

# Návrh zabezpečovacího systému strojírenské firmy

Bc. Marek Vraj

---

Diplomová práce  
2016

 Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2015/2016

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Marek Vraj**  
Osobní číslo: **A14358**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **prezenční**

Téma práce: **Návrh zabezpečovacího systému strojírenské firmy**  
Téma anglicky: **A Security System Designed for an Engineering Company**

Zásady pro vypracování:

1. Proveďte obecný rozbor zabezpečovacích systémů a zařízení určených k ochraně průmyslových objektů.
2. Seznamte se s aktuálním stavem celého areálu firmy a popište jeho stávající zabezpečení.
3. Proveďte bezpečnostní analýzu rizik provozovny firmy a to s ohledem na její specifický provoz.
4. Vyberte vhodné zabezpečovací systémy a zařízení s ohledem na kladené požadavky.
5. Na základě analýzy rizik navrhnete dva systémy zabezpečení provozovny.
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. ČANDÍK, Marek. Objektová bezpečnost II. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2004, 100 s. ISBN 8073182173.
2. VALOUCH, Jan. Projektování bezpečnostních systémů. Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2012, 152 s. ISBN 978-80-7454-230-5. Dostupné také z: <http://dspace.k.utb.cz/handle/10563/18663>.
3. KOLEKTIV, Luděk Lukáš a. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBUm, 2012, 386 s. ISBN 978-808-7500-194.
4. UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8.
5. LOVEČEK, Tomáš; NAGY, Peter. Bezpečnostné systémy: kamerové bezpečnostné systém. Vyd. 1. Žilina: Žilinská univerzita, 2008, 283 s. ISBN 978-80-8070-893-1.
6. IVANKA, Ján. Systemizace bezpečnostního průmyslu. Vyd. 5. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2014, 219 s. ISBN 978-80-7454-410-1. Dostupné také z: <http://hdl.handle.net/10563/27488>.
7. KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 80-902938-2-4.

Vedoucí diplomové práce:

**Ing. Petr Skočík**

Ústav elektroniky a měření

Datum zadání diplomové práce:

**5. února 2016**

Termín odevzdání diplomové práce:

**16. května 2016**

Ve Zlíně dne 5. února 2016



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



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

### **Prohlašuji, že**

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

### **Prohlašuji,**

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

Ve Zlíně, dne 14.5.2016

  
.....  
podpis diplomanta

## **ABSTRAKT**

Diplomová práce je zaměřena na zabezpečení objektu se specifickým provozem, která se specializuje na strojírenský průmysl, pomocí poplachového a kamerového systému s použitými mechanickými zabezpečovacími prvky. Samotná práce je rozdělena do dvou částí, tj. teoretickou a praktickou. V teoretické části jsou uvedeny mechanické zábranné systémy. Na ně navazují signalizační a monitorovací systémy. Rozdělení zabezpečovacích systémů a bezpečnostní analýzy je také nedílnou součástí teoretické části. Hlavním bodem praktické části je návrh dvou zabezpečovacích systémů, které jsou mezi sebou porovnány a zhodnoceny. Tyto návrhy zabezpečení obsahují prvky a systémy zmíněné v teoretické části. Při postupu je zohledněno bezpečnostní posouzení a bezpečnostní analýza, zaměřená na odhalení hrozeb působící na objekt.

Klíčová slova: Zabezpečovací systémy, mechanické zábranné systémy, poplachový zabezpečovací a tísňový systém, kamerový systém, bezpečnostní analýza

## **ABSTRACT**

This diploma thesis is focused on security systems of building with specific operation, which is interested in engineering industry. There are used alarm and camera system with mechanical safety elements. This piece of work is divided into two parts – theoretical and practical. In the first section are described mechanical barrier systems. This is followed by signalling and monitoring systems. Distribution of security systems and security analysis is also integral part of theoretical background. Main point of practical part is suggestion of two version of security systems, which are evaluated and compared with each other. This suggestions of security comprise elements and systems mentioned in theoretical section. In the process are taken into account the safety assessment and safety analysis, that reveals threats acting on object.

Keywords: Security systems, mechanical barrier system, intruder and hold-up alarm system, closed circuit television, security analysis

Chtěl bych poděkovat vedoucímu mé diplomové práce Ing. Petru Skočíkovi, za odborné vedení, užitečné rady, čas a trpělivost při konzultacích. Dále bych chtěl poděkovat vedení firmy, že mi vyšli vstříc a poskytli potřebné informace. V neposlední řadě i rodině a kamarádům za psychickou podporu.

