásiče detekují dosaženou teplotu nebo změnu teplot v místnosti. Změna teploty je vyhodnocována na teplotně závislém prvku a má za následek změnu protékajícího elektrického proudu.

- **hlásiče plamene**

K detekci požáru se využívá vyzařování plamene. Pří hoření se detekuje ultrafialové záření nebo infračervené záření. Detektor ultrafialového záření je přesnější, ale snímací prvek má nižší životnost. U detektoru infračerveného záření se vyskytuje vetší množství falešných poplachů (teplé předměty, sluneční záření apod.)

- **lineární kouřové hlásiče**

Požár je detekován, pokud dojde k přerušení infračerveného paprsku mezi vysílačem a přijímačem. Přerušit IR paprsek můžou kouřové částice nebo teplotní turbulence při požáru. Vzdálenost mezi vysílačem a přijímačem je do 100 m.

Speciální druhy hlásiče požáru [2;5]:

- **CO hlásiče**

Hlásiče požáru reagují na koncentraci oxidu uhelnatého v prostoru. CO vzniká při hoření většiny paliv. Tento plyn je jedovatý a bez zápachu. Při nižších koncentracích způsobuje únavu, bolest hlavy, nevolnost. Při kontrakci 10000 ppm (1 % = 10000 ppm) smrt nastane v průběhu 2 a 3 minut. Reakce detektoru je nastavena na 40 ppm.

- **lineární teplotní hlásiče**

Umožňuje zachytit požár nebo přehřátí rovnou v rizikovém místě. Poskytuje nepřetržité monitorování po cele délce detekční kabeláže. Změny teploty vyvolávají změnu rezistence kabeláže. Tato změna je sledována a vyhodnocována. Výhodou je odolnost proti vlhkosti, špíně prachu, agresivním párám aj.

- **multisenzorové hlásiče**

Je sledováno více fyzikálních jevů hoření současně. Hlásiče jsou vybaveny dvěma nebo třemi senzory, které mezi sebou komunikují. Nejčastější kombinace senzorů jsou:

  - tepelný a opticko-kouřový,
  - tepelný, ionizační a opticko-kouřový,
  - Co a tepelný.

- **hlásiče s aktivním nasávacím systém – kouřové**

Princip spočívá v detekci rozptýleného světla. Pulzní laser generuje rozptýlené světlo, které detekují výkonné fotosenzory. Pomocí nasávacího zařízení a soustavy trubek jsou vzorky vzduchu přiváděny k laserovému detektoru. Vyhodnocuje se hustota kouře. Citlivost těchto hlásičů je vyšší než u běžných typu hlásičů.

### 1.4.6 Uzavřené televizní okruhy

Už řadu let dochází k rozvoji odvětví bezpečnostního průmyslu. Je to dáno prudkým vývojem informačních a komunikačních technologií (ITC). ITC se implementují za účelem

přizpůsobení současným trendům, mezi které patří např. integrace bezpečnostních systémů jako je SKV, PZTS a CCTV do jednoho propracovanějšího celku. Pro zabezpečení objektu se čím dál častěji využívají tzv. uzavřené televizní okruhy (Closed Circuit Television). Ty nám umožnují monitorování objektu v reálném čase. Dnešním trendem v CCTV jsou právě IP kamery. IP kameru (síťovou kameru) lze charakterizovat jako kameru s počítačem. Obsahuje centrální procesorovou jednotku (CPU), flash paměť a DRAM paměť. IP kamera tak může komunikovat s okolními zařízeními. Tím, že má kamera svoji IP adresu, umožnuje funkce jako [7]:

- sledovaní obrazu kamery téměř odkudkoliv,
- vzdálené ovládaní kamery,
- vzdálené konfigurování kamery.

IP kamery lze rozdělit dle konstrukce na:

- fixní IP kamery,
- PTZ IP kamery.

- **Fixní IP kamery**

Jde o IP kamery, které mají určen směr natočení. Změna směru natočení vzdáleně není možná. Využívají se tam, kde je potřeba snímat konkrétní oblast a není zde zapotřební možnosti otáčení, přiblížení apod. Existují fixní IP kamery s tzv. dome krytem. Tento kryt má tvar kopule. Fixní Dome kamery jsou méně nápadné a při využití neprůhledného krytí objektivu nelze z pohledu pachatele určit, která oblast je snímána [7].

- **PTZ IP kamery**

Název PTZ vznikl kombinací anglických slov pan, tilt a zoom. Tyto kamery umožnují tedy pohyb po horizontální, pohyb po vertikální ose a měnit zvětšení. Pohybovat těmito kamerami lze jak manuálně, tak automatický. Automatický pohyb může být nastaven na předem naprogramovaný podmět (analýza obrazu, naprogramované trasy) Existují mechanické IP PZT kamery, nemechanické IP PZT kamery a PTZ dome IP kamery [7].

Mechanické kamery se využívají převážně pro monitorování vnitřních prostor a jsou obsluhovány operátorem. Nemechanické kamery jsou při pohybu neslyšitelné. Využívá se zde širokoúhlé objektivy pro pokrytí rozsáhlých prostor. Nevýhodou je omezený pohyb kamery. PZT dome IP kamery vyžívají výhod jak PZT, tak dome krytu. Pohybu

v osách je neomezený a díky využití dome krytu nelze určit poloha kamery. Novými trendy v této oblasti jsou termální kamery a kamery s infračerveným přísvitem. Tyto kamery nám umožnují sledování oblastí pří naprosté tmě [7].

### 1.4.7 Systém kontroly vstupu

SKV slouží k ověření identity osob. Setkáváme se zde s tzv. autentizací (ověření, zda osoba, za kterou se vydává, je opravdu tou osobou). SKV se často kombinují se docházkovými systémy, které poskytují informace o důvodu a času průchodu místem kontroly. Osoby jsou identifikovány nejčastěji pomocí magnetických karet, karet s čarovým kódem, kontaktních a bezkontaktních čipových karet a biometrických rysů. Každé osobě jsou pak přiděleny konkrétní přístupová práva, podle personálních, časových a prostorových dispozic. Systém kontroly vstupu se většinou skládá z [4;5]:

- řídící jednotky,
- centrální jednotky,
- snímacího zařízení,
- blokovacího zařízení,
- identifikačního prvku,
- jednotky zápisu.

**Nejpoužívanější identifikační prvky rozdělit dle principu činnosti na:**

- **Magnetické identifikační prvky**

Jedná se o plastovou kartičku, na které je nanesen magnetický pásek. Po zmagnetizování pásku se na jeho povrchu vytvoří mále permanentní magnety. Zmagnetizovaný permanentní magnet představuje logickou jedničku a nezmagnetizovaný permanentní magnet představuje logickou nulu. Na magnetickou kartu jsou data zapsány tedy v binární podobě [4;5].

Výhody magnetických karet [4;5]:

- dynamická data,
- vysoká životnost,
- ekonomicky nenáročné.

Nevýhody magnetických karet [4;5]:

- poškození dat mechanický poškozením,
- poškození dat vlivem silného magnetické pole,
- omezená kapacita (délka proužku, hustota záznamu),
- snadně kopírovatelné.

- **Optické identifikační prvky**

Na plastové kartičce je nanesen kód, který je tvořený kombinací vertikálních tmavých čar a světlých mezer. Pokud dojde k osvícení čarového kódu infračerveným světlem, černé čáry toto záření pohlcují, zatímco světlé mezery záření odráží. Fotosenzor snímá odražené světlo, které je následně převedeno na elektrický signál. Podle délky elektrického signálu lze určit tloušťku čar a mezer [4;5].

Výhody karet s čarovým kódem [4;5]:

- ekonomicky nenáročné,
- rychlost a spolehlivost.

Nevýhody karet s čarovým kódem [4;5]:

- nelze použít v bezpečnostních systémech (snadné zkopírování),
- statická data,
- problém číst špinavé, rozmazané čarové kódy.

- **Čipové identifikační prvky**

Čipové identifikační prvky můžou být karty nebo přívěsky, které mají v sobě zabudovaný mikročip. Komunikace mezi mikročipem a snímacím zařízením může probíhat kontaktně nebo bezkontaktně [4;5].

**Kontaktní karty:**

Jako komunikační medium mezi čipovou kartou a snímacím zařízením se využívají pozlacené kontaktní plošky (piny). Tyto čipové karty neobsahují baterii a jsou napájený přes snímací zařízení. Nevýhodou je poškozovaní kontaktních plošek postupem času (odření, znečistění, oxidace) [4;5].

**Bezkontaktní karty:**

Ke komunikaci mezi snímacím zařízením a čipovou kartou se využívá technologie RFID (Radio Frequency Identification). Bezkontaktní identifikační karty mohou být aktivní nebo pasivní. Pozornost věnujme spíše pasivním čipovým kartám [13;14].

Snímací zařízení vysílá do okolí elektromagnetické vlny o konkrétní frekvenci. Pokud se čip ocitne v tomto elektromagnetickém poli, kondenzátor se nabije a dojde k aktivování logických a radiových obvodů. Následně jsou data přeposlány z čipu do snímacího zařízení. Důležitým parametrem je zde komunikační frekvence, která muže být různá. Od zvolené frekvence se pak odvíjí rychlost zápisu a čtení, komunikační dosah, prostupnost vln prostředím a materiálem [13;14].

Kritéria ovlivňující výkonnost systému [13;14]:

- nevhodně zvolené frekvenční pásmo,
- elektromagnetická interference jiných zdrojů,
- problémový materiál v okolí (kov, voda),
- špatné umístění komponentů RFID.

- **Biometrické prvky**

Identifikace pomocí jedinečných biologických charakteristik člověka patři mezi nejbezpečnější. RFID karty, magnetické karty aj. mohou být zkopírovány, odcizeny, ztraceny. Hesla a kódy PIN můžou být zapomenuty, popřípadě odpozorovány jinou osobou. Výhody biometrických systému vůči ostatním identifikačním prvkům jsou znázorněny na Obr. 7. Toto se u identifikace podle biometrických dat nemůže stát. Odpadá zde také potřeba nosit externí identifikační prvek u sebe a je nutné, aby při identifikací byla fyzická osoba na místě. Pro vyšší úroveň zabezpečení se biometrické systémy používají v kombinaci s dalšími systémy kontroly vstupu [15].

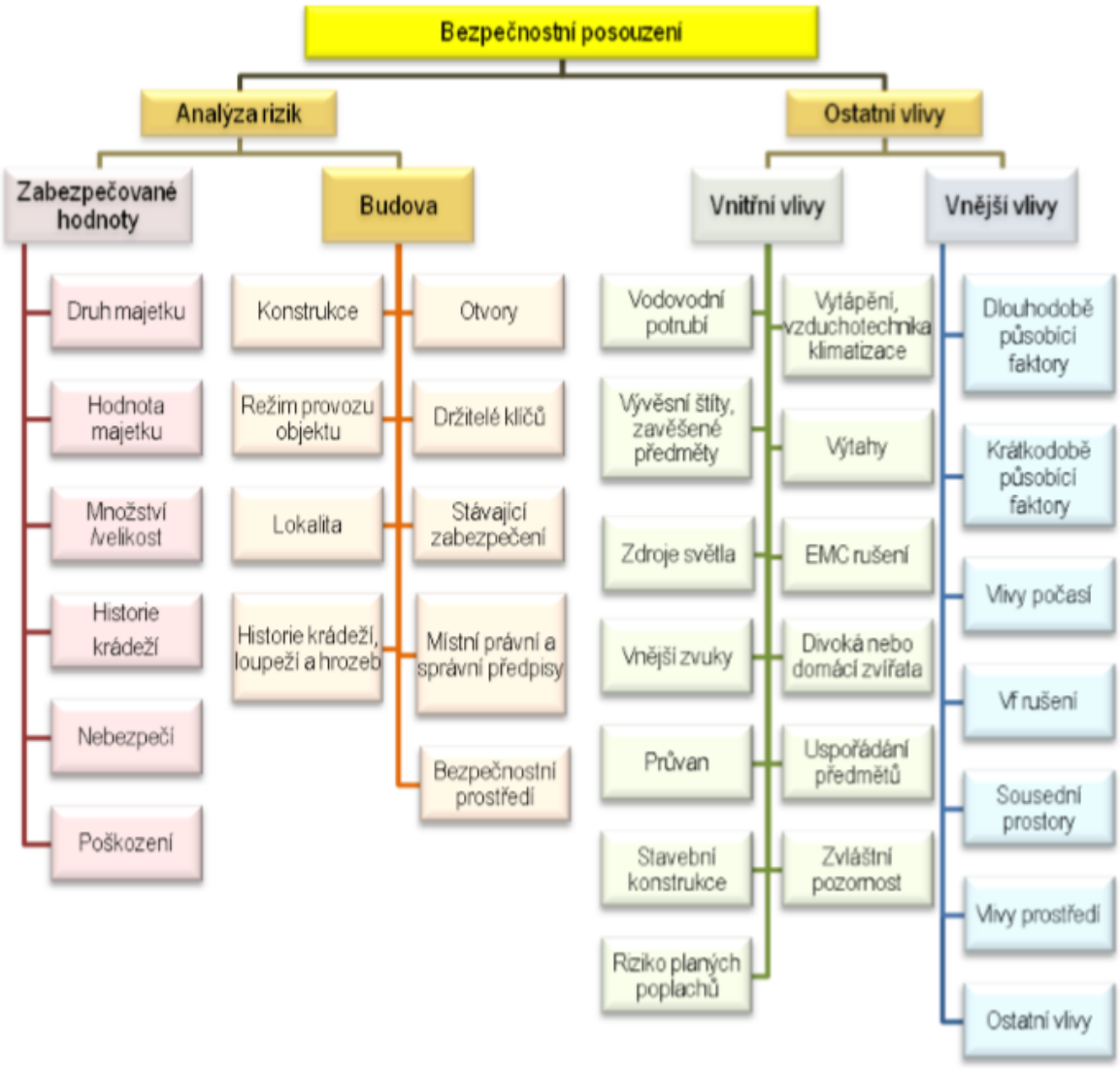

Obr. 7. Výhody Biometrie [15]

V biometrii existuje široká škála způsobů, jak identifikovat osobu. Setkat se může např. s identifikací podle otisku prstů, krevního řečiště ruky, geometrie ruky, oka (sítnice, duhovky), obličeje (2 D, 3 D), lidského hlasu, dynamiky podpisu a další. Mezi nejlevnější a nejvíce dostupné biometrické systémy patří čtečky otisku prstu. U snímačů skenujících povrch prstu se používají různé fyzikální principy. Snímače mohou být kapacitní, optické, teplotní, elektroluminiscenční, radiofrekvenční a multispektrální. Čtečky jsou nejčastěji vybaveny optickým senzorem. Tyto čtečky pracují na principu rozdílného odrazu světla (papilární linie odráží světlo, rýhy pohlcují světlo). Odražené světlo od povrchu prstu dopadá na CCD maticový detektor, kde se dále obraz digitalizuje a předává na zpracovaní. Poškození nebo znečištění prstu může mít vliv na správné vykreslení povrchu prstu [15].

# 2 BEZPEČNOSTNÍ POSOUZENÍ

Jeden z kroku, při návrhu poplachového zabezpečovacího systému, je bezpečnostní posouzení. Jeho legislativní základ je dán technickou normou ČSN CLC/TS 50131-7, TNI 334591-1 a směrnicemi pojišťoven. Bezpečnostní posouzení se věnuje čtyřem základním oblastem zájmu. Jsou to zabezpečované hodnoty, budova, vnitřní vlivy působící na PZTS (původ těchto vlivů je uvnitř zabezpečovaných objektů) a vnější vlivy působící na PZTS (původ těchto vlivů je mimo zabezpečované objekty) [3].

Tyto čtyři oblasti lze rozdělit do dvou kapitol – analýzu rizik a ostatní vlivy. Cílem bezpečnostního posouzení je zjistit, které faktory mají vliv na volbu a umístění komponentů PZTS, a dále stanovit potřebný stupeň zabezpečení. Přibližný obsah bezpečnostního posouzení můžeme vidět na Obr. 8 [3].




Obr. 8. Obsah posouzení objektu [3]

## 2.1 Zabezpečované hodnoty

Míra rizika vloupání do objektu závisí na charakteru objektu. Bezpečnostní analytik by tak měl navrhnout takové typy a množství komponentů, které odpovídají míře rizika vloupání. Pozornost by měla být věnována těmto faktorům [3;7]:

- **Druh majetku**

Zda se objekt stane obětí bezpečnostní hrozby, závisí z velké části právě na druhu majetku (aktiv) v objektu. Druh majetku nám určuje atraktivnost pro pachatele. Je zřejmé, že pachatel bude mít zájem spíše o majetek snadno zpeněžitelný nebo nenáročný na přepravu.

- **Hodnota majetku**

Nejen pro tvůrce bezpečnostního objektu, ale i pro pojišťovny, je tento údaj velice významný. Částka, kterou je klient schopný investovat do návrhu, se často odvíjí od pravděpodobné hodnoty ztráty a dalších výdajů týkajících se ztrát. Majetek nemusí mít vždy velkou finanční hodnotu, aby byl pro klienta důležitý. Majitel může mít k některým věcem osobní vztah a je potřeba, aby s tím byl obeznámen i tvůrce návrhu.

- **Množství**

Množství majetku je úzce spjato s hodnotu a druhem majetku. Velikost a množství majetku je úzce spojeno s jeho transportem, manipulací a příležitostí ukrýt tento odcizený majetek.

- **Historie krádeží**

Historie krádeží je nezbytnou součástí bezpečnostního posouzení. V případě, že v minulosti došlo ke vloupání (krádeži), lze zjistit způsob vloupání a druh majetku, na který se pachatel zaměřil. Tyto informace navrhovatel využije při určování hlavních rizik.

- **Nebezpečí**

Je posuzováno, zda majetek je nebezpečný pro osoby a okolní prostředí. Týká se to především skladů nebezpečných látek.

- **Poškození**

Majetek nemusí být vždy odcizen, a přesto může dojít k jeho ztrátě. V závislosti na poloze a charakteru objektu se můžeme setkat také s vandalismem a žhářstvím. Tvůrce návrhu musí v bezpečnostním posouzení zahrnout i tuto možnost.

## 2.2 Budova

Tam kde mají být naistalovány poplachové zabezpečovací a tísňové systémy, je potřeba brát v úvahu stavební dispozice objektu. Pozornost by měla být věnována těmto faktorům [3;7]:

- **Konstrukce**

Jsou hodnoceny konstrukce střech, stěn, podlah a dalších možných prostor objektu (např. sklepy)

- **Otvory**

Posuzují se všechny možné otvory, které by mohly usnadnit pachateli vstup do zabezpečovaného objektu (např. dveře, okna, ventilační kanály, střešní světlíky apod.)

- **Režim provozu**

Vyhodnocuje se doba osídlení (např. pracovní směny zaměstnanců), zda jsou využíváni pracovníci ostrahy, možnosti vstupu veřejnosti do objektu a jeho části.

- **Držitele klíčů**

Dosažitelnost držitelů klíčů, kteří jsou schopni reakce na činnost poplachového a zabezpečovacího systému.

- **Lokalita**

Hodnotí se zde úroveň kriminality v lokalitě, kde se objekt nachází. Posuzují se okolní sousední budovy, které by mohly usnadnit pachateli přístup do zabezpečovaného objektu. Podstatná je i kvalita a rychlost odezvy na signalizaci poplachového zabezpečovacího a tísňového systému.

- **Stávající zabezpečení**

Úroveň a rozsah současného poplachového zabezpečovacího a tísňového systému. Pozornost je věnovaná i mechanickým zábranným systémům.

- **Místní legislativa**

Požární předpisy a bezpečnostní požadavky, které by mohly mít vliv na návrh poplachového zabezpečovacího a tísňového systému.

- **Prostředí**

Musí se vzít v úvahu i to, jestli je objekt situován na venkově nebo v městské zástavbě.

## 2.3 Vnitřní vlivy

Před instalací poplachového zabezpečovacího a tísňového systému je potřeba vyhodnotit i vnitřní faktory, které by mohly mít vliv na systém. Jedná se především o plané poplachy. Pro komponenty PZTS je teda potřeba zvolit správné umístění a nastavení (obzvlášť u detektorů). Pozornost by měla být věnována těmto faktorům [3;7]:

- **Vodovodní potrubí**

Proudění vody v plastovém potrubí může mít vliv na mikrovlnné detektory.

- **Vytápění, vzduchotechnika a klimatické systémy**

Zde je riziko ovlivnění detektorů turbulentním prouděním vzduchu vznikající z činnosti těchto systému. Turbulentní proudění může mít vliv na ultrazvukové detektory.

- **Závěsné předměty**

V zorném poli detektorů se nesmí vyskytovat závěsné předměty, který by se mohly pohybovat. Jedná se o rostliny, lampy, záclony aj.

- **Výtahy**

Na detektory můžou mít vliv i vibrace způsobené výtahy. Tyto vibrace se přenáší na stěny budovy, a tak může dojit k ovlivnění otřesových detektorů.