# OBSAH

|  |           |
|--|-----------|
| <b>ÚVOD</b> .....  | <b>9</b>  |
| <b>I TEORETICKÁ ČÁST</b> .....                             | <b>10</b> |
| <b>1 TECHNICKÁ OCHRANA OBEJKTU</b> .....                   | <b>11</b> |
| 1.1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY .....                      | 11        |
| 1.1.1 Obvodová ochrana .....                               | 12        |
| 1.1.2 Plášťová ochrana .....                               | 13        |
| 1.1.3 Předmětová ochrana .....                             | 13        |
| <b>2 SIGNALIZAČNÍ A MONITOROVACÍ ZAŘÍZENÍ</b> .....        | <b>15</b> |
| 2.1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY .....       | 15        |
| 2.1.1 Přehled prvků .....                                  | 18        |
| 2.2 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE .....                   | 21        |
| 2.2.1 Dělení hlásičů .....                                 | 22        |
| 2.3 KAMEROVÉ SYSTÉMY .....                                 | 25        |
| 2.3.1 Přenosy signálu .....                                | 26        |
| 2.3.2 Snímače obrazu .....                                 | 27        |
| 2.3.3 Technické parametry kamer .....                      | 29        |
| 2.4 PŘÍSTUPOVÝ SYSTÉM.....                                 | 30        |
| 2.4.1 Identifikace uživatele .....                         | 31        |
| 2.4.2 Způsoby přístupu .....                               | 32        |
| 2.4.3 Biometrické systémy .....                            | 33        |
| <b>3 ZABEZPEČOVACÍ SYSTÉMY</b> .....                       | <b>35</b> |
| 3.1 OPERAČNÍ HLEDISKO .....                                | 35        |
| 3.2 TECHNICKÉ HLEDISKO .....                               | 38        |
| <b>4 ANALÝZA RIZIK A BEZPEČNOSTNÍ ANALÝZY</b> .....        | <b>40</b> |
| 4.1 ANALÝZA RIZIK.....                                     | 40        |
| 4.2 VYBRANÉ KVALITATIVNÍ ANALÝZY .....                     | 41        |
| 4.3 VYBRANÉ KVANTITATIVNÍ ANALÝZY .....                    | 45        |
| <b>II PRAKTICKÁ ČÁST</b> .....                             | <b>47</b> |
| <b>5 ÚVOD DO PRAKTICKÉ ČÁSTI</b> .....                     | <b>48</b> |
| <b>6 POPIS OBJEKTU A JEHO BEZPEČNOSTNÍ POSOUZENÍ</b> ..... | <b>49</b> |
| 6.1 AREÁL OBJEKTU SPOLEČNOSTI .....                        | 49        |
| 6.2 BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU .....                   | 52        |
| 6.2.1 Zabezpečované hodnoty .....                          | 52        |
| 6.2.2 Budovy objektu .....                                 | 54        |
| 6.2.3 Vnitřní vlivy .....                                  | 55        |
| 6.2.4 Vnější vlivy .....                                   | 56        |
| 6.3 BEZPEČNOSTNÍ ANALÝZA .....                             | 56        |
| 6.3.1 Vyhodnocení bezpečnostní analýzy .....               | 60        |
| <b>7 NÁVRH ZABEZPEČOVACÍHO SYSTÉMU – VERZE 1</b> .....     | <b>61</b> |

|          |   |            |
|----------|---|------------|
| 7.1      | POŽADAVKY NA NÁVRH ZABEZPEČENÍ – VERZE 1 .....                    | 61         |
| 7.2      | STUPEŇ ZABEZPEČENÍ A TŘÍDA PROSTŘEDÍ.....                         | 62         |
| 7.3      | PŮDORYSY ZABEZPEČOVANÉ BUDOVY .....                               | 63         |
| 7.3.1    | Použitý SW pro vytvoření půdorysů objektu .....                   | 65         |
| 7.4      | VÝBĚR VHODNÝCH PRVKŮ PRO NÁVRH ZABEZPEČENÍ – VERZE 1 .....        | 66         |
| 7.5      | ROZMÍSTĚNÍ PRVKŮ ZABEZPEČENÍ DO PŮDORYSŮ – VERZE 1.....           | 74         |
| 7.6      | KONFIGURACE SYSTÉMU A ZÓNY ZABEZPEČOVACÍHO SYSTÉMU – VERZE 1..... | 76         |
| 7.7      | CENOVÁ KALKULACE VYBRANÝCH ZABEZPEČOVACÍCH PRVKŮ – VERZE 1 .....  | 78         |
| 7.8      | ZPŮSOB HLÁŠENÍ POPLACHU A ZÁSAH .....                             | 79         |
| 7.9      | ÚDRŽBA SYSTÉMU.....   | 79         |
| 7.10     | LEGISLATIVA A NORMY .....   | 79         |
| <b>8</b> | <b>NÁVRH ZABEZPEČOVACÍHO SYSTÉMU – VERZE 2.....</b>               | <b>80</b>  |
| 8.1      | POŽADAVKY NA NÁVRH ZABEZPEČENÍ – VERZE 2.....                     | 80         |
| 8.2      | DOPLŇUJÍCÍ VYBRANÉ PRVKY PRO NÁVRH ZABEZPEČENÍ – VERZE 2.....     | 80         |
| 8.3      | ROZMÍSTĚNÍ PRVKŮ ZABEZPEČENÍ DO PŮDORYSŮ – VERZE 2.....           | 85         |
| 8.4      | KONFIGURACE SYSTÉMU A ZÓNY ZABEZPEČOVACÍHO SYSTÉMU – VERZE 2..... | 87         |
| 8.5      | CENOVÁ KALKULACE VYBRANÝCH ZABEZPEČOVACÍCH PRVKŮ – VERZE 2.....   | 89         |
| <b>9</b> | <b>POROVNÁNÍ NAVRŽENÝCH SYSTÉMŮ ZABEZPEČENÍ.....</b>              | <b>91</b>  |
|          | <b>ZÁVĚR .....</b>  | <b>93</b>  |
|          | <b>SEZNAM POUŽITÉ LITERATURY.....</b>                             | <b>95</b>  |
|          | <b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>                    | <b>99</b>  |
|          | <b>SEZNAM OBRÁZKŮ .....</b>                                       | <b>102</b> |
|          | <b>SEZNAM TABULEK.....</b>  | <b>104</b> |
|          | <b>SEZNAM PŘÍLOH.....</b>   | <b>105</b> |