- **Zdroje světla**

Je důležité brát v úvahu vliv osvětlovacích zařízení jako jsou kompaktní výbojky, fluorescenční světelné zdroje (vliv na mikrovlnné detektory) nebo bodové reflektory (vliv na PIR detektory).

- **Elektromagnetické rušení**

Funkčnost PZTS může být ovlivněna rušením, které může do zařízení vnikat po signálním vedení nebo napájecím vedení. Je potřeba brát v úvahu i vlivy elektrostatických výbojů při práci s elektronickými součástkami.

- **Vnější zvuky**

Netěsnosti ve vzduchovém potrubí, kompresory, telefonní zvonky a další zařízení můžou generovat zvuky ve stejném frekvenčním spektru, ve kterém detektory pracují.

- **Divoká nebo domácí zvířata**

Detektory musí výt vybrány, rozmístěny a nastaveny tak, aby maximálně eliminovaly plané poplachy způsobené pohybem zvířat.

- **Průvan**

Průvan může ovlivnit funkci pasivních infračervených detektorů a ultrazvukových detektorů. Proudění vzduchu může způsobovat zvuky, rychle změny teplot, pohyb závěsných předmětů.

- **Uspořádání skladovaných předmětů**

Změny v uspořádání skladovaných předmětu můžou vést k zastínění zorného pole detektorů.

- **Stavební konstrukce objektu, zvláštní pozornost**

Hodnotí se materiál a konstrukce sklepů, podlah, stěn, střech. Stavební konstrukce má vliv na výběr a umístění detektorů. Lehký stavební materiál konstrukce může mít za následek vznik vibrací. Typ konstrukce skla může mít vliv na kondenzaci vodních par na jeho povrchu.

- **Riziko planých poplachů u tísňových systémů**

Norma doporučuje rozmístění detektorů tak, aby vznik planých poplachu byl minimální. Jedná se například o zamezení neúmyslného aktivování tísňového zařízení dětmi apod.

## 2.4 Vnější vlivy

Tyto vlivy nemůžeme žádným způsobem ovlivnit. Je potřeba je zhodnotit a přizpůsobit jim volbu a rozmístění detektorů. Pozornost by měla být věnována těmto faktorům [3], [7]:

- **Dlouhodobé působící faktory**

Předpokládané působení těchto vlivů jsou roky nebo desítky let. Jedná se zejména o podzemní dopravní systém, železnice, silnice, parkoviště, leteckou dopravu a přírodní vlivy (pohyb půdy, silné poryvy větru).

- **Krátkodobé působící faktory**

Působení těchto vlivu je krátkodobé. Jedná se zejména o výstavby, které probíhají v blízkosti objektu.

- **Vlivy počasí**

Na volbu komponentů PZTS má vliv převažující počasí. Je nutné zjistit, zda se objekt nachází v oblastí s výskytem silných dešťů, silných větrů, nadměrnému množství blesků apod.

- **Vysokofrekvenční rušení**

Je potřeba věnovat pozornost odolnosti vůči elektromagnetickému rušení vybraných zařízení v případě, že se nachází v blízkosti antén vojenských a civilních radarů, vysílačů televize nebo veřejné sítě, základových stanic systému GSM apod.

- **Sousední objekty**

Sousední objekty žádným způsobem nesmí ovlivňovat činnost prvku PZTS. Je potřeba se informovat o případném využívání těžkých strojů (vytváření vibrací) nebo zařízení generující vysoké elektromagnetické rušení.

- **Vlivy klimatických podmínek**

Je potřeba zvolit zařízení, které jsou vhodné pro příslušné klimatické podmínky a splňovat požadované parametry (pracovní rozsah teplo a vlhkosti).

- **Ostatní vlivy**

Osoby pohybující se v perimetru objektu nebo děti hrající si v okolí objektu můžou být příčinou planých poplachů. Je tedy potřeba předcházet i těmto způsobům vyvolání poplachů.

## 2.5 Stupeň zabezpečení a třída prostředí

Cílem bezpečnostního posouzení je vybrat vhodný stupeň zabezpečení a vhodnou třídu prostředí. Stupně zabezpečení jsou definovány v normě ČSN EN 50131-1 ed. 2 a jsou rozděleny dle předpokládaného vybavení a znalostí potenciálního pachatele (viz. Tab. 3). Dalším krokem je stanovení tříd prostředí, které nám určují, v jakém prostředí budou komponenty PZTS pracovat. Klasifikace třídy prostředí je uvedena v Tab. 4 [3].

Tab. 3. Stupeň zabezpečení [3]

| Stupeň | Míra rizika | Předpokládaný typ pachatele |
|---|---|---|
| 1 | Nízké | Narušitel má malou znalost PZTS; má základní sortiment snadno dostupných nástrojů |
| 2 | Nízké až střední | Narušitel má omezenou znalost PZTS; má základní sortiment běžného nářadí a přenosných přístrojů |
| 3 | Střední až vysoké | Narušitel je obeznámen s PZTS; má rozsáhlý sortiment nástrojů a přenosných elektronických zařízení |
| 4 | Vysoké | Narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí; má kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů PZTS |

Tab. 4. Třídy prostředí [3]

| Třída prostředí | Název prostředí | Popis prostředí, příklady | Rozsah teplot |
|---|---|---|---|
| I. | Vnitřní | Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách při stálé teplotě (např. v obytných nebo obchodních objektech) | + 5 °C až + 40°C |
| II. | Vnitřní všeobecné | Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách, kde není stálá teplota (např. na chodbách, v halách nebo na schodištích a tam, kde může docházet ke kondenzaci na oknech a v nevytápěných skladových prostorách nebo skladištích, v nichž vytápění není trvalé). | - 10 °C až + 40°C |
| III. | Venkovní chráněné | Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty PZTS nejsou plně vystaveny povětrnostním vlivům. | -25 °C až + 50°C |
| IV. | Venkovní všeobecné | Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty PZTS jsou plně vystaveny povětrnostním vlivům. | -25 °C až + 60°C |

Rozsah PZTS lze dále stanovit dle informativní přílohy normy ČSN CLC/TS 50131-7. Ta nám slouží jako pomůcka pro stanovení rozsahu PZTS dle stupně zabezpečení, který byl pro daný objekt zvolen (viz Tab. 5) [3].

Tab. 5. Rozsah PZTS [3]

| Střeží se | Stupeň 1 | Stupeň 2 | Stupeň 3 | Stupeň 4 |
|---|---|---|---|---|
| Obvodové dveře | O | O | O+P | O+P |
| Okna | | O | O+P | O+P |
| Ostatní otvory | | O | O+P | O+P |
| Stěny | | | P | P |
| Stropy nebo střechy | | | P | P |
| Podlahy | | | | P |
| Místnosti | T | T | T | T |
| Předmět (vysoké riziko) | | | S | S |

O – otevření
P – průnik (dohled na stavební komponenty pro detekci narušení nebo pokusu o narušení)
T – past (dohled ve vybraných prostorech, v nichž je vysoká pravděpodobnost detekce)
S – objekt vyžadující zvláštní pozornost

## 2.6 Bezpečnostní analýza

Při provádění bezpečnostního posouzení je zapotřebí vždy provést analýzu. Každá analytická metoda je nějakým způsobem jedinečná. U bezpečnostního posouzení objektu není konkrétně definované, jakou analytickou metodu použít. Typ analytické metody a její rozsah závisí na navrhovateli. Než začneme provádět analýzu, je zapotřebí si objasnit některé ze základních pojmů [7]:

- **Aktivum**

Aktivum má vždy nějakou hodnotu pro zabezpečovaný objekt. Motivace útočníka je závislá na hodnotě aktiva. Aktiva lze rozdělit na:

- Hmotná – jedná se např. o elektroniku, nemovitosti, šperky, cenné papíry apod.,
- Nehmotná – jedná se např. o „know how“ firem apod.

- **Riziko**

Vyjadřuje nám stupeň nebo míru ohrožení, pravděpodobnost vzniku negativního jevu, výsledek tohoto negativního jevu.

- **Hrozba**

Silová složka, aktivita či událost, popřípadě osoba, která stojí za vznikem např. požáru, přírodní katastrofy, krádeže nebo má nějaký podíl na vzniku škody.

- **Zranitelnost**

Parametr, který se týká určitého aktiva, na které má vliv existující hrozba. Míra zranitelnosti aktiva se klasifikuje dle kritičnosti (důležitost aktiva pro daný subjekt) a citlivosti (náchylnost aktiva k poškození existující hrozbou).

- **Protiopatření**

Jsou procesy, postupy, technické prostředky a další prvky, jejichž využití vede k omezení vlivu hrozby, popřípadě k jejímu úplnému odstranění. Hlavním cílem protiopatření je předcházet vzniku škody a popřípadě ulehčit překonání následků škody. Parametry, které charakterizují protiopatření jsou:

- míra efektivnosti protiopatření,
- náklady potřebné k realizaci opatření.

Analýza rizik je proces, ve kterém dochází k určení konkrétních hrozeb, jejich velikosti a jejich vlivu na bezpečnost daného objektu. Cílem vyhodnocení velikosti rizik je stanovení pravděpodobnosti projevení ohrožení a stanovení následku po projevení ohrožení [7].

Analýza rizik většinou obsahuje [7]:

- určení aktiv,
- ohodnocení aktiv,
- určení slabin a hrozeb,
- určení závažnosti.

### 2.6.1 Metody bezpečnostních analýz

K vytváření bezpečnostních analýz lze využít širokou škálu metod. Analytické metody lze rozdělit podle metody vyjádření používaných veličin (viz. Obr. 9) [7].


Obr. 9. Dělení metod dle vyjádření používaných veličin [17]

- **Kvalitativní**

Tyto metody jsou sice rychlejší a jednodušší, ale za to subjektivní. Aktiva, hrozby a zranitelnost mají slovní nebo číselné hodnocení. Výsledek těchto metod záleží hodně na osobním názoru hodnotitele. Chybí zde jednoznačné finanční vyjádření (např. kontrola nákladů). Příklady kvalitativních metod jsou uvedeny níže [8;16].

a) FMEA – analýza selhání a jejich dopadu,

Metodu je vhodné použít při zavádění nových výrobků, systémů, procesů nebo ke zlepšení kvality výrobku, systémů a procesů. Zjišťují se poruchy, či závady ve výrobním provozu, které vedou k zhoršení celého výrobního provozu. Postup při vypracování analýzy FMEA, v základních bodech, je následující [18]:

- zjištění a popis problému,
- stanovení závažnosti dopadu,
- stanovení pravděpodobnosti, že se v současném procese problém vyskytne,
- stanovení odladitelnosti problému,
- stanovení míry rizika,
- stanovení opatření na okamžité zastavení šíření problému,
- stanovení příčiny výskytu problému,
- stanovení opatření, aby se problém dále nevyskytoval,
- stanovení nové míry rizika.

b) Metoda DELPHI

Metoda patří mezi nejpoužívanější kvalitativní metody analýzy rizik. Jedná se o odhad budoucího vývoje pomocí skupiny expertů. Metoda DELPHI určuje, co se může stát a za jakých podmínek. Využívá se pro generování nových myšlenek stejně jako u brainstormingu. Hlavní nevýhodou je její časová náročnost [17].

c) PHA – PRELIMINARY HAZARD ANALYSIS

Předběžná analýza nebezpečí. Je postup na vyhledávání nouzových situací a nebezpečných stavů, zjištění jejich příčin a dopadů a zařazení do kategorií, podle předem stanovených kritérií. Tato metoda zahrnuje celou řadu technik pro posuzovaní rizik. Metoda může

být aplikovaná v počátečním stádiu projektování, kdy jsou k dispozici pouze velmi všeobecné záměry a technologická schémata [17].

d) HAZOP – HAZARD OPERATION PROCESS

Je analýza ohrožení a provozuschopnosti. Považuje se za týmovou expertní multioborovou metodu, při které se využívá brainstorming. Postup se zakládá na pravděpodobnostním hodnocením ohrožení a možných rizik. Účelem je identifikace scénářů potenciálního rizika. Díky své jednoduchosti se stala jednou z nejrozšířenějších metod pro identifikaci rizika a provozuschopnosti zařízení [17].

e) ETA – EVENT TREE ANALYSIS

Analýza stromu událostí je graficko-statistická metoda. Postup spočívá v sledování průběhu procesu od iniciační události přes konstruování událostí vždy na základě dvou možností nepříznivé a příznivé. Systémový strom událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Znázorněny jsou veškeré události, které se mohou vyskytnout v posuzovaném systému. Při nárůstu událostí se graf rozvětvuje jako větvě stromu [17].

f) SWOT analýza

Univerzální analytická metoda sloužící ke zjištění vnějších a vnitřních faktorů, které ovlivňují úspěšnost organizace nebo konkrétního záměru (např. nový produkt nebo služba). Často se používá v rámci strategického plánovaní či marketingu. Při SWOT analýze dochází k identifikaci faktorů, kterými jsou silné stránky, slabé stránky, vnější příležitosti a hrozby. Cílem je identifikovat problémové oblasti, definovat cílový stav pro dané oblasti a stanovit opatření [17].

g) Safety Audit

Bezpečnostní kontrola je nejstarší metodou analýzy rizik. Dochází k hledaní rizikových situací a navržení opatření na zvýšení bezpečnosti. Hledají se potencionální možné nehody nebo provozní problémy, které se mohou naskytnout v posuzovaném systému. Formálně je využíván připravený seznam otázek a matice pro skórování rizik [17].

h) Check List analysis

Analýza pomocí kontrolního seznamu je systematická kontrola plnění předem stanovených podmínek a opatření. Kontrolní seznam je vytvořen na základě charakteristik sledovaného systému a souvisejících činností. Struktura seznamu může být od jednoduché až po složitou, kde muže být zahrnuta relativní důležitost parametru v rámci daného souboru [17].

i) WHAT – IF ANALYSIS

Analýza „co se stane když “. Tato metoda využívá brainstormingu. Jde o spontánní diskuzi skupiny zkušených odborníků, kteří jsou obeznámení s procesem. Hledají se možné dopady vybraných provozních situací (ohrožující situace nebo přímo havarijní události). Ze získaných informací je možno určit předpokládané následky, vyhodnotit existující preventivní opatření a dále doporučit možnosti pro snížení rizika [17].

- **Kvantitativní**

Kvantitativní metody jsou mnohem více přesnější než kvalitativní. Jejich vypracování zabere větší množství času. Hodnoty aktiv a rizik jsou vyjádřeny ve finančních jednotkách a zvládaní rizik je tak jednodušší. Příklady kvantitativních metod jsou uvedeny níže [8;16].

a) FTA – FAULT TREE ANALYSIS

Analýza stromu poruch je založena na systematické zpětném rozboru událostí za využití řetězce příčin, které můžou směřovat k vybrané vrcholové události. Jedná se o graficko-statistickou metodu. Systémový strom poruch představuje rozvětvený graf s dohodnutou symbolikou a popisem. Cílem této metody je posoudit pravděpodobnost vrcholové události [17].

b) HRA – HUMAN RELIABILITY ANALYSIS

Analýza lidské spolehlivosti je zaměřena na posouzeni vlivu lidského činitele na výskyt havárii, nehod, živelných pohrom, útoků apod. Koncept analýzy HRA míří k systematickému posouzení lidské chyby a lidského faktoru. Zahrnuje přístupy makro-ergonomické a mikro-ergonomické. Analýza má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce [17].

c) QRA – QUANTITATIVE RISK ANALYSIS

Kvalitativní posuzovaní rizika je systematický a komplexní přístup pro predikci odhadu četnosti a dopadů nehod pro zařízení nebo pro provoz systému. Metoda se využívá v oblasti bezpečnostních organizaci, projektů, procesu a informačních systému. Umožnuje identifikaci nebezpečí a určit jejich prioritu. Přínos metody je jednoznačný, odhalit zdroje rizika a navrhnout potřebná opatření s ohledem na efektivitu investice [17].

# II. PRAKTICKÁ ČÁST

# 3 ÚVOD DO PRAKTICKÉ ČÁSTI

Cílem praktické části je navrhnout zabezpečovací systém firmy, zaměřené na elektroinstalační práce v oblasti vysokého i nízkého napětí. Objektem zabezpečení je její areál, včetně provozovny. Objekt se nachází v blízkém okolí města Zlín.

Na přání majitele nebudou v této práci uveřejněny žádné údaje, které by přímo identifikovaly nejmenovanou firmu, a to z bezpečnostních důvodů. Firma vzhledem ke své činnosti skladuje velké množství drahých kovů, které by se mohly stát předmětem odcizení. Práce by pak mohla sloužit jako manuál k překonání stávajícího zabezpečovacího systému.

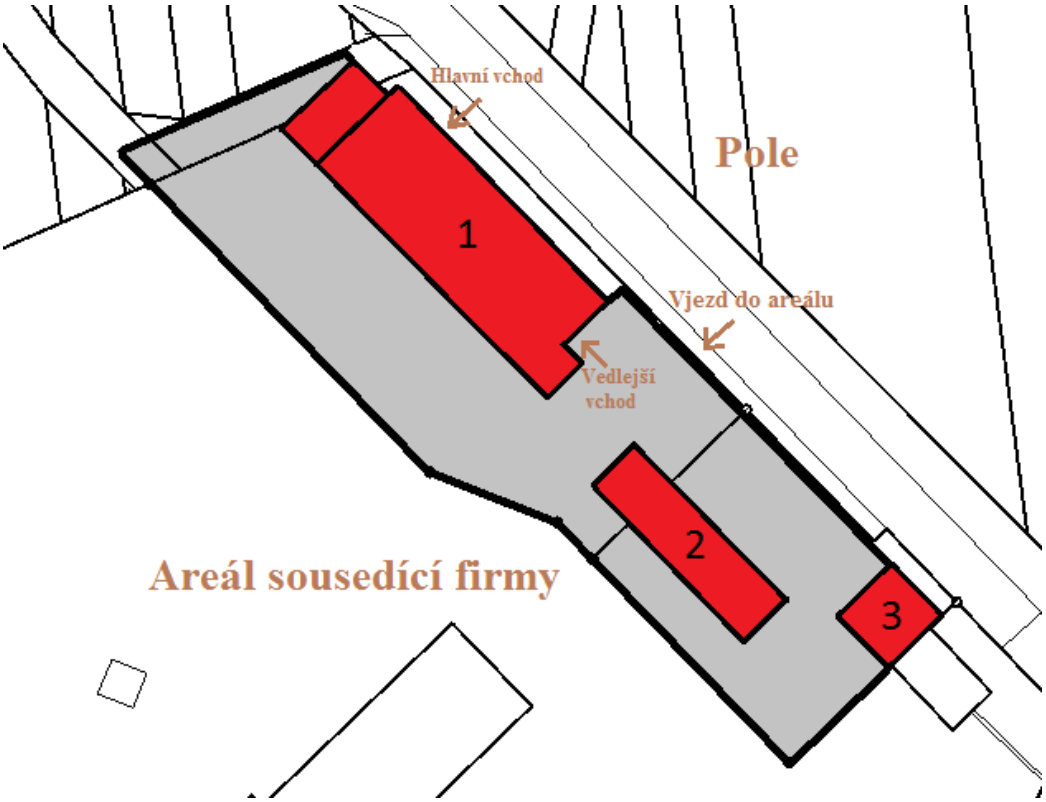
Dále firma plánuje modernizaci zabezpečení celého objektu a ráda by výsledky této práce použila pro inspiraci, event. na možné porovnání s podklady, které pro ně bude zpracovávat v rámci zakázky profesionální firma v daném oboru. Z těchto důvodů budou vypracovány na základě provedeného bezpečnostního posouzení a bezpečnostní analýzy rizik dva návrhy zabezpečení.

První bude navržen i s ohledem na kladené požadavky majitele firmy a druhý se bude pouze opírat o zkušenosti a znalosti získané během mého studia oboru Bezpečnostní technologie, systémy a management na Fakultě aplikované informatiky, Univerzity Tomáše Bati ve Zlíně.

K vypracování firma přislíbila plnou svou podporu, a to v rozsahu poskytování nutných informací týkajících se jejího provozu a technických dokumentacích příslušného areálu, včetně objektů v něm.

# 4 POPIS OBJEKTU

Zabezpečovaným objektem je firma poskytující kompletní portfolio služeb v oblasti elektromontážních prací. Rozloha celého areálu firmy je přibližně 2645 $m^2$. V areálu firmy se nachází tři budovy. Budova č.1, o rozloze 423 $m^2$, je využívána pro administrativní účely, a běžné potřeby montážních techniků. Součástí budovy č.1 je i garáž pro montážní jeřáb. Budova č.2, o rozloze 120 $m^2$, slouží jako sklad materiálu a sklad nářadí. Budova č.3, o rozloze 64 $m^2$, slouží jako sklad materiálu a současně je využívána jako garáž pro vysokozdvižný vozík. Venkovní prostory areálu firmy, tvořené betonovými panely, jsou využívány pro skladování materiálu a parkování firemních automobilů. Do areálu je možný příjezd prostřednictvím brány, ze severní strany. Z této strany se nachází hlavní vchod do budovy č.1. Před budovou se nachází parkoviště, které slouží zaměstnancům i zákazníkům firmy.