## ÚVOD

Pocit bezpečí je jednou z nejdůležitějších vlastností napříč celým vývojem lidské populace, jen namátkově lze připomenout z minulosti zajištění přístřešků v přírodě, vyhledávání vhodných a bezpečných míst k přenocování nebo přebývání. Stavba a vyhledávání skrýší před nepříznivými vlivy počasí a zvířaty byla na denním pořádku. S rychlým nárůstem moderní techniky se bohužel rozvíjí i trestná činnost související nejen s krádežemi a vloupáním, čímž se obecně zvyšuje kriminalita. Krádeže a vloupání jsou nejčastější trestnou činností na světě, bohužel to tak bylo, je a bude. Většina pachatelů se v dnešní době nespokojí s málem, tudíž se zaměřují především na společnosti, které disponují větším kapitálem.

Zabezpečení výrobního podniku musí být provedeno s ohledem pro danou organizaci, která se pohybuje v určitém odvětví. Zvolená společnost pro tuto diplomovou práci se konkrétně specializuje na strojírenský průmysl. Jedná se tedy o objekt se specifickým provozem a zaměřením a bude nutné se s ním podrobně seznámit. Informace získané o společnosti jsou důležitým faktorem při pozdějším návrhu zabezpečovacího systému. Návrhy zabezpečovacích systémů jsou specifické tím, že je třeba řešit každý objekt zabezpečení individuálně. Vnitřní a vnější vlivy, na které se při návrhu zabezpečení upírá velká pozornost, působí pokaždé s jinou účinností a silou na všechny objekty, budovy a prostory týkající se zabezpečovacího systému. Celková obrana proti těmto vlivům je jedním z požadavků na zabezpečovací systém pro danou společnost. A to v nejvyšší možné míře. Za použití vhodně vybrané techniky je možné hrozby působící na objekt eliminovat.

Mnou zvolené téma diplomové práce jsem si vybral z důvodu studia oboru bezpečnostní technologie, systémy a management na fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně. I proto, že jsou zabezpečovací systémy v dnešní době stále se rozšiřující pro dosažení potřebné úrovně zabezpečení.

## **I. TEORETICKÁ ČÁST**

## 1 TECHNICKÁ OCHRANA OBEJKTU

Mechanické zábranné systémy jsou součástí technické ochrany, která je složena z většího počtu systémů, které jsou na sobě závislé. Pokud navzájem spolupracují, jsou nazývány jako integrované systémy. Cílem těchto systémů je zlepšit opatření a ochranu, aby byl ochráněn majetek před napadením narušitele a zabránění mu v dalším pronikání a páchání výtržností. V nejlepším možném případě úplně eliminovat toto pronikání, což v současné době není možné a proto nám to dává další možnosti jak bezpečnost, ochranu a tyto opatření zlepšit a posunout dále. [1]

Technická ochrana je rozdělena na tyto části [1]:

- mechanické zábranné systémy,
- signalizační a monitorovací zařízení.

### 1.1 Mechanické zábranné systémy

Všechny prvky mechanických zábranných systémů jsou považovány za základní prvky pro ochranu objektů a osob zejména v průmyslu komerční bezpečnosti. Mezi prvky, které jsou řazeny mezi mechanické zábranné systémy, patří všechny ty, které svým principem a použitím zabráňují vniknutím nepovolaných osob do prostor, které jsou určeny pro ochranu těmito prvky. Nebo do objektů, které jsou chráněny různými druhy oplocení, nebo otvory, ať už se jedná o dveřní nebo okenní otvory. Grafické znázornění procesů bezpečnosti v MZS je pro lepší přehlednost znázorněno na obrázku 1. [2], [24]



Obrázek 1 Grafické znázornění procesů bezpečnosti v MZS [2]

Mechanické zábranné systémy tedy poskytují ochranu svou mechanickou pevností. To znamená, pokud je zvolen pevnější a kvalitnější zábranný systém, tedy vyšší stupeň pyramidy bezpečnosti, tím je samozřejmě těžší překonání systému pachatelem. Každý MZS je překonatelný, avšak záleží to právě na tom, který stupeň bezpečnosti je použit, proto je nejdůležitější u mechanických zábranných systémů, když je v jeho souvislostech hovořeno s pojmem „průlomová odolnost“. Průlomová odolnost je tedy čas, který musí být pachatelem vynaložen k překonání systému. Je rozdělena na dobu, která je nutná k překonání otvorových výplní (dveře, okna, mříže) a na dobu nutnou k překonání úschovných objektů (skříně, trezory, atd.). Minimální čas průlomové odolnosti k překonání otvorových výplní je stanovena podle normy ČSN P ENV 1627 a ČSN P ENV 1630, v těchto dvou normách je seznam, který bezpečnostní třídy a pro každou z nich je přidělen minimální čas, který musí prvek vydržet, než bude překonán. Pro úschovné předměty je minimální doba průlomové odolnosti stanovena podle normy ČSN EN 1143-1. [24], [3]

Mezi mechanické prvky jsou zařazeny např.: všechny zámkové systémy, bezpečnostní dveře, mechanické závory, mříže, rolety, bezpečnostní fólie. Tyto zmíněné prvky jsou pro jednoduchost rozděleny do tří typů ochrany, jedná se o [3]:

- prvky obvodové (perimetrické) ochrany,
- prvky plášťové ochrany,
- prvky předmětové ochrany.

### 1.1.1 Obvodová ochrana

Jsou zde brány v potaz prostředky, které svým významem zajišťují bezpečnost pro vyhrazené území a prostor mezi objektem a stanovenou hranicí. Obvod objektu je značen jeho hranicemi, které jsou omezeny bariérami, ať je uvažována umělými (ploty, zdi, zídky) nebo přírodními (vodní toky, živé ploty, houští, keře). Obvodová ochrana je také nazývána jako perimetrická. Tento stanovený perimetr slouží k upozornění na nepovolanou osobu do prostor chráněného objektu, než se dostane ke střeženým objektům. [2]

K obvodové ochraně jsou používány i různé detektory narušení, na které jsou kladeny přísnější nároky vzhledem k svému vnějšímu využití. Dělí se na aktivní a pasivní.

Prvky obvodové ochrany jsou následující [3]:

- ploty,

- zábrany,
- závory,
- retardéry,
- zídky,
- vjezdy a jiné vstupní prostory.

### 1.1.2 Plášťová ochrana

Pod plášťovou ochranou je považováno zabezpečení všech otvorů na střeženém objektu, které zamezují vstupu nepovolaným osobám do objektu. Jedná se zejména o dveře, okna (balkónové, sklepní), vrata, balkóny a větrací šachty. Jak již bylo zmíněno, tak se zabezpečují všechny stavební otvory. Mezi stavební otvory jsou považovány všechny otvory, které mají rozměry obdélníku (400 x 250 mm), elipsy (400 x 300 mm) nebo kruhu o průměru 350 mm. Někdy se u plášťové ochrany setkáváme s pojmem objektová ochrana. [2]

Prvky plášťové ochrany [3]:

- bezpečnostní kování,
- bezpečnostní fólie,
- bezpečnostní a sandwichová skla,
- mříže,
- dveřní křídlo,
- okenice.

### 1.1.3 Předmětová ochrana

U této ochrany je možné se setkat s pojmem individuální ochrana. Pod touto ochranou je myšleno zabezpečení předmětů, úschovných míst, nebo prostorů a to z důvodu zabránění pachatele před odcizením nebo nepovolenou manipulací s předměty, které jsou zabezpečovány (peníze, cennosti, utajované skutečnosti, šperky, umělecká díla, atd.). V podstatě cílem předmětové ochrany je zabránění před odcizením předmětů, které mají určitou hodnotu, díky které jsou zabezpečovány. [2]

Prvky předmětové ochrany [3]:

- mobilní a stabilní trezory,
- sejfy,
- trezorové skříně,

- příruční pokladny,
- manipulační schránky,
- přenosové kontejnery,
- bezpečnostní kufry,
- zámky.