Obr. 10. Půdorys areálu firmy [19]

Na Obr. 1 je zobrazení půdorysu areálu firmy. Pozemek areálu firmy je vybarven šedou barvou a zabírá plochu přibližně 2038 $m^2$. Budovy jsou vybarveny červenou barvou.

Z půdorysu můžeme vidět, že firma vlastní budovu č.3 jen z části. Druhou část budovy vlastní jiná firma, která dříve tuto část budovy využívala jako místnost pro fyzickou ostrahu objektu. V současné době, sousedící firma tuto část budovy nevyužívá a její areál je střežen zabezpečovacími systémy.

Objekt se nachází asi dva kilometry od centra města. Příjezd k objektu je možný po komunikaci, která propojuje dvě odlehlejší částí města s centrem města. V okolí areálu zabezpečovaného objektu a sousedící firmy jsou pouze pole. Nejbližší obydlené objekty jsou ve vzdálenosti přibližně 350 m.

Zabezpečovaný objekt je osídlen pouze přes týden od 6:00 do 15:00 hod. O víkendu objekt není osídlen. Areál sousedící firmy je bez přítomnosti lidí a je navštěvován zaměstnanci v případě rekonstrukcí, oprav, revizních a údržbových prací.

# 5 BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU

Bezpečnostní posouzení objektu bylo provedeno dle normy ČSN CLC/TS 50131-7, kde cílem bylo zjistit do jaké míry objekt zabezpečit a jaké použít komponenty při realizaci.

## 5.1 Bezpečnostní posouzení – zabezpečované hodnoty

Jde o firmu, která poskytuje kompletní služby v oblasti elektromontážních prací. To znamená, že v jejich skladech je uloženo speciální nářadí pro spojování, montáž, instalaci a elektrické ruční nářadí.

Sklady jsou dále naplněny uloženým elektroinstalačním materiálem jako např. hromosvodařský materiál, úložný a spojovací materiál, rozvaděče a skříně, transformátory, kabely pro výstavbu rozvodů vysokého a nízkého napětí, a spousta dalšího elektroinstalačního materiálu. Venkovní plochy areálu jsou rovněž využívány pro skladování materiálu viz. Obr. 11 a Obr. 12. Celková hodnota skladovacího elektroinstalačního materiálu je více jak dva milióny korun.

Obr. 11. Venkovní skladování elektroinstalačního materiálu 1

Obr. 12. Venkovní skladování elektroinstalačního materiálu 2

V případě vloupání do budovy č. 1, budou pravděpodobně pro pachatele cílem počítače, notebooky, tiskárny a firemní mobilní telefony, které se nacházejí v kancelářských prostorech. Cena tohoto kancelářského vybavení je přibližně 100 tisíc korun.

Pro případného pachatele by mohl být cílem i vozový park firmy, který čítá deset automobilů v celkové hodnotě 3 milióny korun. Jedná se osobní automobily, montážní dodávky a montážní jeřáb. Většina automobilů je po pracovní době parkována uvnitř areálu firmy a nejsou běžně využívány k osobním účelům zaměstnanců. Občas je osobní automobil využit k přepravě zaměstnance do práce. Firma je pojištěná na vzniklou škodu do deseti miliónů korun.

- **Historie krádeží**

V minulost došlo k vloupání do objektu už třikrát. Přesný způsob vloupání není znám. Pachatelé se většinou zaměřili na elektroinstalační materiál. Pachatele se podařilo dopadnou pouze v jednom případě.

## 5.2 Bezpečnostní posouzení – budova

Jak bylo zmíněno, v zabezpečovaném objektu se nachází tří budovy. Budova č. 1 a budova č. 2 prošly částečnou rekonstrukcí. Budova č. 3 je v původním stavu.

- **Konstrukce budovy**

Budova č.1 je jednopodlažní budova s půdou. Půdou vedou rozvody EPS, ale jinak není firmou využívána. Střecha je sedlového typu pokrytá lepenkovou střešní krytinou. Nosná konstrukce střechy je dřevěná. Obvodové stěny jsou z plných cihel tloušťky 340 mm. Zdivo je omítnuté jak z vnější strany, tak z vnitřní strany. Budova není zateplená. Místnosti

budovy tvoří vnitřní zdivo z plných cihel tloušťky 160 mm a dozdívky z tvárnic ytongu tloušťky 100 mm a 150 mm. Z východní strany budovy č. 1 se nachází nižší přístavba s pultovým typem střechy. Střecha je pokryta lepenkovou střešní krytinou. Po střese této přístavby se lze dostat ke dveřím od půdy. Z půdy není umožněn průchod do podlažní části budovy. Z jižní strany se nachází balkón, na který je možný přistup z kanceláře majitele firmy. Ze severní strany je k budově č. 1 přistavena garáž s výsuvnými sekčními vraty. Garáž má pevnou železnou konstrukci. Střecha je sedlového typu a je tvořena dřevěnou nosnou konstrukcí s plechovou střešní krytinou. Tato střecha nenavazuje na hlavní sedlovou střechu budovy č. 1. Na vytvoření boční stěny garáže byl použit vlnitý plech a polykarbonát Lexan.

Obr. 13. Budova č.1

Budova č. 2 je jednopodlažní budova se sedlovitou střechou (viz Obr.12). Střecha je pokryta lepenkovou střešní krytinou. Obvodové stěny jsou z plných cihel tloušťky 340 mm. Zdivo je omítnuté jak z vnější strany, tak z vnitřní strany. Budova není zateplená.

Budova č. 3 je jednopodlažní s plochou, jednoplášťovou střechou. Střecha je pokryta plechovou krytinou. Obvodové stěny jsou z plných cihel tloušťky 340 mm. Zdivo je omítnuté jak z vnější strany, tak z vnitřní strany. Boční stěna je společná se sousední budovou. Budova není zateplená.

Obr. 14. Budova č.3

- **Otvory**

K vstupu do budovy č. 1 lze využít hlavní vchod ze severní strany budovy, který je určen jak pro zaměstnance, tak pro zákazníky. Hlavní vstupní dveře do této budovy jsou plastové konstrukce, o rozměrech 1100 x 2100 mm. Ke vstupu do budovy č. 1 lze použít i dva vedlejší vstupy z venkovního areálu firmy, které jsou určeny pouze pro zaměstnance. Jedná se o dvoukřídlé dřevěné dveře o rozměrech 1250 x 2100 mm. Všechny vstupní dveře jsou opatřeny cylindrickou vložkou s kováním. Po celém obvodu budovy je umístěno patnáct dvoukřídlých oken o rozměrech 1300 x 1300 mm, pět dvoukřídlých oken o rozměrech 1000 x 1300 mm, tři jednokřídlá okna o rozměrech 955 x 1300 mm, dvě jednokřídlá okna o rozměru 600 x 600 mm a francouzské okno složené ze tří dílů, z nichž prostřední díl lze otevřít. Francouzské okno má rozměry 2550 x 2100 mm. Půda je uzavřena plechovými dveřmi o rozměrech 900 x 1500 mm. Plechové dveře jsou uzamčeny visacím zámkem.

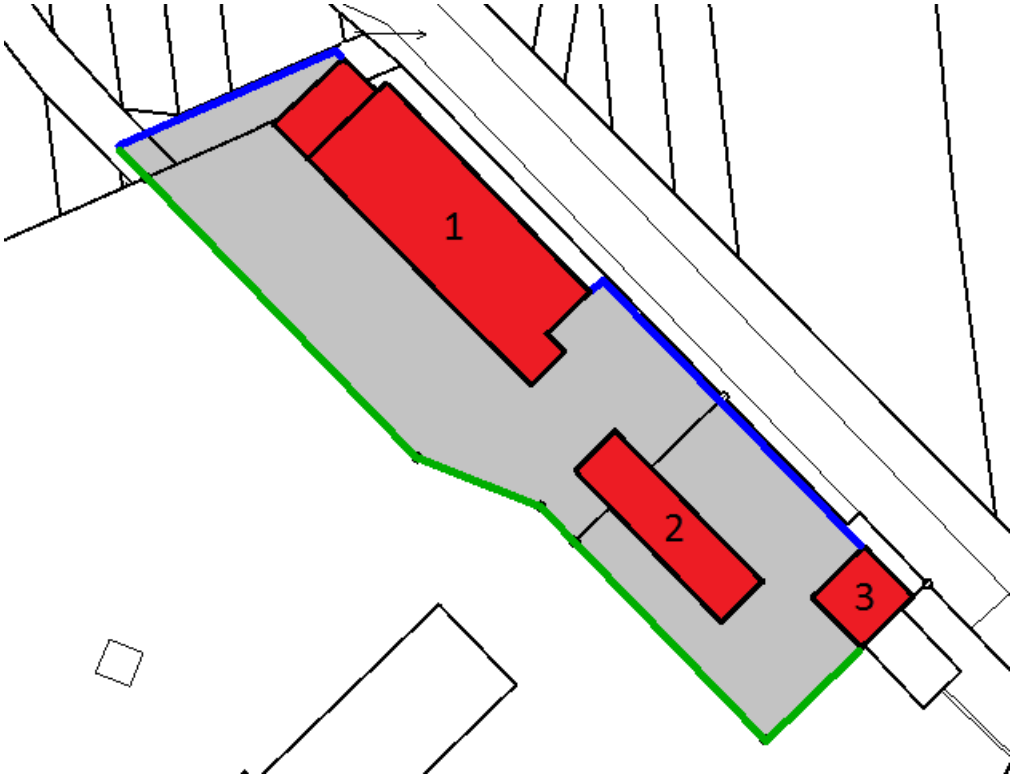
Budova č. 2 má dva vstupy. Pro vstup zaměstnanců se využívají dvoukřídlá plechová vrata o rozměrech 1500 x 2000 mm. Pro vyvážení a navážení materiálu vysokozdvižným vozíkem se používají dvoukřídlá plechová vrata o rozměrech 3000 x 3000 mm. K uzamčení obou vrat jsou použity visací zámky. Budova má devět neotevíratelných oken o rozměru 1200 x 600 mm. Všechny okna jsou plastové konstrukce s izolačními dvojskly.

Do budovy č. 3 je možný vstup dvěma dvoukřídlými plechovými vraty. Vrata mají rozměry 2800 x 3300 mm. Jedny vrata se využívají ke vstupu do části budovy se skladem materiálu. Druhé vrata se využívají pro parkování vysokozdvižného vozíku. K uzamčení obou vrat

jsou použity visací zámky. Budova má šest neotevíratelných oken o rozměru 1200 x 600 mm. Okna mají železnou konstrukci a jako výplň je použito sklo s drátěnou vložkou.

- **Perimetr objektu**

Oplocení objektu, ze severní a západní strany, tvoří dřevěný plot o výšce dvou metrů, který se napojuje na budovu č. 1 a č. 3. Mezi budovou č. 1 a č. 3 se nachází dřevěná posuvná brána s pohonem, která je využívána při vjezdu a výjezdu automobilů z areálu objektu. Brána má železnou konstrukci. Oplocení objektu z jižní a východní strany je tvořeno drátěným pletivem o výšce dvou metrů. Pletivo je potažené plastem. Ochranu proti přelezení oplocení zajišťují šikmé vzpěry, na kterých je nainstalovaný ostnatý a žiletkový drát. Pro lepší představu je perimetr objektu zaznačen na Obr. 15 (zelená čára – drátěné oplocení, modrá čára – dřevěné oplocení).




Obr. 15. Perimetr objektu [19]

- **Režim provozu objektu**

Firma čítá dvacet zaměstnanců. V objektu se pracuje pouze přes týden. O víkendu je objekt neosídlen. Pracuje se na jednosměnný provoz od šesti do patnácti hodin. Firemní automobily jsou po pracovní době zaparkovány v areálu firmy. Vstup veřejnosti do areálu firmy není možný. Zákazníci mohou vejít do budovy č. 1 hlavním vchodem, za překladu, že jim je otevřeno majitelem nebo zaměstnancem firmy. V budově č.1 je pro zákazníky vyhrazena jedna místnost.

- **Držitele klíčů**

Klíče od budovy č. 1 mají všichni zaměstnanci. Klíče od budovy č. 2 a č. 3 má skladník. Dálkové ovladače od posuvné brány jsou připnuty ke všem klíčům firemních automobilů. Klíče jsou vždy po skočení pracovní doby uloženy v uzamykacím plechovém boxu v místnosti 1.06. Klíček od boxu je schován v šuplíku jedno z pracovních stolků.

- **Lokalita objektu**

Objekt se nachází asi dva kilometry od centra města, v odlehlejší lokalitě. Pohyb osob je zde minimální a s vandalismem se zde nesetkáme. Pro potencionální pachatele by odlehlejší klidná lokalita mohla být výhodou. Cesta autem z centra města k zabezpečovanému objektu trvá přibližně pět minut.

- **Stávající zabezpečení**

Prostory firmy jsou proti vniknutí cizích osob chráněny PIR detektory, reagující na pohyb. PIR detektory jsou instalovány v prostorách kanceláří a skladů. U hlavního a vedlejšího vchodu budovy č.1 se nachází ovládací panel. Tyto panely jsou instalovány uvnitř budovy. Pro řízení celého systému je použita ústředna AMOS 1600, která je umístěna v jedné z kanceláří. Tento zabezpečovací systém byl instalován v roce 2004 firmou Systém plus Zlín, s.r.o. Systém EPS byl ve firmě vybudován před pár lety. Objekt je napojen na DPPC firmy Systém plus Zlín. Systém je dle majitele firmy a mého názoru nekompletní. Obvodová a plášťová ochrana objektu zde není řešená vůbec. V prostorové ochraně objektu lze najít nedostatky hlavně v budově č. 1. Vniknutí a pohyb pachatele v některých místnostech je nezjistitelný právě kvůli absenci prostorové ochrany. Kvůli stáří celého systému bude nový zabezpečovací systém realizován z nových komponentů.

**Bezpečnostní prostředí**

Objekt se nachází mezi centrem města a dvěma odlehlejšími částmi města. Centrum města a tyto dvě další části města propojuje jedna pozemní komunikace, která vede hned vedle zabezpečovaného objektu. V okolí objektu se nachází pouze sousedící firma, která má svůj areál střežen zabezpečovacím systémem. Areál sousedící firmy je bez přítomnosti lidí a je navštěvován zaměstnanci v případě rekonstrukcí, oprav, revizních a údržbových prací.

## 5.3 Bezpečnostní posouzení – vnitřní vlivy na PZTS

- **Vodovodní potrubí a vytápění**

Předtím než budeme navrhovat jednotlivé komponenty PZTS, je potřeba brát v úvahu i možné působící vlivy na tyto komponenty. K vytápění budovy č. 1 se využívá voda. Vodovodní potrubí v budově č. 1 je vedeno ve zdech objektu. Budovy č. 2 a č. 3 nejsou žádným způsobem vytápěny a ani zde nejsou udělány rozvody vody.

- **Vzduchotechnické a klimatizační systémy**

Ve všech budovách areálu firmy se nevyužívají žádné vzduchotechnické systémy. V budovách se používá výhradně přirozené větrání. Klimatizační jednotky jsou umístěny pouze v kancelářských prostorech budovy č. 1.

- **Zavěšené předměty**

V budově č. 1 se nachází zavěšené obrazy různé velikosti a vývěsné tabule s papíry připíchnutými rýsovačky. V budovách č.2 a č.3 jsou na zdech zavěšené různé druhy firmou používaného nářadí a elektromateriál.

- **Zdroje světla**

Osvětlení pracoviště přes den ve všech budovách zajištují okna a zářivkové osvětlení. Jelikož se nejbližší veřejné osvětlení nachází přibližně 100 m od zabezpečovaného objektu, firma si naistalovala stožárové lampy po perimetru objektu. Na všech budovách jsou umístěny reflektory, které osvětlují venkovní areál firmy.

- **Elektromagnetické rušení**

V zabezpečovaném objektu a jeho blízkém okolí se nevyskytují žádné zdroje elektromagnetického rušení, které by mohly mít vliv na PZTS.

- **Divoká a domácí zvířata**

V areálu podniku se nepohybují žádná divoká nebo domácí zvířata.

- **Uspořádání předmětů**

Pozornost je třeba věnovat hlavně venkovnímu skladování materiálu, aby nedocházelo k zastínění zorného pole detektorů.

## 5.4 Bezpečnostní posouzení – vnější vlivy na PZTS

V oblasti, kde se zabezpečovaný objekt nachází, nedochází k žádné seismické aktivitě, která by mohla mít za následek sesuv půdy nebo zemětřesení. V budovách č. 1 a č.3 můžou být zaznamenány otřesy a vibrace od těžkých vozidel, které projíždí po komunikaci okolo zabezpečovaného objektu. Zvýšený hluk může být zaznamenán v období, kdy zemědělské stroje obdělávají pole v okolí areálu objektu. Sousedící objekt svým provozem neovlivňuje funkci prvků PZTS zabezpečovaného objektu. Venkovní zařízení je potřeba volit tak, aby byly schopné provozu za příslušných klimatických podmínek.

## 5.5 Stupeň zabezpečení, třída prostředí

Všechny komponenty, které budou použity u PZTS v objektu, musí splňovat stupeň zabezpečení 2, dle normy ČNS EN 50131-1 ed.2. Předpokládá se, že narušitel má omezenou znalost PZTS a používá základní sortiment běžného nářadí a přenosných přístrojů.

Komponenty, které budou umístěny ve venkovních prostorech, musí splňovat třídu prostředí IV. Předpokládá se, že komponenty jsou plně vystaveny povětrnostním vlivům. Rozsah teplot je od -25 °C do +60 °C. Komponenty, které budou umístěny v prostorách budov č. 2 a č. 3, musí splňovat třídu prostředí II. Předpokládají se zde výkyvy teplot. Rozsah teplot je od -10 °C do +40 °C. Komponenty, které budou umístěny v prostorách budovy č. 1, musí splňovat třídu prostředí I. Předpokládá se obvykle stála teplota. Rozsah teplot je od +5 °C do +40 °C.

Rozsah PZTS bude stanoven dle informativní přílohy normy ČSN CLC/TS 50131-7. Je tedy potřeba zabezpečit minimálně obvodové dveře, okna a ostatní otvory (otevření) a místnosti (past – dohled ve vybraných prostorech).

# 6 ANALÝZA BEZPEČNOSTNÍCH RIZIK

V této kapitole bude provedena bezpečnostní analýza rizik firmy. Pro identifikaci rizik, jejich hodnocení a zavedení vhodných opatření bude použita analýza možných způsobů a důsledků poruch v procesu (PFMEA). Po získaní výsledků byly navrženy protiopatření. Na začátku bylo potřeba definovat hrozby, které byly zjištěny dle bezpečnostního posouzení objektu. Dále bylo potřeba definovat jednotlivá aktiva.

Hrozby:

- požár (způsobený technickou závadou nebo vlivem člověka),
- vandalismus (poškození budov, firemních automobilů a oplocení),
- vloupání (v době, kdy je objekt neosídlen),
- krádež (v jednotlivých budovách a venkovním areálu),
- provozní havárie (havárie vodovodního a vytápěcího potrubí).

Aktiva:

- osoby, budovy, vybavení, stroje, nářadí a vozidla.

Vztah mezi jednotlivými aktivy a hrozby je v uveden v Tab. 6. Pokud hrozba souvisí s aktivem, je vztahu přirazena hodnota 1. Pokud hrozba nesouvisí s aktivem, je vztah znázorněn hodnotu 0.

Tab. 6. Vztah hrozeb a aktiv

| **Aktiva** | **Hrozby** | | | | |
|---|---|---|---|---|---|
| | I. Požár | II. Vandalismus | III. Vloupání | IV. Krádež | V. Provozní havárie |
| 1. osoby | **1** | 0 | 0 | 0 | **1** |
| 2. budovy | **1** | **1** | **1** | 0 | **1** |
| 3. vybavení | **1** | **1** | **1** | **1** | **1** |
| 4. stroje a nářadí | **1** | **1** | **1** | 1 | 0 |
| 5. vozidla | **1** | **1** | 0 | 1 | 0 |

### Hodnocení rizik

K hodnocení rizik se používají tři parametry:

- Závažnost dopadu rizika (Z),
- Pravděpodobnost výskytu rizika (P),
- Odhalitelnost rizika (O).

Součinem těchto tří parametrů získáme míru rizika (index RPN – Risk priority number). Čím vyšší je hodnota RPN, tím více se musíme zaobírat daným problémem. Před hodnocením je potřeba stanovit stupnice hodnocení pro všechny tři parametry (viz Tab. 7, Tab. 8, Tab. 9). Rozsahy stupnic jsem si volil dle vlastního uvážení.