## 2 SIGNALIZAČNÍ A MONITOROVACÍ ZAŘÍZENÍ

Za větší rozmach signalizačních a monitorovacích zařízení mohl revoluční rozvoj techniky a především elektroniky, který nastal v 90. letech minulého století. Do té doby se hojně využívalo MZS, které patřilo právě za jeden z nejstarších typů ochran. Avšak s vzrůstajícím rozvozem elektroniky se od MZS postupně ustupovalo a začala se psát novější a modernější éra používáním bezpečnostních systémů, které v sobě integrují elektronické prvky. Jsou-li využívány detektory, nebo kamery, je možno detekovat pohyb a pácháání narušitele proti chráněnému objektu. Aby pácháání narušitele bylo mnohem více eliminováno, jsou v kombinaci s detektory a kamerami používány přístupové systémy. Nebezpečí ovšem není vyvoláno jen osobou, ale je zde počítáno i s nebezpečím vyvolaným přírodou, nebo požárem, který vyvolávají jisté chemické reakce. Proto se zde musí počítat s prvky požární ochrany, zejména různými druhy hlásičů. Nejdůležitější je pro tyto systémy norma ČSN EN 50 130. [3], [4], [5]

Signalizační a monitorovací zařízení je rozděleno do kategorií podle funkcí a vlastností, jsou to [5]:

1. poplachové zabezpečovací a tísňové systémy – PZTS,
2. elektronická požární signalizace – EPS,
3. kamerové systémy – CCTV,
4. přístupové systémy – ACS,
5. dohledové přijímací a poplachová centra – DPPC.

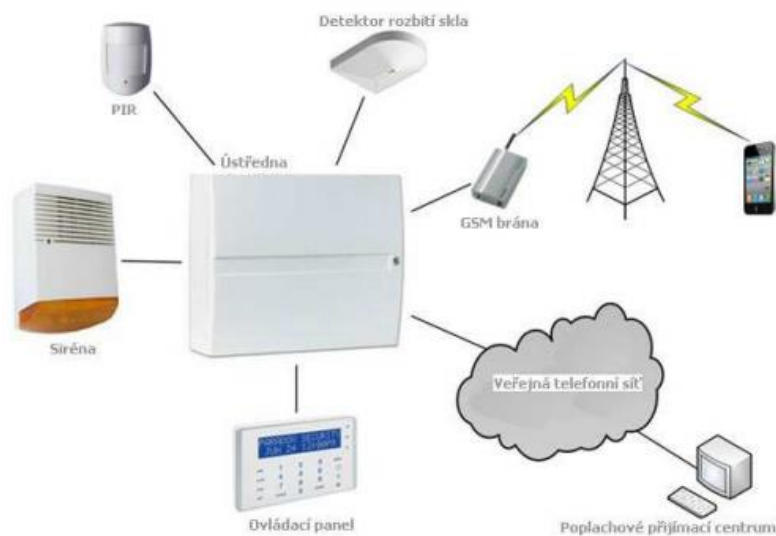
### 2.1 Poplachové zabezpečovací a tísňové systémy

U poplachových zabezpečovacích a tísňových systémů je nutné si dávat pozor hlavně na zkratky, které se často mění a taktéž na normy, které jsou nedílnou součástí PZTS. V minulosti bylo možno se setkat se zkratkou EZS, která nejdřív znamenala „elektrická zabezpečovací signalizace“, následně zkratka zůstala stejná, avšak změnil se název na „elektrické zabezpečovací systémy“. Zkratka PZTS je podle českého překladu z anglické zkratky I&HAS, která znamená Intruder and Hold-up Alarm System. [1], [6], [24]

PZTS jsou určeny pro signalizaci nebezpečí, které se vyskytlo v chráněném objektu. Jak z názvu vyplývá, jedná se o kombinaci dvou systémů – systém k detekci poplachu vniknutí a systém tísňového poplachu. Tyto dva systémy upravuje nová, podle které se tyto systémy

řídí, ČSN EN 50-131-1. Poplachový zabezpečovací systém je součástí technické ochrany a je rozdělen do kategorií, podobně jako u prvků MZS, avšak s pár odlišnostmi [6]:

- obvodová ochrana,
- plášťová ochrana,
- prostorová ochrana,
- předmětová ochrana a
- tísňová ochrana.



Obrázek 2 Schéma PZTS [6]

Na obrázku 2 je znázorněno schéma PZTS s prvky, které mohou být připojeny k ústředně. Důležitým kritériem u PZTS jsou stupně zabezpečení, podle kterých jsou jednotlivé prvky rozděleny. Všechny čtyři rizika jsou rozděleny podle míry rizika od nejmenšího k největšímu a jsou stanoveny v normě ČSN EN 50-131-1. Riziko je odvozeno podle znalostí a vybavení narušitele, pro lepší přehlednost jsou stupně v tabulce 1. [6], [20]



Tabulka 1 Stupně zabezpečení [20]

| Stupeň zabezpečení | Míra rizika       | Typ narušitele  |
|--------------------|-------------------|---|
| 1                  | Nízká             | Narušitel má malou znalost PZTS a k dispozici omezený výběr dostupných nástrojů.  |
| 2                  | Nízká až střední  | Narušitel má znalost PZTS a používá základní nástroje a přenosné přístroje  |
| 3                  | Střední až vysoká | Narušitel je seznámen s PZTS a má k dispozici veškeré nástroje a přenosné elektrické zařízení                             |
| 4                  | Vysoká            | Narušitel je schopen zpracovat plán vniknutí a má kompletní zařízení i prostředky pro náhradu rozhodujících prvků v PZTS. |

Kromě stupně zabezpečení je dalším důležitým pojmem třída prostředí. Klasifikace jednotlivých tříd je podle normy rozdělena a znázorněna v tabulce 2.

Tabulka 2 Třídy prostředí [20]

| Třída | Název prostředí    | Popis prostředí (příklady)  | Rozsah teplot [°C] |
|-------|--------------------|---|--------------------|
| I     | Vnitřní            | Vytápěná obytná nebo obchodní místa   | +5 až +40          |
| II    | Vnitřní všeobecné  | Přerušovaně vytápěná nebo nevytápěná místa (chodby, schodiště, sklady)          | -10 až +40         |
| III   | Venkovní chráněné  | Prostředí vně budov, kde komponenty nejsou vystaveny vlivům počasí (přístřešky) | -25 až +50         |
| IV    | Venkovní všeobecné | Prostředí vně budov, kde jsou komponenty trvale vystaveny vlivům počasí         | -25 až +60         |

### 2.1.1 Přehled prvků

V tabulce 3 tyhle kapitoly, jsou uvedeny jednotlivé prvky, které jsou v souvislosti s PZTS používány.

Tabulka 3 Jednotlivé prvky používané u PZTS [7]

|                                 |                                      |  |  |
|---------------------------------|--------------------------------------|--|--|
| <b>Prvky plášťové ochrany</b>   | Magnetické kontakty                  | <b>Ovládací zařízení</b>               | Blokovací zámky                        |
|                                 | Čidla na ochranu skleněných ploch    |  | Spinací a spouštěcí zámky              |
|                                 | Mechanické kontakty                  |  | Kódové klávesnice                      |
|                                 | Vibrační čidla                       |  | Ovládací a indikační díly              |
|                                 | Poplachové tapety, folie, polepy     |  | Kartové ovládání                       |
|                                 | Drátová čidla                        |  | Klasické smyčkové ústředny             |
|                                 | Rozpěrné tvče                        |  | Ústředny s přímou adresací             |
| <b>Prvky tishňové ochrany</b>   | Veřejné tishňové hlásiče             | <b>Poplachové ústředny PZS</b>         | Ústředny smíšeného typu                |
|                                 | Osobní tishňové hlásiče              |  | Ústředny s bezdrátovým přenosem        |
|                                 | Skryté tishňové hlásiče              |  | Zábleskový maják                       |
| <b>Prvky prostorové ochrany</b> | Pasivní infračervená čidla           | <b>Signalizační zařízení</b>           | Siréna                                 |
|                                 | Aktivní infračervená čidla           | <b>Přenosová zařízení</b>              | Automatické telefonní hlásiče a voliče |
|                                 | Mikrovlnná čidla                     |  | Bezdrátová přenosová zařízení          |
|                                 | Ultrazvuková čidla                   | <b>Prvky venkovní obvodové ochrany</b> | Mikrofonické kabely                    |
|                                 | Duální kombinovaná čidla             |  | Infračervené závory a bariéry          |
| <b>Prvky předmětové ochrany</b> | Otřesová čidla                       | Mikrovlnné bariéry                     |  |
|                                 | Čidla na ochranu zavěšených předmětů | Štěrbinové kabely                      |  |
|                                 | Kapacitní čidla                      | Zemní tlakové hadice                   |  |

- Senzory na ochranu skleněných ploch

Jsou určeny pro ochranu plášťové ochrany a umisťují se zejména na okenní plochy. Princip spočívá ve spojení čidla se sklem. Proto jsou tyto čidla nazývaná jako kontaktní, protože se přímo dotýkají skleněné plochy a rozbití skla, což má za následek vyvolání tříštivého zvuku, který je šířen v tělese a následně je vlnění zaznamenáno čidly, která vyvolají poplach poté, co elektronika vyhodnotí vlnění, které bylo vyvolané prasknutím, nebo rozbitím skla. Další variantou jsou aktivní čidla, která jsou určeny pro nejvyšší riziko ohrožení, které obsahují přijímač a vysílač. Výhodou těchto čidel je, že mohou střežit až 25 m<sup>2</sup> velkou plochu, což představují objekty větších průmyslových hal a firem. V našich krajinách je

rozšířena poslední varianta čidel a to akustická, u kterých elektronika vyhodnotí akustických efekt elektretovým mikrofonom, namísto vlnění, tak jak to bylo u předchozích variant. Přijímačem se u akustických senzorů myslí elektretový mikrofón. [12], [23], [24]

- Ultrazvukové senzory

K plnění funkce využívají část mechanického vlnění. Jedná se o aktivní senzory, což znamená, že vysílají do chráněného prostoru vlnění, které je stálé a přijímač dostává zpět vlnění od různých překážek v takovém prostoru. Je-li v prostoru vysílání vlnění těleso, které zapříčiní změnu vlnění. Celý princip je založen právě na vyhodnocení změny vlnění elektronikou, jde o aplikaci Dopplerova jevu, který je dán vztahem [12]:

$$f_1 = \frac{f}{1 - \left(\frac{v}{c}\right)^2} \quad (1)$$

kde  $f_1$  [Hz] je přijaté vlnění,  $f$  [Hz] je vysílané vlnění,  $v$  [m/s] je rychlost pohybu odrazné plochy a  $c$  [m/s] je rychlost pohybu vlnění užitého k detekci. Ultrazvukové senzory jsou svou funkcí vhodné k prostorové ochraně.