Tab. 7. Závažnost dopadu rizika

| Hodnocení | Závažnost dopadu rizika |
|---|---|
| 1 | Žádná |
| 2 | Nevýznamná |
| 3 | Průměrná |
| 4 | Významná |
| 5 | Vážná |

Tab. 8. Pravděpodobnost výskytu problému

| Hodnocení | Pravděpodobnost výskytu rizika |
|---|---|
| 1 | Nepravděpodobná |
| 2 | Mála |
| 3 | Průměrná |
| 4 | Vysoká |
| 5 | Jistá |

Tab. 9. Odhalitelnost problému

| Hodnocení | Odhalitelnost rizika |
|---|---|
| 1 | Jistá |
| 2 | Vysoká |
| 3 | Průměrná |
| 4 | Malá |
| 5 | Nemožná |

Po zjištění hodnot RPN je důležité věnovat pozornost výsledkům, které mají hodnoty RPN vyšší než součin středních hodnot všech tří parametrů. Součin středních hodnot těchto tří parametrů je 27.

Dále bylo potřeba stanovit opatření k jednotlivým hrozbám. Prvky, které tvoří opatření jsou dvojího typu. Jedny prvky zajištují odstranění hrozby (eliminaci) a druhé typy prvku zajištují odhalení probíhající hrozby (identifikaci). V Tab. 10 jsou uvedeny aktuální opatření a navrhované opatření, vůči jednotlivým hrozbám.

Tab. 10. Hrozby – opatření

| Hrozby | Aktuální opatření | Navrhované opatření |
|---|---|---|
| Požár | Hasící přenosné přístroje, EPS | - |
| Vandalismus | MZS, PZS | Rozšíření PZS, CCTV |
| Vloupání | MZS, PZS | Rozšíření PZS, CCTV |
| Krádež | MZS, PZS | Rozšíření PZS, CCTV |
| Provozní havárie | Kontroly, revize | - |

Jako opatření pro snížení míry rizika závažných hrozeb bylo stanoveno:

- Rozšíření PZTS,
  - použití magnetických kontaktů,
  - rozšíření PIR detektorů,
  - použití IR závor.
- použití CCTV.

Výsledky hodnocení rizik jsou uvedeny v Tab. 11. Z tabulky je zřejmé, že je nutné věnovat pozornost hrozbě Krádež a Vloupání. Analýza nám odhalila šest závažných problémů, kterými je potřeba se zaobírat. U těchto závažných problémů bylo zapotřebí stanovit další opatření, které povedou ke snížení hodnot RPN. Po snížení hodnot RPN bude riziko akceptovatelné.

Tab. 11. Hodnocení rizik

| **Hrozba – Aktivum** | **Z** | **P** | **O** | **RPN** |
|---|---|---|---|---|
| Požár – osoby | **5** | **2** | **2** | **20** |
| Požár – budovy | **4** | **2** | **2** | **16** |
| Požár – vybavení | **2** | **2** | **2** | **8** |
| Požár – stroje a nářadí | **2** | **2** | **2** | **8** |
| Požár – vozidla | **2** | **1** | **4** | **8** |
| Vandalismus – budovy | **2** | **2** | **4** | **16** |
| Vandalismus – vybavení | **2** | **1** | **3** | **6** |
| Vandalismus – stroje a nářadí | **2** | **1** | **3** | **6** |
| Vandalismus – vozidla | **2** | **2** | **4** | **16** |
| Vloupání – budovy | **3** | **4** | **3** | **36** |
| Vloupání – vybavení | **3** | **4** | **3** | **36** |
| Vloupání – stroje a nářadí | **3** | **4** | **3** | **36** |
| Krádež – vybavení | **4** | **4** | **3** | **48** |
| Krádež – stroje a nářadí | **4** | **4** | **3** | **48** |
| Krádež – vozidla | **4** | **3** | **4** | **48** |
| Provozní havárie – osoby | **3** | **1** | **3** | **9** |
| Provozní havárie – budovy | **2** | **1** | **3** | **6** |
| Provozní havárie – vybavení | **3** | **1** | **3** | **9** |

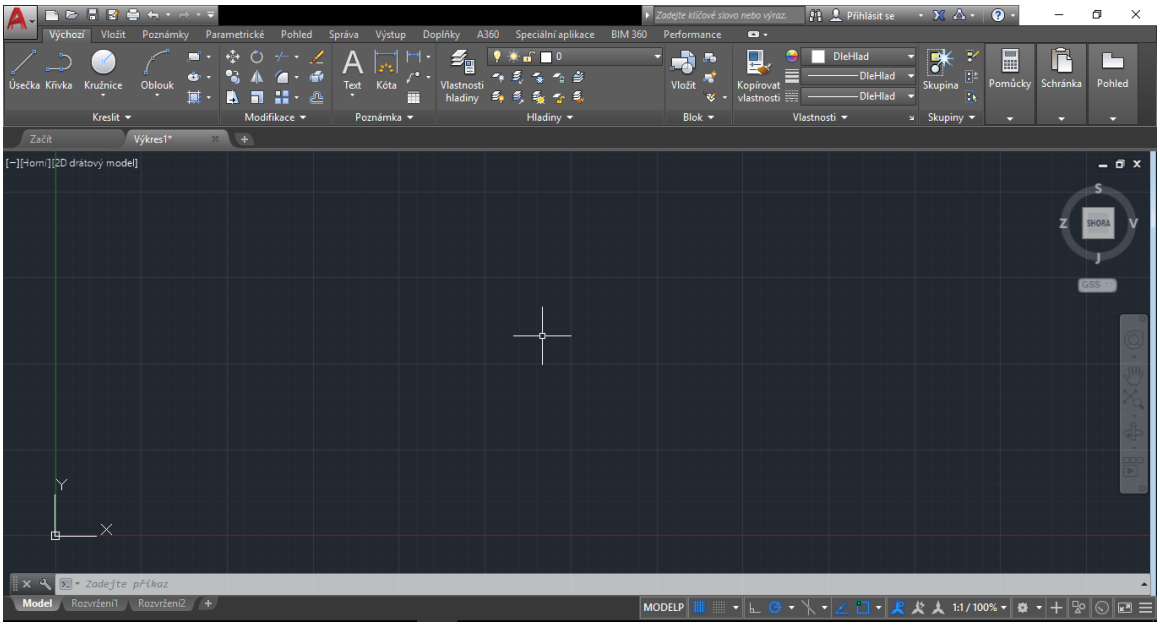
# 7 NÁVRH ZABEZPEČENÍ OBJEKTU – VERZE I

Na základě bezpečnostního posouzení daného objektu a výstupů získaných z bezpečnostní analýzy rizik vyplývá, že je potřeba se zaměřit na instalaci PZS. Dalšími aspekty, které je potřeba zahrnout do návrhu zabezpečení objektu, jsou požadavky dané firmy. Z tohoto důvodu byla první verze zabezpečení objektu vytvořena s ohledem na finanční prostředky firmy.

## 7.1 Půdorysy budov

Pro vytvoření půdorysů budov mně byly zapůjčeny stavební dokumentace všech budov firmy. Tyto výkresy se využijí pro získaní přehledu o rozlohách budov a rozmístění místností. K vytvoření všech výkresů jsem využil modelovací nástroj AutoCAD 2017. S tímto programem jsem se předtím nikdy nesetkal. Třicetidenní zkušební verze tohoto programu mi stačila nato, abych se s tímto programem dostatečně obeznámil a výkresy vytvořil.

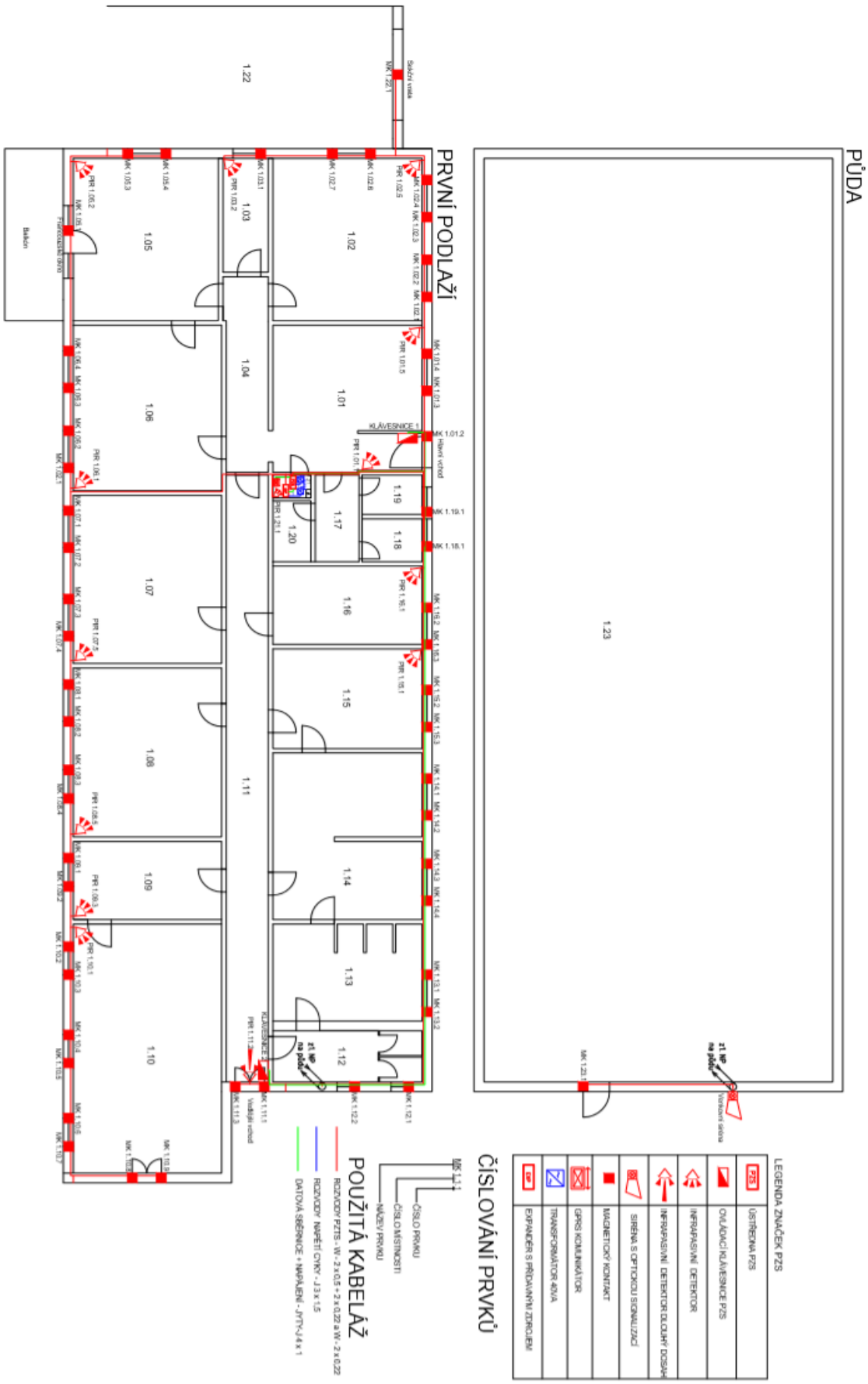
- Software AutoCAD – Tento modelovací nástroj vyvinula firma Autodesk. Je využíván pro 2D a 3D modelování a konstruování. Užívá se po celém světě např. ve strojírenství, stavebnictví apod. Program obsahuje nástroje, které usnadňují vytváření technických výkresů. Ukázka prostředí AutoCAD 2017 je na Obr. 16



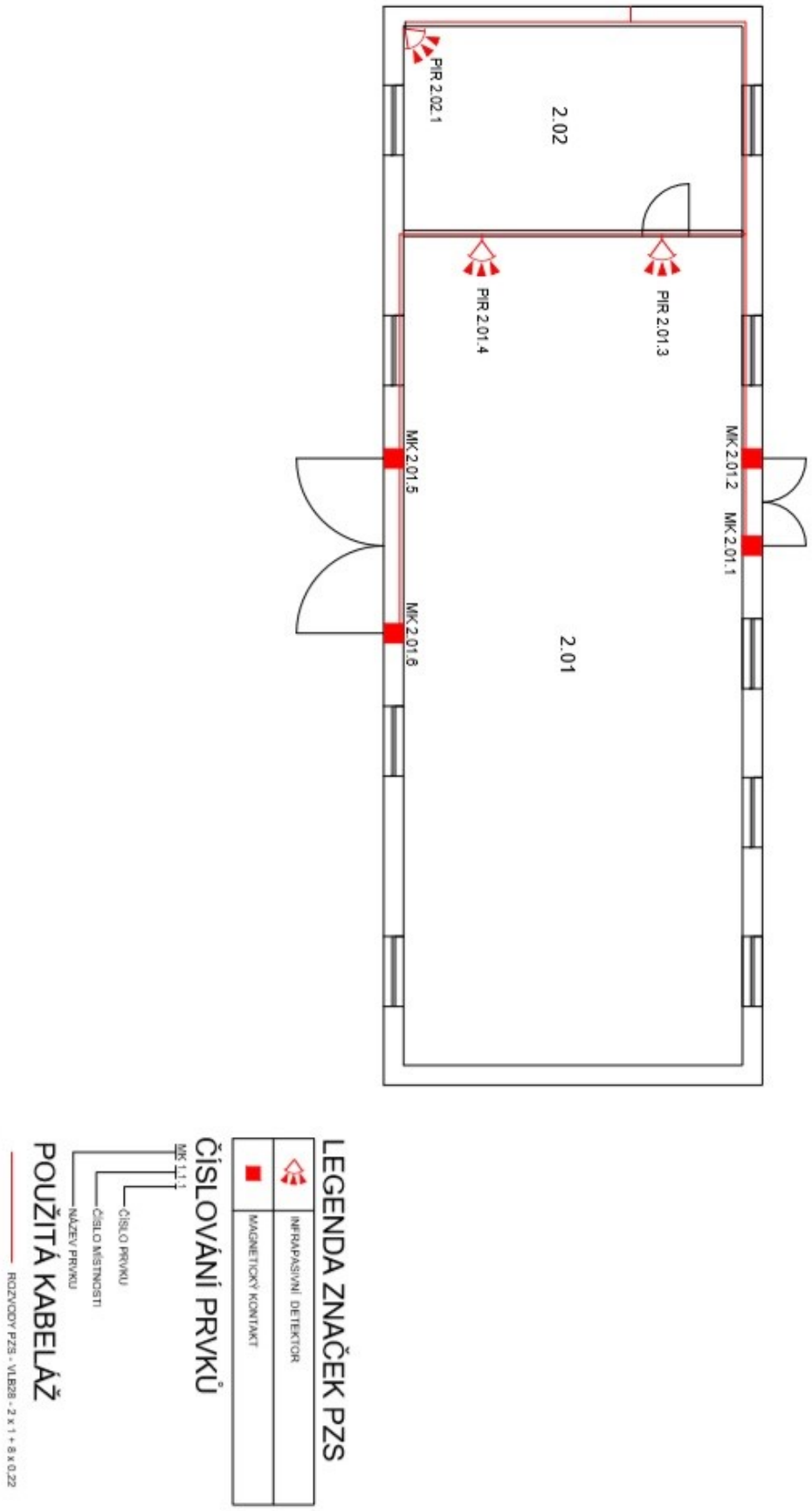

Obr. 16. AutoCAD 2017 – Hlavní okno

AutoCAD umožnuje použít knihovnu se značkami komponentů PZTS. Tyto značky se shodují se značkami pro projektování, které jsou uvedeny v normě TNI 33 4591-1. AutoCAD tedy umožnuje kompletní náhled na půdorysy budov s rozmístěním komponentů PZTS a jejich propojením. Pokud je výkres kreslen v určitém měřítku, je možné zjistit i přibližnou délku kabeláže.

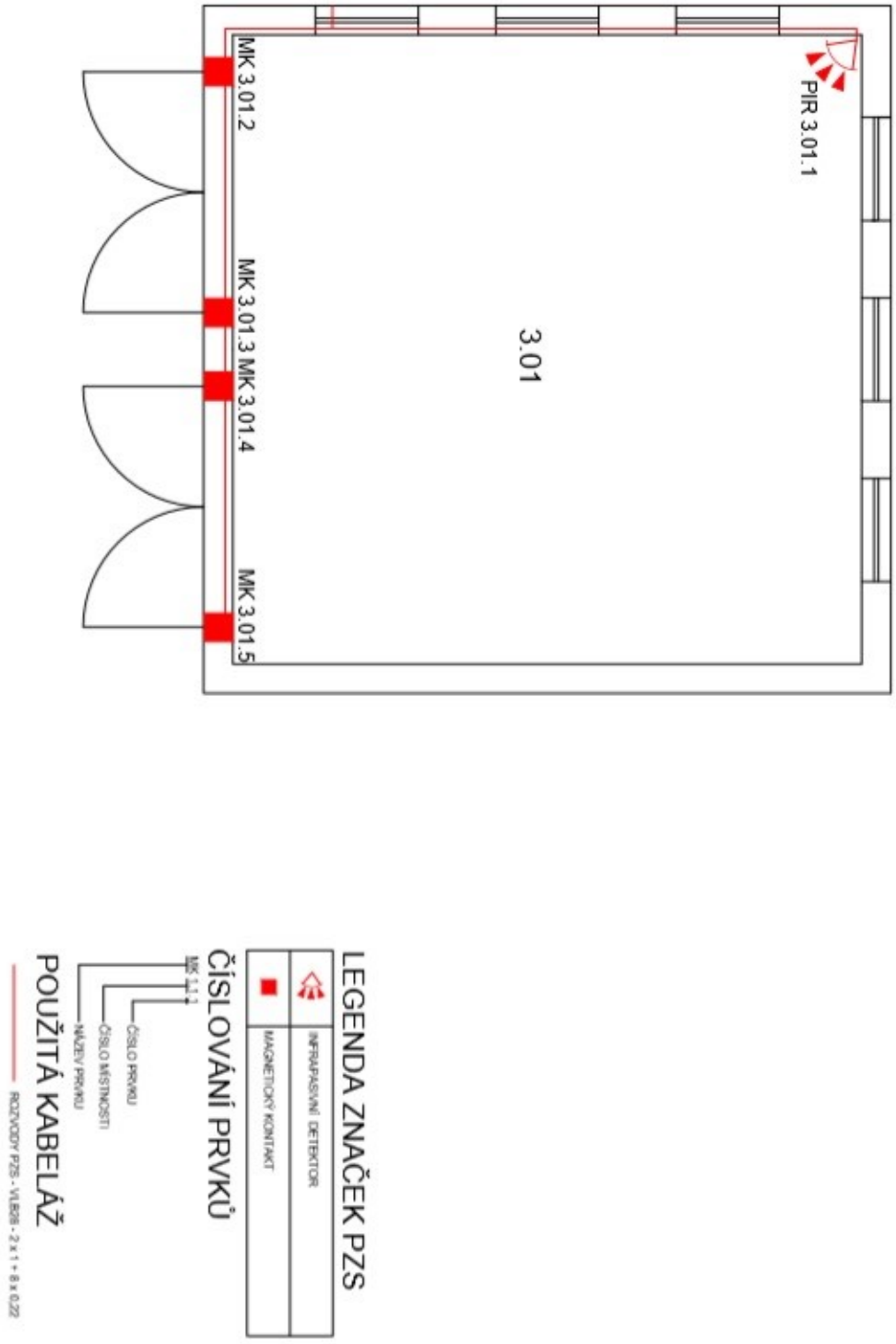
Rozmístění komponentů PZS a jejich propojení je uvedeno na Obr. 17 až Obr. 20. Aby bylo možné výkresy vložit do diplomové práce, bylo potřeba výkresy zmenšit a ořezat. Veškerá výkresová dokumentace v plné velikosti je uložena v přílohách na přiloženém CD. V příloze jsou vloženy výkresy podlaží všech tří budov a výkres areálu firmy. Celkem tedy čtyři výkresy. Všechny výkresy jsou ve formátu PDF a DWG.



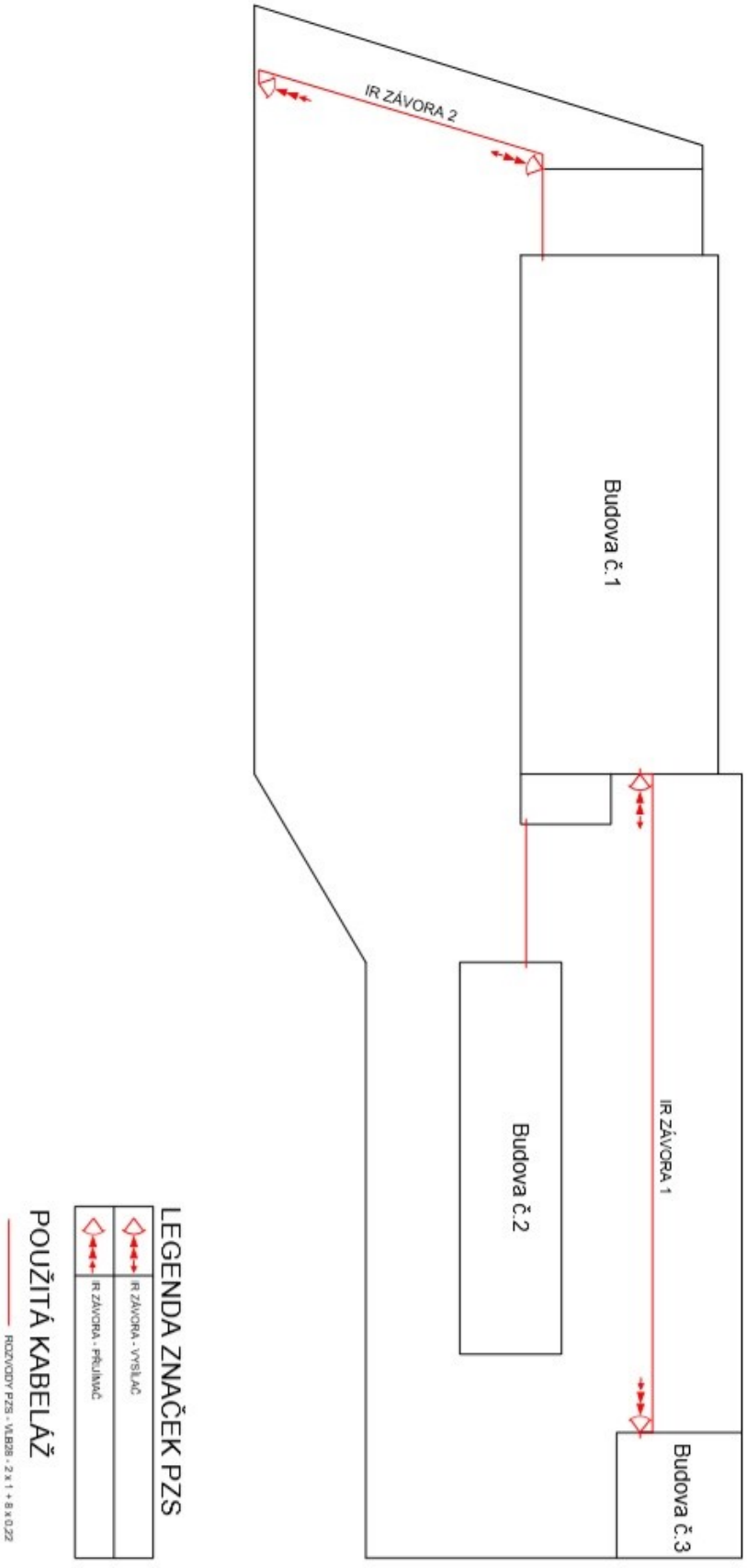

Obr. 17. Rozmístění zařízení – budova č.1




Obr. 18. Rozmístění zařízení – budova č.2




Obr. 19. Rozmístění zařízení – budova č.3




Obr. 20. Rozmístění zařízení – venkovní areál

## 7.2 Poplachový zabezpečovací a tísňový systém

Pro vhodný výběr komponentu PZTS jsem kontaktoval firmu SYSTEM Plus Zlín s. r.o., která má dlouholeté zkušeností s dodávkami zabezpečovací techniky. Bylo mi oznámeno, že pro elektronické zabezpečení objektů využívají komponenty od výrobců PARADOX, DSC, SIEMENS aj. Doporučení směrovalo na využití právě komponentů od výrobce PARADOX. Odpadají zde problémy s kompatibilitou jednotlivých komponentů a poměr cena / výkon je zde velmi slušná. Velkou výhodou je i dostupnost všech dokumentací komponentů. Proto jsem se rozhodl produkty od tohoto výrobce použít v obou verzích návrhu.

**Ústředna PZTS**

- Smíšená ústředna Spectra SP7000.

Tato ústředna je vhodná pro malé až střední aplikace. Počet zón na desce ústředny je 16. K ústředně lze připojit expandéry pomocí sběrnice. Počet vstupů na expandéru je 8. Ústředna umožnuje využití i bezdrátových zón.

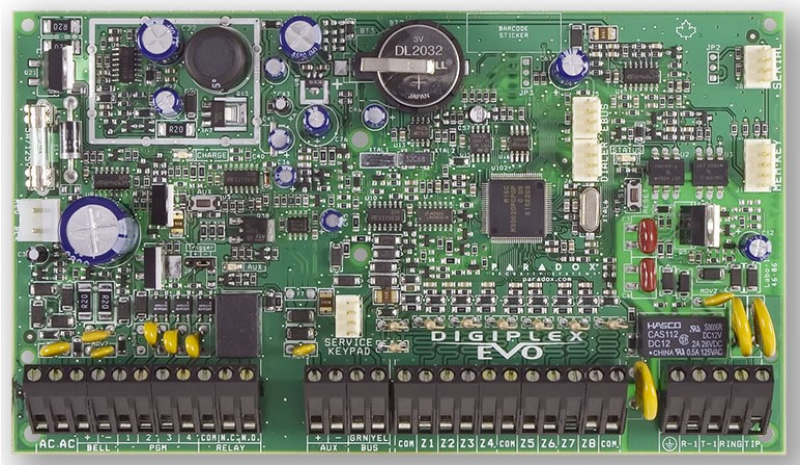

Obr. 21. Ústředna Spectra SP7000 [20]

Tab. 12. Technické parametry ústředny SP7000

| | |
|---|---|
| Celkový počet zón v systému | 32 |
| Počet uživatelských kódů | 32 |
| Proudový odběr ústředny | 100 mA |
| Maximální proudový odběr z výstupu | 1 A |
| Stupeň zabezpečení | 2 |

- Ústředna Digiplex Evo 192.

Tato ústředna je vhodná pro střední a velké objekty. Počet zón na desce ústředny je 8. K ústředně lze připojit expandéry pomocí sběrnice. Lze připojit expandéry s 1, 4, 8, 16 nebo 32 vstupy. Ústředna umožňuje využití i bezdrátových zón.




Obr. 22. Ústředna Evo 192 [20]

Tab. 13. Technické parametry ústředny Evo 192

| | |
|---|---|
| Celkový počet zón v systému | 192 |
| Počet uživatelských kódů | 999 |
| Proudový odběr ústředny | 100 mA |
| Maximální proudový odběr z výstupu | 1 A |
| Stupeň zabezpečení | 3 |

- Výběr ústředny

Pro svůj návrh zabezpečení objektu jsem vybral prvně ústřednu Spectra SP7000. V průběhu vypracování návrhu jsem zjistil, že objekt bude rozdělen minimálně do 27 zón. Dvacet sedm zón lze u ústředny Spectra SP7000 realizovat připojením dvou osmi zónových expandérů. Zůstalo by pouze pět volných zón a nebylo by v budoucnu možné větší rozšiřování daného systému. Z toho důvodu jsem raději zvolil ústřednu Digiplex Evo 192, ke které je možné připojit expandér s 32 vstupy.

Výhody použití ústředny Digiplex Evo 192 oproti Spectra SP7000:

- větší počet volných zón,
- menší možnost poruchy (menší počet zařízení),

- možnost dalšího rozšíření systému (až 192 zón).

Ústředna je uložena v úklidové místnosti a je ji možné ovládat pomocí dvou klávesnic, umístěných u hlavního a vedlejšího vchodu budovy č. 1. Je uložena v plechovém boxu dohromady se záložním akumulátorem a napájecím transformátorem 40VA.

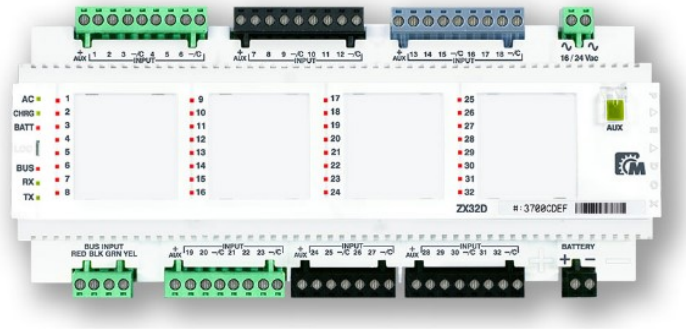
**Záložní akumulátor**

Jsou zvoleny bezúdržbové akumulátory s napětím 12 V a kapacitou 18 Ah. Pro záložní napájení systému by mohli být použity akumulátory o kapacitě 12 Ah. Bohužel tyto akumulátory mají větší hloubku než boxy, do kterých mají být umístěny. Z tohoto důvodu jsou zvoleny akumulátory o kapacitě 18 Ah, které do boxu lze umístit. Cenový rozdíl je zanedbatelný.


Obr. 23. Záložní baterie 12 V/18 Ah [20]

**Expandér**

Objekt je rozdělen do 27 zón. Expandéry jsou voleny tak, aby jich bylo co nejmíň. Expandéry mohou být 1, 4, 8, 16 nebo 32 vstupové. Byl vybrán expandér Paradox ZX32D. Tento expandér se připojuje na BUS sběrnici ústředny. Obsahuje 32 vstupů a pokryje tedy počet požadovaných zón. Oproti ostatním expandérům, tento expandér obsahuje vnitřní spínaný zdroj. Proudový odběr z výstupu AUX expandéru může být 1 A a dobíjecí proud záložního akumulátoru je 850 mA. Transformátor a záložní akumulátor je tedy připojen přímo k expandéru.




Obr. 24. Expandér Paradox ZX32D [20]

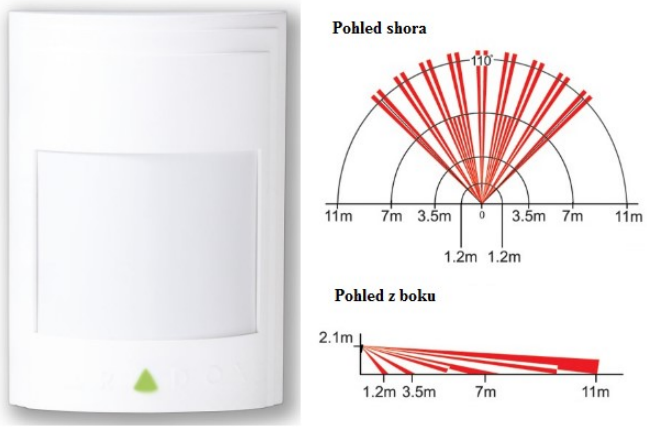
**Komunikátor**

Pro přenos informací na DPPC je zvolen GPRS komunikátor PCS250G. Ten umožnuje posílání SMS zpráv s identifikací poplachů, zprávy o vypnutí, zapnutí, obnovy systému PZTS a poruchy. Modul umožňuje připojit dvě SIM karty.

Obr. 25. Komunikátor PCS250G [20]

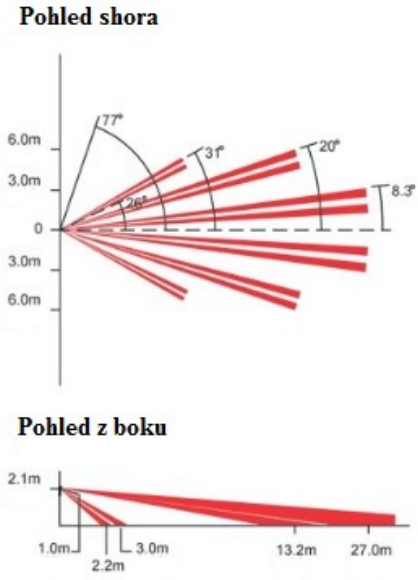
**PIR detektory**

Pro střežení vnitřních prostor objektů je použit analogový PIR detektor PARADOX PRO PLUS 476. Detektor lze umístit na zeď i do rohu. Maximální detekční dosah detektoru je 11 m. Detekční charakteristika je zobrazena na Obr. 26. Výhodu těchto detektorů je vyměnitelná čočka. Je možné měnit detekční charakteristiku detektoru dle volby čočky.




Obr. 26. PIR detektor PARADOX PRO PLUS 476 [20]

V budově č. 1 je dlouhá chodba a je zde nutné použít čočku LR–2, která má detekční dosah 27 m. Detekční charakteristika je zobrazena na Obr. 27.




Obr. 27. Čočka LR – 2 [20]

**Magnetický kontakt**

Na okna a dveře jsou naistalovány povrchové magnetické kontakty SM-50 T. Tyto magnetické kontakty jsou čtyř drátové a obsahují temper. Magnetický kontakt se připevňuje pomoci samořezných šroubů. Pro sekční vrata je použit polarizovaný magnetický kontakt MASS-303, který je určen pro venkovní prostředí, kde se teploty pohybuji od -40 °C až do 70 °C. Teplota v této garáži je stejná jako teplota venkovní.

Obr. 28. Magnetický kontakt
SM-50 T [20]

Obr. 29. Magnetický kontakt MASS-303 [20]

**IR závory**

Pro zabezpečení perimetru objektu jsem vybral paprskové infrazávory od firmy VAR-TEC. Stupeň krytí je 54 (IP54). Skládají se z optického vysílače a přijímače. Infrazávory lze koupit s dosahem 40, 60 nebo 150 m. V návrhu je využita jedna infrazávora s dosahem 40 m a druhá s dosahem 60 m. Zvažoval jsem, že pro svůj návrh vyberu infrazávory od známější firmy OPTEX. Avšak cena infrazávor OPTEX je skoro dvojnásobná.

Obr. 30. Infrazávory VAR-TEC [20]

**Venkovní siréna**

Na budově č. 1 je umístěna zálohová venkovní siréna BELL-TEC MINI s optickou a akustickou signalizací. Zálohování je realizováno záložním akumulátorem, který je uvnitř sirény. Siréna obsahuje temper (detekci otevření sirény a detekci sejmutí ze zdi). Stupeň krytí je 54 (IP54), tzn. siréna může být vystavěna přímému dešti.

Obr. 31. Siréna BELL-TEC MINI [20]

**Klávesnice**

Klávesnice PARADOX – K641+ slouží k ovládání a zobrazování informací o stavu ústředny DIGIPLEX. Klávesnice obsahuje dvouřádkový display a ovládá se pomocí tlačítek.


Obr. 32. Klávesnice PARADOX – K641+ [20]

**Použité zařízení**

Tab. 14. Rozmístění komponentů a jejich počet

| Komponenty | Typ | Budova | | | Venkovní Areál | Počet |
|---|---|---|---|---|---|---|
| | | č.1 | č.2 | č.3 | | |
| Ústředna | Paradox – EVO 192 | 1 | | | | 1 |
| Expandér | Paradox ZX32D | 1 | | | | 1 |
| Komunikátor | PCS250G – GPRS | 1 | | | | 1 |
| Klávesnice | Paradox – K641+ | 2 | | | | 2 |
| PIR detektor | Paradox PRO Plus 476 | 14 | 3 | 1 | | 18 |
| Magnetický kontakt | MS – 50T | 55 | 4 | 2 | | 61 |
| Magnetický kontakt | MASS – 303 | 1 | | | | 1 |
| Venkovní siréna | Bell – tec MINI | | | | 1 | 1 |
| IR závora | Var – tec PB-40DC | | | | 1 | 1 |
| IR závora | Var – tec PB-60DC | | | | 1 | 1 |
| Transformátor | Trafo kryté 40VA | 2 | | | | 2 |
| **Celkem** | | | | | | **90** |

- **Plášťová ochrana**

Plášťová ochrana je zajištěna pomocí magnetických kontaktů SM – 50T. V budově č. 1 jsou ve všech otvorových výplní umístěny magnetickými kontakty. Sekční vrata v garáži jsou osazena magnetickým kontaktem MASS – 303 z důvodu klimatických podmínek. V budově č. 2 a č. 3 jsou neotevíratelné okna. Z toho důvodu jsou magnetické kontakty umístěny pouze na dveře.

- **Prostorová ochrana**

Plášťová ochrana je zajištěna pomocí analogových PIR detektorů PRO plus 476. Ty jsou osazeny základní čočkou s dosahem 11 m. Ve většině případů je tato čočka dostatečná. U PIR detektoru, který je umístěn v místností 1.11 (chodba), je vyměněna základní čočka za čočku LR- 2, které má dosah 27 m. Detektory jsou rozmístěny tak, aby nedocházelo k zastínění zorných polí detektorů.

- **Obvodová ochrana**

Obvodová ochrana je zajištěna pomoci infrazávor VAR-TEC PB-40DC a VAR-TEC PB-60DC. Infrazávory jsou umístěny na místa, kde je největší předpoklad vniknutí pachatele do areálu firmy. V minulosti došlo k vloupání do objektu už třikrát. Pachatel s největší pravděpodobností vniknul do areálu právě přes dřevěný plot ze severní strany nebo přes drátěný plot z výhodní strany. Na jižní a západní straně areálu firmy se nachází drátěné oplocení, které odděluje areál sousední firmy od areálu uvedené firmy. Tato firma má svůj zabezpečovací systém. Při obhlídce okolí jsem zjistil, že využívají i CCTV. Nepředpokládám tedy, že by došlo k vloupání pachatele do areálu firmy z těchto stran.

- **Klávesnice**

K ovládaní a nastavení systému slouží dvě klávesnice K641+ od výrobce Paradox. Jsou umístěny u hlavního a vedlejšího vchodu budovy č.1 tak, aby nebyly vidět z venku. Nachází se v místností 1.01 a 1.11.

- **Kabeláž**

Sběrnice je tvořena kabelem JYTY – J 4 x 1.Tímto kabelem jsou propojeny ústředna s klávesnicemi, GPRS komunikátorem a expandérem. Pro připojení transformátoru k rozvodu síťového napětí 230 V / 50 Hz a ústředně jsou použity kabely CYKY-J 3 x 1,5. Pro zapojení detektorů k ústředně a expandéru jsem se rozhodl využít smyčkový systém. Jedna zóna odpovídá jedné smyčce NC. Je tím snížen počet expandérů a délka kabeláže v systému. Jedinou nevýhodou je, že při vyhlášení oplachu na zóně nejde poznat, který detektor sepnul smyčku. Zóny jsou ale rozděleny podle místností a v případě poplachu jde vidět, ve které místnosti byl vyhlášen poplach. Pro připojení detektorů v budově č.1 jsou použity kabely W–2 x 0,5 + 2 x 0,22 a W-2 x 0,22. Pro připojení všech detektorů, které se nachází mimo budovu č. 1, byl použit venkovní kabel VLB28 - 2 x 1 + 8 x 0,22.

Tento kabel, mimo budovy, je veden pod betonovými panely, které tvoří areál firmy. Délky a ceny kabeláží jsou uvedeny v Tab. 15.

Tab. 15. Soupis kabeláže

| Typ | Délka [m] | Cena |
|---|---|---|
| JYTY – J 4 x 1 | 80 | 880 Kč |
| CYKY-J 3 x 1,5 | 10 | 110 Kč |
| W-2 x 0,22+2 x 0,5 | 400 | 4 000 Kč |
| W-2 x 0,22 | 400 | 2 000 Kč |
| VLB28 - 2 x 1 + 8 x 0,22 | 650 | 14950 Kč |

- **Zóny**

Jedná se o menší firmu, proto není potřeba rozdělovat systém na podsystémy. Systém bude rozdělen do 27 zón. Je použit jeden třiceti dvou zónový expandér s vnitřním spínaným zdrojem. Rozdělení zón viz. Příloha II.

- **Napájení**

Ústředna je napájená transformátorem 40VA s výstupní proudem 2 A. Transformátor je napojen na přívod síťového napětí 230 V / 50 Hz. Maximální proudový odběr systému je větší než proud, který je schopný dodat transformátor do systému. Proto byl vybrán expandér s vnitřním spínaným zdrojem, který je schopný poskytnout výstupní napětí 1 A. Maximální proudový odběr z AUX výstupu ústředny i vnitřního spínaného zdroje expandéru je 1 A (celkem tedy 2 A). Odběr systému je uveden v Tab. 16. Hodnoty byly převzaty s dokumentací jednotlivých komponentů.

Tab. 16. Odběr systému

| Komponenty | Typ | Počet | Klid. odběr [mA] | Max. odběr [mA] |
|---|---|---|---|---|
| Ústředna | Paradox – EVO 192 | 1 | 100 | 100 |
| Expandér | Paradox ZX32D | 1 | 160 | 160 |
| Komunikátor | PCS250G – GPRS | 1 | 100 | 450 |
| Klávesnice | Paradox – K32LCD+ | 2 | 90 | 250 |
| PIR detektor | Paradox PRO Plus 476 | 18 | 270 | 486 |
| Venkovní siréna | Bell-tec Mini | 1 | 0 | 350 |
| IR závora | Var-tec PB-40DC | 1 | 50 | 50 |
| IR závora | Var-tec PB-60DC | 1 | 90 | 90 |
| **Proudový odběr všech komponentů** | | | **860** | **1936** |
| Dobíjecí proud záložního akumulátoru | | | | 700 |
| **Celkem** | | | | **2636** |

Ústředna a komponenty k ní připojené (viz. Tab. 17) mají maximální proudový odběr 1285 mA. K tomu je nutné připočítat dobíjecí proud záložního akumulátoru 700 mA. Celkový maximální proudový odběr je tedy 1985 mA. Výstupní proud transformátoru je 2 A. Z toho vyplývá, že transformátor je schopný zajistit požadovaný celkový maximální odběr ústředny a komponentů k ní připojené.

Tab. 17. Odběr ústředny

| Komponenty | Typ | Počet | Klid. odběr [mA] | Max. odběr [mA] |
|---|---|---|---|---|
| Ústředna | Paradox – EVO 192 | 1 | 100 | 100 |
| Komunikátor | PCS250G – GPRS | 1 | 100 | 450 |
| Klávesnice | Paradox – K32LCD+ | 2 | 90 | 250 |
| PIR detektor | Paradox PRO Plus 476 | 5 | 75 | 135 |
| Venkovní siréna | Bell-tec Mini | 1 | 0 | 350 |
| **Celkem** | | | **365** | **1285** |

Vnitřní zdroj expandéru napájí expandér s připojenými komponenty a případně dobíjí záložní akumulátor. Vnitřní zdroj expandéru zajišťuje dostatečné napájení všech komponentů na něj připojených. Odběry těchto komponentů jsou uvedeny v Tab. 18.

Tab. 18. Odběr expandéru s připojenými komponenty

| **Komponenty** | **Typ** | **Počet** | **Klid. odběr [mA]** | **Max. odběr [mA]** |
|---|---|---|---|---|
| PIR detektor | Paradox PRO Plus 476 | 13 | 195 | 351 |
| IR závora | Var-tec PB-40DC | 1 | 50 | 50 |
| IR závora | Var-tec PB-60DC | 1 | 90 | 90 |
| Expandér | Paradox ZX32D | 1 | 160 | 160 |
| **Celkem** | | | **495** | **651** |

**Výpočet kapacity akumulátoru**

Pokud dojde k výpadku primárního napájení, je zapotřebí zajistit funkčnost celého systému záložním akumulátorem po dobu 12hodin. Maximální doba dobití záložního akumulátoru je 72hodin. Kapacity záložního akumulátoru se vypočítá dle vztahu:

$$KNZ = l_M \times T\ [Ah] \tag{23}$$

kde: KNZ – kapacita záložního akumulátoru [Ah],

$I_m$ – maximální odebíraný proud [A],

T – doba provozu na náhradní zdroj [h].

Výpočet kapacity záložních akumulátorů:

- ústředna

$KNZ = 1{,}285 \times 12 = 15{,}42\ Ah$

- vnitřní zdroj expandéru

$KNZ = 0{,}651 \times 12 = 7{,}81\ Ah$

Pro záložní napájení ústředny byl použit akumulátor o kapacitě 18Ah. Pro záložní napájení expandérů s připojenými komponenty by postačil akumulátor o kapacitě 12Ah, ale z důvodu vhodnějších rozměrů a zanedbatelnému cenovému rozdílu, byl použit akumulátor o kapacitě 18Ah.

**Úbytek napětí na vedení**

Výrobce udává, že napětí na vedení nesmí klesnout pod 11 V, kvůli zajištění funkčnosti komponentů. Při výpočtu úbytku napětí je potřeba počítat s napětím záložního akumulátoru, které je 12 V. Úbytek napětí na vedení nesmí být tedy větší než 1 V. Pro stanovení úbytku napětí je nutné zjistit typ kabelu (průřez), délku kabelu a proudové odběry veškerých

komponentů v systému. Kabeláž, o průřezu 0,5 $mm^2$, má odpor páru 0,08 Ω / m. Podle Ohmova zákona se pak vypočítá úbytek napětí na jednotlivých komponentech:

$$U = R \times l \times I \; [V] \tag{24}$$

kde: U – úbytek napětí na vedení [V],

I – maximální odebíraný proud [A],

l – délka kabelu [m].

Příklad výpočtu úbytku napětí na nejvzdálenějším prvku:

$U = 0{,}08 \times 92 \times 0{,}027 = 0{,}198 \; [V]$

Vypočítaný úbytek napětí musíme odečíst od napětí zdroje (12 V):

$U = 12 - 0{,}198 = 11{,}801 \; [V]$

Napětí neklesne pod minimální hodnotu 11 V, a tak by detektor měl fungovat správně.

- **Umístění komponentů v boxech**

Tab. 19. Umístění komponentu v boxech

| **Box** | **Komponenty** | **Tamper – zóna** |
|---|---|---|
| Box S 1 | Ústředna, akumulátor, transformátor | 8 |
| Box S2 | Expandér, akumulátor, transformátor | 40 |

- **Cenová kalkulace**

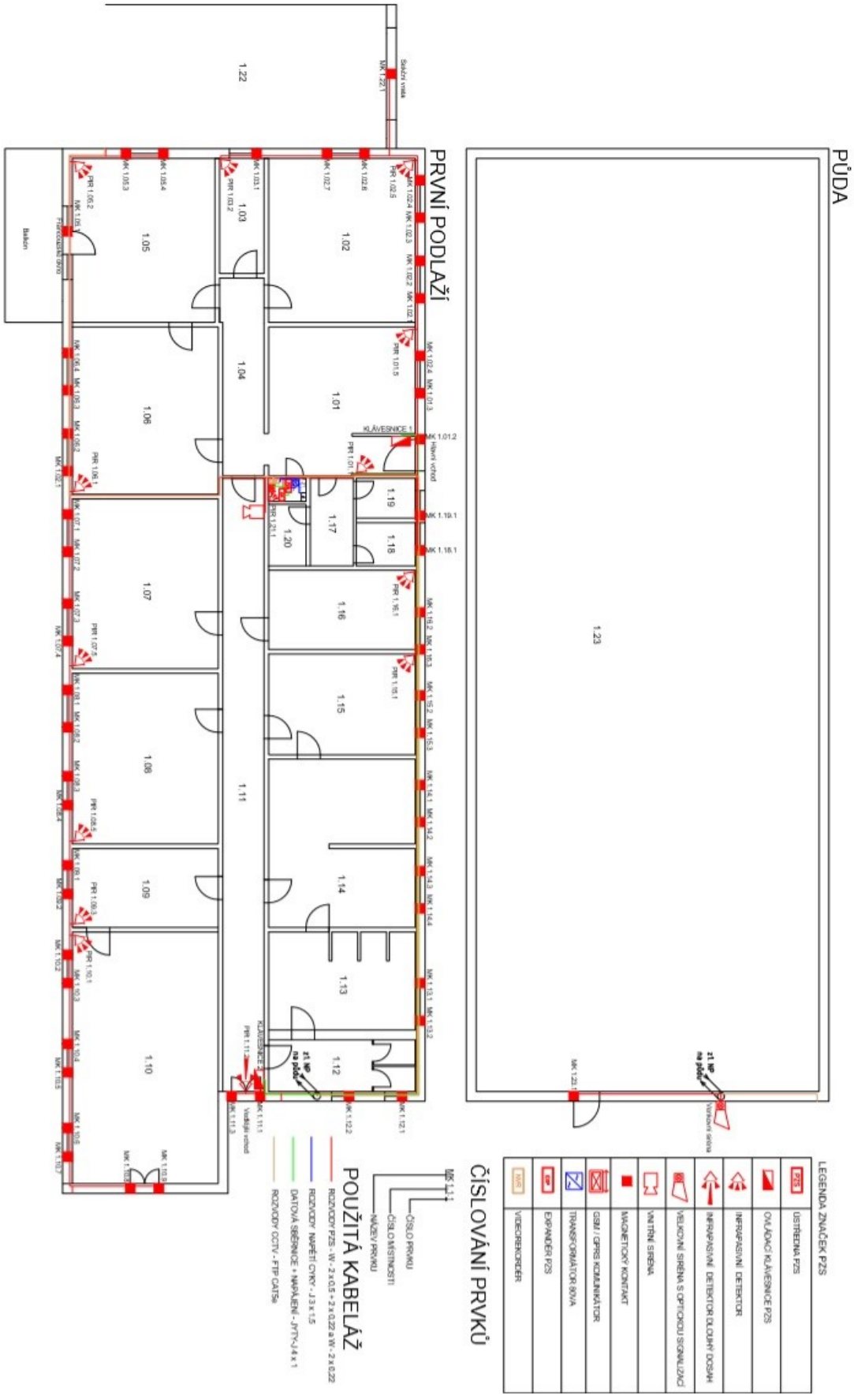
Komponenty pro zabezpečení objektu byly vybrány hlavně od výrobce Paradox. Komponenty od jiných výrobců jsou kompatibilní s výrobky Paradox. Délka kabeláže zahrnuje rezervu, pro případné překážky a nespecifikované prostory, které jsou zjištěny až při instalaci. Do cenového rozpočtu nejsou zahrnuty ceny šroubů, plastové trubky a další instalační materiál.

Tab. 20. Soupis všech komponentů a jejich cena

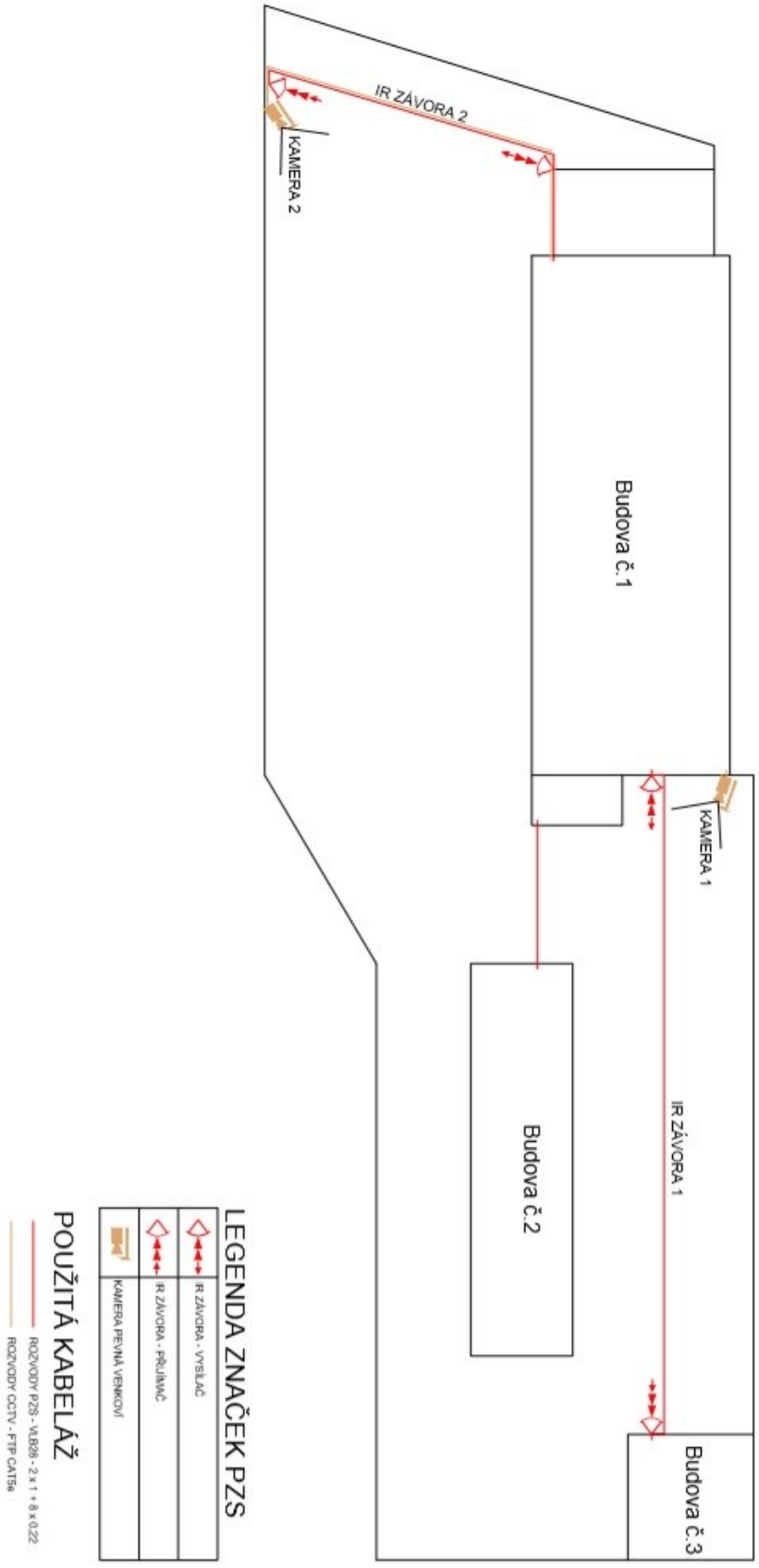
| Komponenty | Typ | Počet | Cena za kus | Celková cena s DPH |
|---|---|---|---|---|
| Ústředna Spectra | Paradox – EVO 192 | 1 | 3 534 Kč | 3 534 Kč |
| Expandér | Paradox ZX32D | 1 | 6 480 Kč | 6 480 Kč |
| Komunikátor | PCS250G – GPRS | 1 | 4 700 Kč | 4 700 Kč |
| Klávesnice | Paradox – K641+ | 2 | 3 915 Kč | 7 830 Kč |
| PIR detektor | Paradox PRO Plus 476 | 18 | 362 Kč | 6 516 Kč |
| Magnetický kontakt | MS – 50T | 61 | 94 Kč | 5 734 Kč |
| Magnetický kontakt | MASS - 303 | 1 | 380 Kč | 380 Kč |
| Venkovní siréna | Bell-tec Mini | 1 | 990 Kč | 990 Kč |
| IR závora | Var-tec PB-40DC | 1 | 2 540 Kč | 2 540 Kč |
| IR závora | Var-tec PB-60DC | 1 | 3 090 Kč | 3 090 Kč |
| Transformátor | trafo kryté 40VA | 2 | 435 Kč | 870 Kč |
| Box | Box S | 2 | 556 Kč | 1 112 Kč |
| Čočka | LR-2 | 1 | 169 Kč | 169 Kč |
| Mechanický zámek | pro Box S | 2 | 133 Kč | 266 Kč |
| Záložní akumulátor | Smart SM18,0 | 2 | 1 609 Kč | 3 218 Kč |
| Kabeláž | | | | 21 940 Kč |
| **Celkem** | | | | **69 370 Kč** |

# 8 NÁVRH ZABEZPEČENÍ OBJEKTU – VERZE II

Druhá verze zabezpečení je vhodným doplněním a úpravou první verze návrhu. Prioritně vychází z mých poznatků a zkušeností získaných během studia uvedeného oboru, kdežto první verze je ovlivněna mimo jiné i požadavky dané firmy. Některé komponenty z první verze zabezpečení objektu jsou použity ve této verzi zabezpečení, a tak nebudou znovu popisovány. Výkresy s rozmístěním jednotlivých zařízení a jejich propojení jsou uvedeny níže. Výkresy budov č.2 a č.3 jsou shodné v obou verzích zabezpečení, a proto zde nebudou znovu uvedeny. Veškerá výkresová dokumentace v plné velikosti je uložena v přílohách na přiloženém CD.



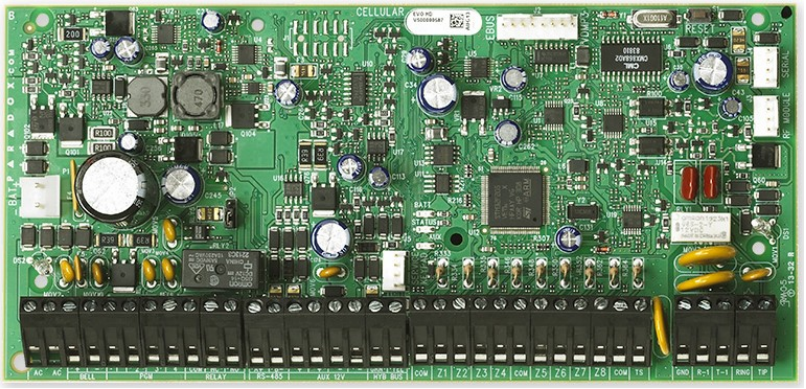

Obr. 33. Rozmístění zařízení – budova č.1




Obr. 34. Rozmístění zařízení – venkovní areál

## 8.1 Poplachový a zabezpečovací systém.

Ústředna Paradox Evo HD tvoří základ v systému. Tato ústředna, stejně jako ústředna Evo 192, je určena pro střední a velké objekty. Maximální počet zón je 192. Ústředna Evo HD disponuje lepšími technickými parametry. Maximální proudový odběr z výstupu AUX je 2 A. Oproti ústředně Evo 192 je to o 1 A více. Dobíjecí proud záložního akumulátoru je taktéž dvojnásobný (1,5 A). Už dle technických parametrů lze vidět, že ústředna má daleko větší maximální proudový odběr, a proto je zapotřebí výkonnější transformátor a záložní akumulátor o větší kapacitě. Pro napájení ústředny je použit transformátor 80VA. Ústředna bude uložena v úklidové místnosti (místnost 1.21) a bude ji možné ovládat pomocí dvou klávesnic, umístěných u hlavního a vedlejšího vchodu budovy č. 1. Bude uložena v plechovém boxu dohromady s transformátorem.



Obr. 35. PARADOX EVO HD [20]

Tab. 21. Technické parametry ústředny Evo HD

| Technické parametry ústředny: | |
|---|---|
| Celkový počet zón v systému | 192 |
| Počet uživatelských kódů | 999 |
| Proudový odběr ústředny | 100 mA |
| Maximální proudový odběr z výstupu | 1 A |
| Stupeň zabezpečení | 3 |

### Záložní akumulátor

Pro záložní napájení ústředny je vybrán akumulátor 12 V o kapacitě 40Ah. Nevýhodou tohoto akumulátorů jsou jejich rozměry. Baterie je příliš velká, aby se vlezla do boxu pro ústřednu. Baterie musí být umístěna v samostatném boxu, který je přímo pro tuto baterii určen. Box obsahuje sabotážní kontakt. Tento box bude umístěn hned vedle boxu s ústřednou a transformátorem.


Obr. 36. Záložní baterie 12 V/40 Ah [20]

### Venkovní a vnitřní siréna

Venkovní siréna je použita stejná jako v první verzi zabezpečení. Oproti ostatním sirénám má sice menší akustický výkon, ale kompenzací je pak nižší proudový odběr, nižší cena. Do budovy č. 1 je umístěna siréna BELL-TEC SIREN. Bude umístěna v místnosti 1.11. Jedná se o nezálohovanou magnetodynamickou sirénu, určenou do vnitřního i venkovního prostředí. Stupeň krytí je 33 (IP33). Obě sirény jsou napájené z ústředny, přes výstup BELL, který má maximální proudový odběr 2 A.


Obr. 37. Siréna BELL-TEC

SIREN [20]

**Klávesnice**

Pro ovládání systému jsou zvoleny klávesnice Paradox TM-50, které mají 5 palcový LCD display. Systém se ovládá pomocí ikon a textu. Na klávesnici je možné zobrazovat půdorysy zabezpečovaného objektu se zobrazením stavu každého detektoru. Toto ovládání je přehledné a pro uživatele pohodlné.


Obr. 38. Klávesnice Paradox TM-50 [20]

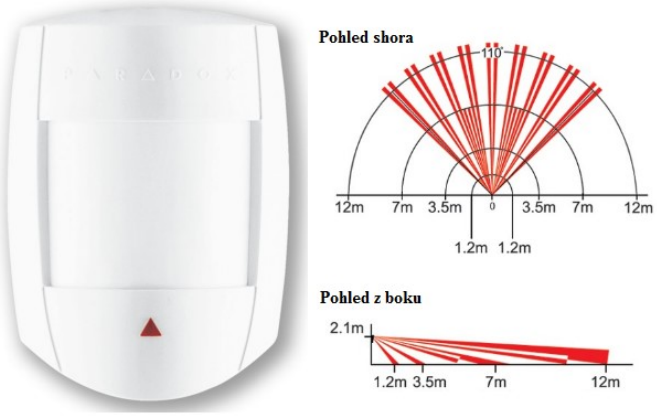
**Komunikátor**

Pro zajištění komunikace systému s DPPC je použit podobný komunikátor jako v první verzi zabezpečení. Komunikátor PARADOX PCS 250 umožňuje přenos zpráv přes sít GPRS a i GSM. Je tak možné si vybrat, která síť bude pro přenos signálu na DPPC využívána.

**PIR detektor**

Paradox DG55 je PIR detektor s plně digitálním zpracováním obrazu, digitální softwarovou teplotní kompenzací. Detektor má softwarovou ochranu „SHIELD“ se dvěma stupni nastavení, digitální automatický čítač impulsů. Maximální detekční dosah detektoru je 12 m. Detekční charakteristika je zobrazena na Obr. 39. V budově č. 1 je dlouhá chodba a je zde

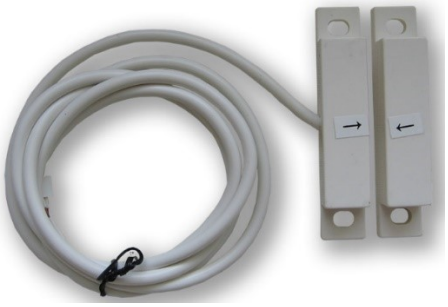
nutné použít čočku LR–2, která má detekční dosah 27 m. Detekční charakteristika je zobrazena na Obr. 27.




Obr. 39. Paradox DG55 – dual [20]

**Magnetický kontakt**

Je použit čtyřdrátový polarizovaný magnetický kontakt 3G-SM-60. V případě, že se k polarizovanému kontaktu přiblíží cizí magnet, smyčka se rozepne. Magnetický kontakt obsahuje tamper, pro případ pokusu o odejmutí plastového krytu. Má lepší ochranu proti překonání než magnetický kontakt použitý v první verzi zabezpečení. Pro sekční vrata bude použit polarizovaný magnetický kontakt MASS-303 stejně jako v první verzi zabezpečení.



Obr. 40. Magnetický kontakt
3G-SM-60 [20]

**IR závory**

Pro zabezpečení perimetru objektu jsem vybral paprskové infrazávory od firmy OPTEX. Skládají se z optického vysílače a přijímače. Infrazávory lze koupit s dosahem 20, 40, 60, 100 nebo až 200 m. V této verzi zabezpečení bude využita jedna infrazávora s dosahem 20 m a druhá s dosahem 60 m. Oproti infrazávorám VAR-TECH jsou tyto infrazávory dražší. Na druhou stranu, tyto závory mají vyšší stupeň krytí (IP65) a menší proudový odběr.


Obr. 41. Infrazávory OPTEX [21]

**IP kamery**

IP kamery byly vybrány od firmy Hikvision. Jedná se o model DS-2CD2T42WD-I8/4, který je určen pro venkovní použití. Stupeň krytí je 66 (IP66). Tyto 4 megapixelové IP kamery byly vybrány na základě požadovaných technických parametrů jako režim den/noc, dosah IR přísvitu, úhel záběrů. Jedna kamera bude umístěna na budově č.1, tak aby zabírala vozový park, budovu č.2 a č.3. Druhá kamera bude umístěna na stožárově lampě, která bude zabírat venkovní sklady materiálu, budovu č.1 a budovu č. 2. Technické parametry kamery jsou uvedeny v Tab. 22. Jelikož záznamy z kamer budou ukládány po dobu 3 dnů, je potřeba, dle zákona č. 101/200 Sb. §16, oznámit tuto skutečnost písemně Úřadu pro ochranu osobních údajů.

Tab. 22. Technické parametry kamer

| | |
|---|---|
| Snímací čip | 1/3" progressive scan CMOS |
| Objektiv | 4 mm @ F2.0 |
| Maximální rozlišení | 2688 × 1520 |
| Citlivost | 0.01 lux @ F1.2 / 0 lux s IR |
| IR přísvit (dosah) | 80 m |
| Úhel záběru | 83° |
| Poplachové funkce | Detekce pohybu, chyba LAN, nefunkční/zaplněný HDD |


Obr. 42. Venkovní kamera Hikvision [22]

**Videorekordér**

K ukládání záznamu IP kamer je použit videorekordér DS-7604NI-E1 od stejného výrobce. Umožnuje připojení 4 IP kamer s podporou PoE napájení (kamery jsou napájený přes síťový kabel). Pomocí videorekordéru je pak možnost, přes webový prohlížeč, se připojit ke IP kamerám. Data jsou ukládána na disk o maximální kapacitě 4 TB.


Obr. 43. Videorekordér DS-7604NI-E1 [22]

Velikost disku lze zvolit, dle potřebné doby uchování záznamu. Pro zjištění potřebné velikosti disku jsem použil mobilní aplikací CCTV kalkulátor, pomocí které jsem vypočítal doporučenou kapacitu záznamového média. Vstupními parametry jsou počet kamer, rozlišení, typ komprese, snímkovací frekvence a doba archivace. Doba archivace je stanovena na 3 dny se 100 % záznamem. Potřebná kapacita záznamového média byla stanovena na 658 GB. Na doporučení výrobce Hikvision, je vhodné použít disk značky Western Digital. K archivaci záznamu je vybrán disk Western Digital Purplem o kapacitě 1TB, který je určen po kamerové systémy. Jsou vytvořeny pro nepřetržitý provoz bezpečnostních sledovacích systému s vysokým rozlišením.

**Záložní zdroj**

Pro napájení kamerového systému je použit záložní napájecí zdroj UPS 650 VA. V případě výpadku napájení tento zdroj sepne a kamerový systém bude napájen z tohoto zdroje. Výrobce udává dobu zálohy 72 minut při příkonu 33 W při napětí 230 V. Z toho plyne, že při připojení videorekordéru se dvěma kamerami, je odhadována doba zálohy 69 minut.

## 8.2 Použité zařízení

Tab. 23. Rozmístění komponentů a jejich počet

| Komponenty | Typ | Budova | | | Venkovní areál | Počet |
|---|---|---|---|---|---|---|
| | | č.1 | č.2 | č.3 | | |
| Ústředna Spectra | Paradox – EVO HD | 1 | | | | 1 |
| Expandér | Paradox ZX32D | 1 | | | | 1 |
| Komunikátor | PCS250 – GSM/GPRS | 1 | | | | 1 |
| Klávesnice | Paradox TM-50 | 2 | | | | 2 |
| PIR detektor | Paradox DG55 | 14 | 3 | 1 | | 18 |
| Magnetický kontakt | 3G-SM-60 | 55 | 4 | 2 | | 61 |
| Magnetický kontakt | MASS - 303 | 1 | | | | 1 |
| Vnitřní siréna | Bell-tec Siren | 1 | | | | 1 |
| Venkovní siréna | Bell-tec Mini | | | | 1 | 1 |
| IR závora | Optex AX-70TN | | | | 1 | 1 |
| IR závora | Optex AX-200TN | | | | 1 | 1 |
| Transformátor | Trafo kryté 80VA | 1 | | | | 1 |
| IP kamera Hikvision | DS-2CD2T42WD-I8/4 | | | | 2 | 2 |
| Videorekordér | DS-7604NI-E1 | 1 | | | | 1 |
| Zdroj UPS | 650VA | 1 | | | | 1 |
| **Celkem** | | | | | | **94** |

- **Plášťová ochrana**

Plášťovou ochranu zajišťuje polarizovaný magnetický kontakt 3G-SM-60. Magnetický kontakt obsahuje tamper, pro případ pokusu o odejmutí plastového krytu. Lepší ochrana proti překonaní je zajištěna polarizací magnetu. Tyto magnetické kontakty jsou umístěny do otvorových vyplní všech budov. Pro sekční vrata je použit polarizovaný magnetický kontakt MASS-303 stejně jako v první verzi zabezpečení.

- **Prostorová ochrana**

Pro zajištění plastové ochrany jsou použity PIR detektory Paradox DG55, které mají vyšší odolnost proti RF rušení. Detektory jsou rozmístěny tak, aby nedocházelo k zastínění zorných polí detektorů a předešlo se falešným poplachům. V budově č. 1 je dlouhá chodba (místnost 1.11), ve které je nutné použít PIR detektor s čočku LR–2, která má detekční dosah 27 m.

- **Obvodová ochrana**

Je zajištěna pomocí infrazávor OPTEX. Infrazávory jsou umístěny na místa, kde je největší předpoklad vniknutí pachatele do areálu firmy. Dohled nad areálem objektu zajištují IP kamery od firmy Hikvision. Jedna kamera je umístěna na budově č.1 tak, že zabírá vozový park, budovu č.2 a č.3. Druhá kamera je umístěna na stožárově lampě, která zabírá venkovní sklady materiálu, budovu č.1 a budovu č. 2. Kamery jsou natočeny tak, aby pokryly co největší plochu areálu objektu.

- **Klávesnice**

Pro ovládání systému jsou zvoleny klávesnice Paradox TM-50, které mají 5 palcový LCD display. První klávesnice je umístěna u hlavního vchodu do budovy č.1 (místnost 1.01). Druhá klávesnice je umístěna u vedlejšího vchodu budovy č. 1 (místnost 1.11).

- **GSM / GPRS komunikátor**

Pro zajištění komunikace systému s DPPC je použit Komunikátor Paradox PCS 250. Umožňuje přenos zpráv přes síť GPRS a i GSM. Objekt je vzdálen od nejbližšího DPPC přibližně 5 minut cesty.

- **Akustická signalizace**

Venkovní siréna je použita stejná jako v první verzi zabezpečení. Do budovy č. 1 je umístěna siréna Bell-tec Siren. Bude umístěna v budově č.1 (místnost 1.11). Obě sirény jsou napájeny z ústředny, přes výstup BELL s maximálním proudovým odběrem 2 A.

- **Kabeláž**

Použitá kabeláž je stejná jako v první verzi zabezpečení. Dále je uvedena kabeláž pro připojení kamer k videorekordéru. Je použit stíněný kabel FTP CAT5e s pláštěm PE (polyethylen). Plášť PE poskytuje lepší ochranu proti vlivům okolního prostředí a jen určen pro venkovní použití. Kabely, vedoucí přes areál objektu jsou taženy pod betonovými panely. Délka a cena kabeláže kamerového systému je uvedena v Tab. 24.

Tab. 24. Délka a cena kabeláže kamerového systému

| Typ | Délka [m] | Cena |
|---|---|---|
| FTP venkovní kabel CAT5E | 100 | 1000 Kč |

- **Zóny a podsystémy**

Systém je rozdělen do 28 zón. Je použit jeden třiceti dvou zónový expandér s vnitřním spínaným zdrojem. Rozdělení zón viz. Příloha III.

- **Napájení**

Ústředna je napájená transformátorem 80VA s výstupní proudem 5 A. Transformátor je napojen na přívod síťového napětí 230 V / 50 Hz. Maximální proudový odběr systému je menší než proud, který je schopný dodat transformátor do systému. Z toho vyplývá, že transformátor je schopný zajistit požadovaný celkový maximální odběr ústředny a komponentů k ní připojené. V případě rozšiřování systému je vnitřním spínaný zdroj expandéru schopný poskytnout výstupní napětí 1 A. Maximální proudový odběr z AUX výstupu ústředny je 2 A.

Tab. 25. Odběr systému

| **Komponenty** | **Typ** | **Počet** | **Klid. odběr [mA]** | **Max. odběr [mA]** |
|---|---|---|---|---|
| Ústředna | Paradox – EVO HD | 1 | 100 | 100 |
| Expandér | Paradox ZX32D | 1 | 160 | 160 |
| Komunikátor | PCS250G – GPRS | 1 | 100 | 450 |
| Klávesnice | Paradox TM-50 | 2 | 200 | 400 |
| PIR detektor | Paradox DG55 | 18 | 252 | 504 |
| Vnitřní siréna | Bell-tec Siren | 1 | 0 | 400 |
| Venkovní siréna | Bell-tec Mini | 1 | 0 | 350 |
| IR závora | Optex AX-70TN | 1 | 38 | 38 |
| IR závora | Optex AX-200TN | 1 | 45 | 45 |
| **Proudový odběr všech komponentů** | | | **895** | **2447** |
| Dobíjecí proud záložního akumulátoru | | | 1500 | 1500 |
| **Celkem** | | | | **3947** |

**Výpočet kapacity akumulátoru**

- ústředna

$KNZ = 2{,}447 \times 12 = 29{,}364\ Ah$

Pro záložní napájení ústředny byl použit akumulátor o kapacitě 40Ah.

### Úbytky napětí na vedení

Pro všechny komponenty systému, které odebírají proud, byly vypočítány napěťové úbytky na vedení, stejně jako v návrhu I. Napětí neklesne pod minimální hodnotu udávanou výrobcem, a tak by měly komponenty budou fungovat správně.

- **Umístění komponentů v boxech**

Tab. 26. Umístění komponentu v boxech

| Box | Komponenty | Tamper – zóna |
|---|---|---|
| Box S 1 | Ústředna, expandér, transformátor | 8 |
| Box AKKU | Záložní akumulátor | 28 |

- **Cenová kalkulace**

Do celkového rozpočtu byly započítány všechny použité komponenty viz. Tab. 27. Cena kamerového systému navýšila celkovou cenu přibližně o dvacet tisíc korun. Délka kabeláže zahrnuje rezervu, pro případné překážky a nespecifikované prostory, které jsou zjištěny až při instalaci. Do cenového rozpočtu nejsou zahrnuty ceny šroubů, plastové trubky a další instalační materiál.

Tab. 27. Soupis všech komponentů a jejich cena

| Komponenty | Typ | Počet | Cena za kus | Celková cena s DPH |
|---|---|---|---|---|
| Ústředna Spectra | Paradox – EVO HD | 1 | 3 880 Kč | 3 880 Kč |
| Expandér | Paradox ZX32D | 1 | 6 480 Kč | 6 480 Kč |
| Komunikátor | PCS250 – GSM/GPRS | 1 | 5 630 Kč | 5 630 Kč |
| Klávesnice | Paradox TM-50 | 2 | 4 990 Kč | 9 980 Kč |
| PIR detektor | Paradox DG55 | 18 | 603 Kč | 10 854 Kč |
| Magnetický kontakt | 3G-SM-60 | 64 | 228 Kč | 14 592 Kč |
| Magnetický kontakt | MASS - 303 | 1 | 380 Kč | 380 Kč |
| Vnitřní siréna | Bell-tec Siren | 1 | 499 Kč | 499 Kč |
| Venkovní siréna | Bell-tec Mini | 1 | 990 Kč | 990 Kč |
| IR závora | Optex AX-70TN | 1 | 4 099 Kč | 4 099 Kč |
| IR závora | Optex AX-200TN | 1 | 5 440 Kč | 5 440 Kč |
| Transformátor | Trafo kryté 80VA | 1 | 842 Kč | 842 Kč |
| Box | Box S | 2 | 556 Kč | 1 112 Kč |
| Čočka | LR-2 | 1 | 169 Kč | 169 Kč |
| Mechanický zámek | pro box S | 1 | 133 Kč | 133 Kč |
| Box | AKKU 40 Ah | 1 | 605 Kč | 605 Kč |
| Záložní akumulátor | Smart SM40,0 | 1 | 3 989 Kč | 3 989 Kč |
| IP kamera Hikvision | DS-2CD2T42WD-I8/4 | 2 | 4 990 Kč | 9 980 Kč |
| Videorekordér | DS-7604NI-E1 | 1 | 5 231 Kč | 5 231 Kč |
| HDD - 1TB | WD Purple | 1 | 1 692 Kč | 1 692 Kč |
| Zdroj UPS | 650VA | 1 | 1 300 Kč | 1 300 Kč |
| Kabeláž | | | | 22 940 Kč |
| **Celkem** | | | | **110 817 Kč** |

# 9 ZHODNOCENÍ NÁVRHŮ ZABEZPEČOVACÍCH SYSTÉMŮ

První verze zabezpečení byla navržena i s ohledem na kladené požadavky dané firmy, jak již bylo uvedeno v úvodu do praktické části práce. Při výběru vhodných komponent zabezpečovacího systému jsem se opíral o teoretické poznatky získané během studia oboru Bezpečnostní technologie, systémy a management a také o konzultace s odbornou firmou System Plus Zlín, která má dlouhodobé zkušenosti v daném oboru. Jedná se o firmu, která má na starosti současný zabezpečovací systém uvedené firmy. Na základě dobrých zkušeností mně byly doporučeny komponenty od výrobce Paradox. Volbou komponentů od jednoho výrobce odpadají problémy s kompatibilitou jednotlivých komponentů. V první verzi zabezpečení byla použita ústředna Digiplex Evo 192 disponuje velkým počtem zón s možností připojení všech typu expandérů, na rozdíl od ústředny Spectra SP7000, ke které lze připojit pouze osmi zónové expandéry. Byl vybrán třiceti dvou zónový expandér s vnitřním spínaným zdrojem. Ten dostatečně pokryl minimální počet požadovaných zón. Další jeho výhodou je vnitřní spínaný zdroj, který společně s ústřednou pokryje maximální proudový odběr celého systému. Záložní akumulátory byly voleny dle rozměrů tak, aby se vešly společně s ústřednou a transformátorem do boxů. Pro komunikaci s dohledovým a poplachovým přijímacím centrem (dále již DPPC) byl zvolen GPRS komunikátor. Ten bude zasílat SMS o stavu systému pouze na DPPC soukromé bezpečnostní službě. Naskýtala se možnost, že by komunikace s DPPC probíhala po Ethernetové síti, ale dle mého názoru a na základě vlastních zkušeností je tato sít méně stabilní. Poplatky za využívání sítě se platí v obou případech. Pro prostorovou ochranu byly zvoleny PIR detektory, které mají běžnou detekční charakteristiku. Výhodou je vyměnitelná čočka. Otvorové výplně všech budov jsou zabezpečeny magnetickými kontakty s tamperem. Pro obvodovou ochranu objektu byly zvoleny IR závory, které detekují vstup pachatele do areálu firmy. Infrazávory jsou umístěny na místa, kde je největší předpoklad vniknutí pachatele do areálu firmy. Pro odrazení pachatele od vloupání je na budově č. 1 umístěna siréna s akustickou i optickou signalizací. Siréna je umístěna tak, že směruje do areálu firmy. Ovládání celého systému zajištují dvě tlačítkové klávesnice u hlavního a vedlejšího vchodu budovy č.1.

Druhá verze zabezpečení je vhodným doplněním a úpravou první verze návrhu. Prioritně vychází z mých poznatků a zkušeností získaných během studia výše uvedeného oboru. Uvažoval jsem nad zabezpečovacím systémem, který bude založen na sběrnicovém provedení. Hlavní výhodou sběrnicového systému je adresovatelnost jednotlivých

komponentů a menší spotřeba kabeláže. Problém nastal u sběrnicových magnetických kontaktů, jejíž cena je příliš vysoká. Cena sběrnicového magnetického kontaktu od firmy Paradox je 1 000 Kč/ks. Cena za všechny magnetické kontakty činila okolo 61 000 Kč. Proto jsem se rozhodl dát přednost detektorům, které se zapojují do smyček. Pro druhou verzi zabezpečení jsem zvolil ústřednu Digiplex Evo HD, která disponuje lepšími technickými parametry. Oproti ústředně Evo 192 je maximální proudový odběr, z výstupu AUX, dvojnásobný. Díky tomu je potřeba použít, pro napájení ústředny, výkonnější transformátor. Pro záložní napájení ústředny jsou potřeba akumulátory o větší kapacitě. Nevýhodou jsou jejich rozměry, díky kterým se nevlezou do boxů a je zapotřebí je umístit do boxů zvlášť. Na druhou stranu, ústředna zvládá větší proudovou zátěž a není potřeba dokupovat doplňkové zdroje, které vyžadují další transformátory a záložní akumulátory. Pro přenos zpráv na DDPC byl vybrán komunikátor, který umožňuje přenos zpráv přes síť GPRS a i GSM. Je tak možné si vybrat, která síť bude pro přenos signálu na DPPC využívána. V případě vyhlášení poplachu, je hlídka soukromé bezpečnostní služby schopná dorazit na místo do 5 minut. Pro prostorovou ochranu byly zvoleny digitální PIR detektory, které mají běžnou detekční charakteristiku. Od analogových PIR detektorů se odlišují digitálním zpracováním obrazu, a tedy vyšší odolností proti radiofrekvenčnímu rušení. Otvorové výplně všech budov jsou zabezpečeny magnetickými kontakty s tamperem a ochranou proti přepólování. Pro obvodovou ochranu objektu byly zvoleny IR závory, které detekují vstup pachatele do areálu firmy. Tyto IR závory mají menší proudový odběr než IR závory použité v první verzi. Pro odrazení pachatele od vloupání je akustická signalizace doplněna o vnitřní sirénu v budově č. 1. Je umístěna tak, aby se zvuk šířil po celé budově. Ovládání celého systému zajištují dvě klávesnice s LCD displejem, jejichž ovládání je přehledné a pro uživatele pohodlné. Další investicí do ochrany objektu je kamerový systém, který je využit na monitorování areálu firmy. K těmto kamerám by měli přístupu, přes webový prohlížeč, majitel firmy a soukromá bezpečnostní služba. Použití kamer, dle mého názoru, by mohlo snížit i množství krádeží materiálu, které páchají zaměstnanci. Záznamy z kamer jsou archivovány na pevném disk po dobu tří dnů.

První verze zabezpečení byla vytvořena s ohledem na provedené bezpečnostního posouzení a analýzu rizik. Mimo jiné bylo přihlédnuto i na požadavky firmy včetně finančních prostředků. Nebylo zde místo pro volbu kvalitnějších komponentů a využití dalších zabezpečovacích systému jako např. CCTV.

# ZÁVĚR

Cílem této diplomové práce je návrh zabezpečení firmy se specifickým provozem. Jedná se o firmu zaměřenou na elektroinstalační práce a servis v oblasti vysokého i nízkého napětí. Stávající zabezpečovací systém firmy byl vybudován před čtrnácti lety. Bohužel tento systém v současnosti nesplňuje požadovaný standard a není již dostačující. Svědčí o tom i fakt, že se daná firma v poslední době stala opakovaně předmětem vloupání. Cílem těchto trestných činů bylo zejména odcizení drahých kovů nemalé finanční hodnoty. Zabezpečovací systém převzala soukromá bezpečnostní agentura Systém Plus Zlín, která s vedením firmy pracuje na modernizaci celého systému. Tato modernizace se má uskutečnit současně s plánovanou výměnou stávajících, tj. zastaralých elektrických rozvodů, a to v roce 2018. Výstupy této práce budou sloužit jako inspirace, popř. jako srovnávací materiál pro následnou realizaci bezpečnostního systému celého areálu uvedené firmy. Předložená práce je koncipována do dvou částí, a to teoretické a praktické.

Teoretická část se zabývá obecným rozborem zabezpečovacích systémů. Zvýšená pozornost je věnována jednotlivým typům ochran, technickým a jednotlivým systémům. Část práce obecně pojednává o bezpečnostním posouzení objektů a také bezpečnostní analýze rizik.

Praktická část práce je zaměřena na samotný návrh zabezpečovacího systému objektu výše uvedené firmy. Konkrétně se jedná o dva návrhy zabezpečení. Oba návrhy vychází ze zkušeností a znalostí získaných během mého studia oboru Bezpečnostní technologie, systémy a management na Fakultě aplikované informatiky, Univerzity Tomáše Bati ve Zlíně. První návrh se mimo výše uvedené opíral i o konzultace získané u bezpečnostní agentury Systém Plus Zlín, která jak již bylo uvedeno výše provádí dosavadní dohled nad objektem dotčené firmy a v daném oboru má dlouholeté zkušenosti. Při tomto návrhu byl také brán ohled i na požadavky a možnosti zabezpečované firmy, která spolupracovala po stránce poskytování potřebných informací a technických parametrů souvisejících s objekty v areálu firmy. Na základě provedeného bezpečnostního posouzení objektu a bezpečnostní analýzy rizik bylo zjištěno, že největší hrozbou je riziko vloupání a krádeže. Z těchto důvodů bylo převážně soustředěno na rozšíření poplachového zabezpečovacího systému (dále jen PZS). Výrobce jednotlivých komponentů PZS jsem vybral na základě již uvedených svých znalostí a konzultací s odbornou firmou. Cílem navrhovaných opatření bylo snížit míru rizika u závažných hrozeb. Druhá verze zabezpečení je vhodným doplněním

a úpravou první verze návrhu. Prioritně vychází z mých poznatků a zkušeností získaných během studia uvedeného oboru. Podrobnější zhodnocení obou návrhů je popsáno v předchozí kapitole číslo 9.

Veškerá dokumentace, včetně rozmístění všech komponentů zabezpečovacího systému a rozvodů kabelového vedení, byla zpracována v programu AutoCAD 2017 a je součástí i přiloženého CD nosiče. Na přání majitele nebudou v této práci uveřejněny žádné údaje, které by přímo identifikovaly nejmenovanou firmu, a to z bezpečnostních důvodů. Firma vzhledem ke své činnosti skladuje velké množství drahých kovů, které by se mohly stát předmětem dalšího odcizení. Práce by pak mohla sloužit jako manuál k překonání stávajícího a popř. budoucího zabezpečovacího systému.

# SEZNAM POUŽITÉ LITERATURY

[1] UHLÁŘ, Jan. *Technická ochrana objektů II: Elektrické zabezpečovací systémy.* Vyd. 1. Praha: Vydavatelství Policejní akademie České republiky, 2005, 229 s. ISBN 80-7251-189-0.

[2] KINDL, Jiří. *Projektování bezpečnostních systémů*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.

[3] VALOUCH, Jan. *Projektovaní integrovaných systémů*. Zlín. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2015. ISBN 978-80-7454-557-3.

[4] UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8.

[5] ČANDÍK, Marek. *Objektová bezpečnost II.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 100 s. Učební texty vysokých škol / Univerzita Tomáše Bati ve Zlíně. ISBN 8073182173.

[6] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. [aktualiz. S.l.: Cricetus], 2006, 313 s. ISBN 80-902938-2-4.

[7] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. Zlín: VeRBuM, 2011–2015, 368 s. ISBN 978-80-87500-05-7.

[8] ŠEFČÍK, Vladimír. *Analýza rizik*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 98 s. ISBN 978-80-7318-696-8.

[9] DRGA, Michal. *Pult centrální ochran a jeho role v průmyslu komerční bezpečností*. Zlín, 2012. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce JUDr. Josef Čejka.

[10] Způsoby připojení. *Centrpco* [online]. Mladá Boleslav: CENTR PCO, 2016 [cit. 2017-02-08]. Dostupné z: http://www.centrpco.cz/index.php/zpusoby-pripojeni

[11] Pult centralizované ochrany. *Interconnect* [online]. 250 84 Křenice: INTERCONNECT, ©2015 [cit. 2017-02-16]. Dostupné z: https://www.interconnect.cz/ostatni-sluzby/bezpecnostni-systemy/pult-centralizovane-ochrany

[12] HLADÍK, Drahoslav. *Elektronické zabezpečovací systémy a elektronická požární signalizace* [online]. Plzeň, 2010 [cit. 2017-02-18]. Dostupné z: http://docplayer.cz/5837827-Elektronicke-zabezpecovaci-systemy-a-elektronicka-pozarni-signalizace-drahoslav-hladik.html

[13] KUBÁT, Zbyšek. *ČIPOVÝ PŘÍSTUPOVÝ SYSTÉM. Docplayer* [online]. Praha: Střední průmyslová škola elektrotechnická, 2013 [cit. 2017-02-18]. Dostupné z: http://docplayer.cz/950761-Cipovy-pristupovy-system.html

[14] Obecně o RFID technologii. *Eprin* [online]. Brno: EPRIN spol. s r.o., 2016 [cit. 2017-02-18]. Dostupné z: http://www.eprin.cz/rfid-technologie.html

[15] Biometrie. *BiometricLine* [online]. Brno: ABBAS, 2017 [cit. 2017-02-21]. Dostupné z: http://www.biometricke-ctecky.cz/

[16] ČANDÍK, Marek. ANALÝZA BEZPEČNOSTNÍCH RIZIK INFORMAČNÍCH SYSTÉMŮ. *Teorie informační bezpečnosti* [online]. 2015, (2015/2), 10 [cit. 2017-02-25]. Dostupné z: http://www.teorieib.cz/pbi/files/138-06_%C4%8Cand%C3%ADk_Anal%C3%BDza%20bezpe%C4%8Dnostn%C3%ADch%20rizik.pdf

[17] ŠEVČÍK, Jiří. *Bezpečnostní posouzení objektu*. Zlín, 2010. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Jan Valouch, Ph.D.

[18] VESELÝ, Milan. *POUŽITÍ METODY FMEA PRO PREVENCI CHYB V PRŮMYSLOVÉM PODNIKU* [online]. Brno, 2012 [cit. 2017-02-26]. Dostupné z: https://core.ac.uk/download/pdf/30307941.pdf. Diplomová práce. Vedoucí práce Ing. LUBOŠ KOTEK, Ph.D.

[19] Nahlížení do katastru nemovitostí. *Nahlizenidokn* [online]. Praha: Český úřad zeměměřický a katastrální, ©2004-2017 [cit. 2017-05-09]. Dostupné z: http://nahlizenidokn.cuzk.cz/

[20] Obor-ezs. *Variant* [online]. Praha: VARIANT plus, ©2008-2015 [cit. 2017-05-09]. Dostupné z: https://www.variant.cz/dokumenty/obor-ezs/

[21] ZABEZPEČOVACÍ SYSTÉMY. *Euroalarm* [online]. Praha: EUROALARM, ©2008-2015 [cit. 2017-05-09]. Dostupné z: https://www.euroalarm.cz/eshop-zabezpecovaci-technika/zabezpeceni/

[22] IP KAMERY. *Abalarm* [online]. Praha: AB ALARM, ©2017 [cit. 2017-05-09]. Dostupné z: http://www.abalarm.cz/ishop/cs/13-ip-kamery

[23] DOBAIEŠOVÁ, Žaneta. *Zabezpečenie vnútornej ochrany vybraného objektu*. Žilina, 2007. Diplomová práce. Žilinská univerzita v Žilině. Vedoucí práce Ing. Selinger Petr.

[24] SKLÁŘ, Petr. *Návrh zabezpečovacího systému kalírny*. Zlín, 2016. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Petr Skočík.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| A | Ampér |
| Ah | Ampér – hodina |
| AUX | Označení výstupu ústředny |
| CMOS | Complementary Metal-Oxide-Semiconductor |
| CD | Compact Disk |
| CCTV | Close Circuit Television |
| ČSN EN | Evropská norma převzatá do národního systému norem ČR |
| DPPC | Dohledová a poplachová příjímací centra |
| DWG | AutoCAD Drawing |
| ed. | edition |
| EPS | Elektrická požární signalizace |
| GPRS | Global Packet Radio System |
| GSM | Global System of Mobile Communications |
| GB | Gigabyte |
| IP | Internet protokol |
| IR | Infrared |
| KNZ | Kapacita náhradního zdroje |
| LED | Light Emitting Diode |
| LUX | Jednotka intenzity osvětlení |
| LCD | Liquid Crystal Display |
| MZS | Mechanické zábranné systémy |
| mm | Milimetr |
| $mm^2$ | Milimetr čtverečný |
| m | Metr |

| | |
|---|---|
| $m^2$ | Metr čtverečný |
| mA | Miliampér |
| PDF | Packet Definition File |
| PIR | Passive Infrared |
| SMS | Short Message Service |
| SKV | Systém kontroly vstupu |
| SWOT | Strengths, Weaknesses, Opportunities, Threats |
| tzv. | takzvaný |
| TB | Terabyte |
| V | Volt |
| VF | Vysokofrekvenční |
| VA | Volt - ampér |
| Kč | Koruna česká |

# SEZNAM OBRÁZKŮ

Obr. 1. Princip činnosti DPPC [11] ....16
Obr. 2. Smyčka NO [12] ....19
Obr. 3. Smyčka NC [12] ....19
Obr. 4. Smyčka EOL [12] ....20
Obr. 5. Smyčka 2EOL [12] ....21
Obr. 6. Smyčka AZT [12] ....21
Obr. 7. Výhody Biometrie [15] ....30
Obr. 8. Obsah posouzení objektu [3] ....31
Obr. 9. Dělení metod dle vyjádření používaných veličin [17] ....39
Obr. 10. Půdorys areálu firmy [19] ....45
Obr. 11. Venkovní skladování elektroinstalačního materiálu 1 ....47
Obr. 12. Venkovní skladování elektroinstalačního materiálu 2 ....48
Obr. 13. Budova č.1 ....49
Obr. 14. Budova č.3 ....50
Obr. 15. Perimetr objektu [19] ....51
Obr. 16. AutoCAD 2017 – Hlavní okno ....59
Obr. 17. Rozmístění zařízení – budova č.1 ....61
Obr. 18. Rozmístění zařízení – budova č.2 ....62
Obr. 19. Rozmístění zařízení – budova č.3 ....63
Obr. 20. Rozmístění zařízení – venkovní areál ....64
Obr. 21. Ústředna Spectra SP7000 [20] ....65
Obr. 22. Ústředna Evo 192 [20] ....66
Obr. 23. Záložní baterie 12 V/18 Ah [20] ....67
Obr. 24. Expandér Paradox ZX32D [20] ....68
Obr. 25. Komunikátor PCS250G [20] ....68
Obr. 26. PIR detektor PARADOX PRO PLUS 476 [20] ....69
Obr. 27. Čočka LR – 2 [20] ....69
Obr. 28. Magnetický kontakt SM-50 T [20] ....70
Obr. 29. Magnetický kontakt MASS-303 [20] ....70
Obr. 30. Infrazávory VAR-TEC [20] ....71
Obr. 31. Siréna BELL-TEC MINI [20] ....71
Obr. 32. Klávesnice PARADOX – K641+ [20] ....72

Obr. 33. Rozmístění zařízení – budova č.1 ..... 80
Obr. 34. Rozmístění zařízení – venkovní areál ..... 81
Obr. 35. PARADOX EVO HD [20] ..... 82
Obr. 36. Záložní baterie 12 V/40 Ah [20] ..... 83
Obr. 37. Siréna BELL-TEC SIREN [20] ..... 84
Obr. 38. Klávesnice Paradox TM-50 [20] ..... 84
Obr. 39. Paradox DG55 – dual [20] ..... 85
Obr. 40. Magnetický kontakt 3G-SM-60 [20] ..... 85
Obr. 41. Infrazávory OPTEX [21] ..... 86
Obr. 42. Venkovní kamera Hikvision [22] ..... 87
Obr. 43. Videorekordér DS-7604NI-E1 [22] ..... 87

# SEZNAM TABULEK

Tab. 1. Požadované doby nabíjení [6] ....23
Tab. 2. Požadované doby zálohy [6]....23
Tab. 3. Stupeň zabezpečení [3]....37
Tab. 4. Třídy prostředí [3] ....37
Tab. 5. Rozsah PZTS [3] ....38
Tab. 6. Vztah hrozeb a aktiv ....55
Tab. 7. Závažnost dopadu rizika....56
Tab. 8. Pravděpodobnost výskytu problému ....56
Tab. 9. Odhalitelnost problému ....57
Tab. 10. Hrozby – opatření ....57
Tab. 11. Hodnocení rizik ....58
Tab. 12. Technické parametry ústředny SP7000 ....65
Tab. 13. Technické parametry ústředny Evo 192 ....66
Tab. 14. Rozmístění komponentů a jejich počet....72
Tab. 15. Soupis kabeláže ....74
Tab. 16. Odběr systému ....75
Tab. 17. Odběr ústředny ....75
Tab. 18. Odběr expandéru s připojenými komponenty ....76
Tab. 19. Umístění komponentu v boxech....77
Tab. 20. Soupis všech komponentů a jejich cena ....78
Tab. 21. Technické parametry ústředny Evo HD ....82
Tab. 22. Technické parametry kamer ....86
Tab. 23. Rozmístění komponentů a jejich počet....88
Tab. 24. Délka a cena kabeláže kamerového systému....89
Tab. 25. Odběr systému ....90
Tab. 26. Umístění komponentu v boxech....91
Tab. 27. Soupis všech komponentů a jejich cena ....92

# SEZNAM PŘÍLOH

P I Popis místností

PII Rozdělení zón – verze I

PIII Rozdělení zón – verze II

PIV Výkresová dokumentace – verze I.

PV Výkresová dokumentace – verze II.

# PŘÍLOHA P I: POPIS MÍSTNOSTÍ

| **Budova č.1** | |
|---|---|
| **Č.M** | **NÁZEV MÍSTNOSTI** |
| 1.01 | Vstupní hala |
| 1.02 | Denní místnost |
| 1.03 | Kuchyňka |
| 1.04 | Chodba 1 |
| 1.05 | Kancelář 1 |
| 1.06 | Kancelář 2 |
| 1.07 | Kancelář 3 |
| 1.08 | Kancelář 4 |
| 1.09 | Špinavá místnost |
| 1.10 | Dílna |
| 1.11 | Chodba 2 |
| 1.12 | WC |
| 1.13 | Umývárna – sprchy |
| 1.14 | WC |
| 1.15 | Kancelář 5 |
| 1.16 | Archív |
| 1.17 | Předsíň – WC |
| 1.18 | WC – muži |
| 1.19 | WC – ženy |
| 1.20 | Sprcha |
| 1.21 | Úklidová místnost |
| 1.22 | Garáž |
| 1.23 | Půda |
| **Budova č.2** | |
| **Č.M** | **NÁZEV MÍSTNOSTI** |
| 2.01 | Sklad materiálu |
| 2.02 | Sklad nářadí |
| **Budova č.3** | |
| **Č.M** | **NÁZEV MÍSTNOSTI** |
| 3.01 | Sklad materiálu + garáž |

# PŘÍLOHA P II: ROZDĚLENÍ ZÓN – VERZE I

| | Zóna | Účel/Místnost | Komponenty | Druh zóny |
|---|---|---|---|---|
| Deska ústředny | 1 | 1.26 | 1 x PIR | okamžitá |
| | 2 | 1.01 | 3 x MK, 2 x PIR | zpožděná |
| | 3 | 1.02 | 6 x MK, 1 x PIR | okamžitá |
| | 4 | 1.03 | 1 x MK, 1 x PIR | okamžitá |
| | 5 | 1.18, 1.19 | 2 x MK | okamžitá |
| | 6 | 1.22.1 | 1 x MK | okamžitá |
| | 7 | Tamper venkovní sirény | Tamper | 24 hodinová |
| | 8 | Tamper – ústředna | Tamper | 24 hodinová |
| Expandér | 9 | 1.05 | 3 x MK, 1 x PIR | okamžitá |
| | 10 | 1.06 | 4 x MK, 1 x PIR | okamžitá |
| | 11 | 1.07 | 4 x MK, 1 x PIR | okamžitá |
| | 12 | 1.08 | 4 x MK, 1 x PIR | okamžitá |
| | 13 | 1.09 | 2 x MK, 1 x PIR | okamžitá |
| | 14 | 1.10 | 8 x MK, 1 x PIR | okamžitá |
| | 15 | 1.11 | 2 x MK, 1 x PIR | zpožděná |
| | 16 | 1.12 | 2 x MK | okamžitá |
| | 17 | 1.13 | 2 x MK | okamžitá |
| | 18 | 1.14 | 4 x MK | okamžitá |
| | 19 | 1.15 | 2 x MK, 1 x PIR | okamžitá |
| | 20 | 1.16 | 2 x MK, 1 x PIR | okamžitá |
| | 21 | 1.23 | 1 x MK | okamžitá |
| | 22 | 2.02 | 1 x PIR | okamžitá |
| | 23 | 2.03 | 4 x MK, 2 x PIR | okamžitá |
| | 24 | 3.01 | 4 x MK, 1 x PIR | okamžitá |
| | 25 | Venkovní areál | Infrazávora 1 | zpožděná |
| | 26 | Venkovní areál | Infrazávora 2 | okamžitá |
| | - | - | - | - |
| | - | - | - | - |
| | - | - | - | - |
| | 40 | Tamper – expandéru | Tamper | 24 hodinová |

# PŘÍLOHA P III: ROZDĚLENÍ ZÓN – VERZE II

| | Zóna | Účel/Místnost | Komponenty | Druh zóny |
|---|---|---|---|---|
| Deska ústředny | 1 | 1.26 | 1 x PIR | okamžitá |
| | 2 | 1.01 | 3 x MK, 2 x PIR | zpožděná |
| | 3 | 1.02 | 6 x MK, 1 x PIR | okamžitá |
| | 4 | 1.03 | 1 x MK, 1 x PIR | okamžitá |
| | 5 | 1.18, 1.19 | 2 x MK | okamžitá |
| | 6 | 1.22.1 | 1 x MK | okamžitá |
| | 7 | Tamper venkovní sirény | Tamper | okamžitá |
| | 8 | Tamper – ústředna | Tamper | 24 hodinová |
| Expandér | 9 | 1.05 | 3 x MK, 1 x PIR | okamžitá |
| | 10 | 1.06 | 4 x MK, 1 x PIR | okamžitá |
| | 11 | 1.07 | 4 x MK, 1 x PIR | okamžitá |
| | 12 | 1.08 | 4 x MK, 1 x PIR | okamžitá |
| | 13 | 1.09 | 2 x MK, 1 x PIR | okamžitá |
| | 14 | 1.10 | 8 x MK, 1 x PIR | okamžitá |
| | 15 | 1.11 | 2 x MK, 1 x PIR | zpožděná |
| | 16 | 1.12 | 2 x MK | okamžitá |
| | 17 | 1.13 | 2 x MK | okamžitá |
| | 18 | 1.14 | 4 x MK | okamžitá |
| | 19 | 1.15 | 2 x MK, 1 x PIR | okamžitá |
| | 20 | 1.16 | 2 x MK, 1 x PIR | okamžitá |
| | 21 | 1.23 | 1 x MK | okamžitá |
| | 22 | 2.02 | 1 x PIR | okamžitá |
| | 23 | 2.03 | 4 x MK, 2 x PIR | okamžitá |
| | 24 | 3.01 | 4 x MK, 1 x PIR | okamžitá |
| | 25 | Venkovní areál | Infrazávora 1 | zpožděná |
| | 26 | Venkovní areál | Infrazávora 2 | okamžitá |
| | 27 | Tamper vnitřní sirény | Tamper | 24 hodinová |
| | 28 | Tamper box AKKU | Tamper | 24 hodinová |
| | - | - | - | - |
| | - | - | - | - |
| | - | - | - | - |
| | 40 | - | - | - |

Popis zón:

- 24 hodinová – zóna je 24hodin aktivní. Narušení této zóny vyvolá poplach typu sabotáž.
- Okamžitá – Zóna se stává aktivní hned po zastřežení objektu. Narušení této zóny vyvolá poplach.
- Zpožděná – v průběhu provádění zastřežení a odstřežení objektu zóna nevyvolá poplach.