- Osobní tísňové hlásiče

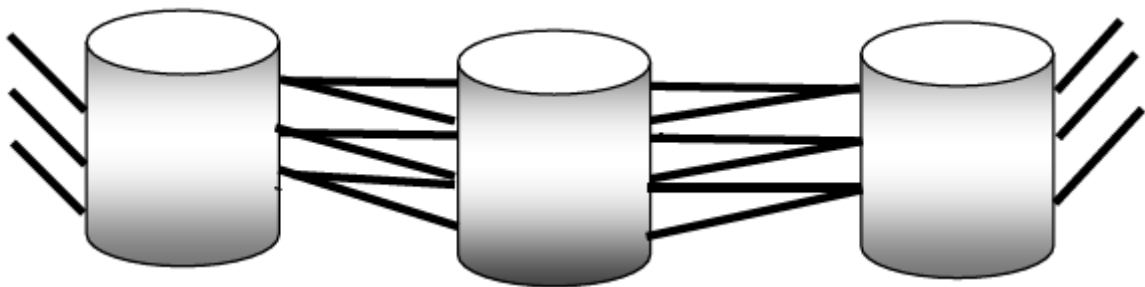
Spadají mezi prvky tísňové ochrany a dělí se na veřejné, speciální, automatické a osobní. Osobní tísňové hlásiče jsou bezdrátové, u kterých je vysílačem vyslaný signál do prostoru a nastaven na shodnou frekvenci přijímače, tak aby jej mohl přijímat. U tísňových hlásičů je využíváno zejména pásmo 27 MHz, 300 MHz a 400 MHz. Kromě těchto frekvencí existují hlásiče, které jsou založeny na ultrazvukovém principu, tedy na Dopplerově efektu, tak jak tomu je popsáno u ultrazvukových senzorů. Pro zamaskování pro pachatele jsou vyráběny jako podobizny přívěšků, náramků, atd. [12], [24]

- Kapacitní čidla

Jsou brána do kategorie předmětové ochrany a jejich primární funkcí je signalizovat přiblížení a varovat před odcizením chráněného předmětu. Na chráněný předmět působí elektrické pole vyvolané senzorem, nebo je napojen na elektrody. Pachatel, který vstoupí do elektrického pole přiblížením se k předmětu, nebo při snaze o jeho odcizení, změní parametry dielektrika a s tím i nastavený kmitočet oscilátoru. Případné změny jsou vyhodnoceny fázovým detektorem, který následně dává pokyn ke spuštění poplachu. [12], [20]

- Infračervené závory a bariéry

Jsou založeny na principu vysílače a přijímače. Mezi přijímačem a vysílačem může být vysílán jeden jediný paprsek, nebo hned několik, které mohou být i kříženy mezi sebou. Dojde-li k přerušení paprsku, je tato změna vyhodnocena přijímačem a následně vyhlášen poplach. Jedná se o častou variantu používanou v praxi k ochraně perimetru. Dosah je od 50 do 200 metrů. Na obrázku 3 je ukázka možné varianty uspořádání paprsků. [12], [23]



Obrázek 3 Uspořádání paprsků bariéry [12]

- Ústředny PZTS

Ústředny jsou mozkiem celého zabezpečovacího systému. Plní hned několik funkcí [15]:

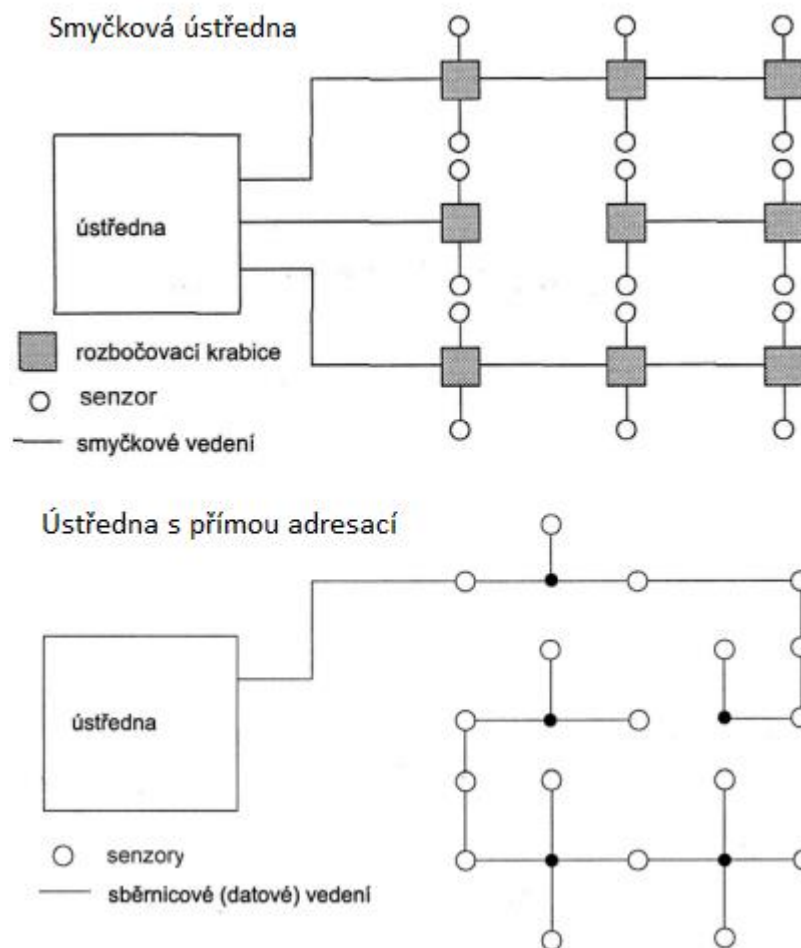
- Přijímají a vyhodnocují signály od senzorů,
- ovládají zařízení se signalizací narušení,
- poskytují napájení prvků,
- ovládají celý PZTS pomocí ovládacích prvků a
- poskytují diagnostiku stavu o PZTS.

Ústředny je možno rozdělit do čtyř základních skupin a to na ústředny [15], [24]:

1. smyčkové – každá smyčka má samostatný vyhodnocovací obvod. Smyčky jsou zakončeny odporem a poplach je vyvolán změnou odporu. Počet smyček se pohybuje v rozmezí jednotek až stovek. Nevýhodou u smyčkových ústředí je rozsáhlá kabeláž.
2. s přímou adresací senzorů – komunikaci senzorů s ústřednou je pomocí datové sběrnice. Každý její senzor má komunikační modul a počet adresovatelných senzorů se pohybuje okolo desítek. Výhodou je, že ústředna rozpozná, který senzor poplach vyvolal a jednoduchá kabeláž, zatím co velkou nevýhodou je v délce vedení.

3. smíšeného typu – komunikace probíhá po datové nebo analogové sběrnici mezi ústřednou a koncentrátorem. Koncentrátorem je myšleno propojení senzorů ve smyčkách.
4. s bezdrátovým přenosem – k přenosu je používáno pásmo 433 MHz, přenos ze senzoru je zde kódovaný z důvodu možného odposlechu. Je využíván na vzdálenost několik stovek metrů. Výhodou bezdrátové přenosu je rychlá instalace snadné rozšíření.

Jak mohou být ústředny zapojeny, je znázorněno na obrázku 4, konkrétně ukázka smyčkové ústředny s ústřednou přímé adresace.



Obrázek 4 Ukázka ústředny smyčkové a s přímou adresací [15]

## 2.2 Elektrická požární signalizace

Elektrická požární signalizace je tvořena souborem prvků, které reagují na výskyt požáru v začínajícím stádiu hoření rychlou identifikací a lokalizací na místě zasaženém požárem. Ne nadarmo je v souvislosti s EPS zmiňováno, že jejím používáním je možné zabránit

vzniku obrovských ztrát, ať už se jedná o materiálové hodnoty, nebo v nejhorším případě o lidské životy, protože s EPS úzce spolupracuje HZS příslušného kraje, okresu. V případě signalizace požáru, je na místo jeho vzniku vyslán HZS kraje, který následně zasahuje na místě. Velkou výhodou EPS je, že může aktivovat návazné zařízení, které se samy podílí na protipožární opatření. [7], [8], [23]

Elektrická požární signalizace je tvořena pomocí ústředny, hlásičů a koncových zařízení. EPS informuje akustickou a vizuální formou v objektu, nebo pomocí dálkového přenosu na příslušné dohledové poplachové a přijímací centra umístěné u HZS. Detekce požáru je zajištěna pomocí detektorů, které jsou založeny na různých principech. Důležitou vlastností EPS je, aby kromě signalizace vzniku požáru dávala signál zařízení, které zabraňují rozšíření požáru po celém objektu (větrací zařízení, stabilní hasicí zařízení, dveře, vrata, atd.). [8], [1]

Elektronickou požární signalizaci je možno si vybrat ze tří systémů [8]:

- Konvenční – možno připojit více hlásičů na smyčku, ale ústředna nerozpozná, který konkrétní hlásič vyvolal poplach, jen ví o poplachu na smyčce.
- Adresovatelné – o poplachovém stavu rozhoduje sám hlásič, zde ústředna ví, podle adresy hlásiče, který poplach vyvolal. Adresace se provádí pomocí rezistoru, nebo datové komunikace.
- Analogové – hlásiče provádí měření fyzikálních veličin, výsledky jsou zaslány na ústřednu, která rozhodne o poplachu.

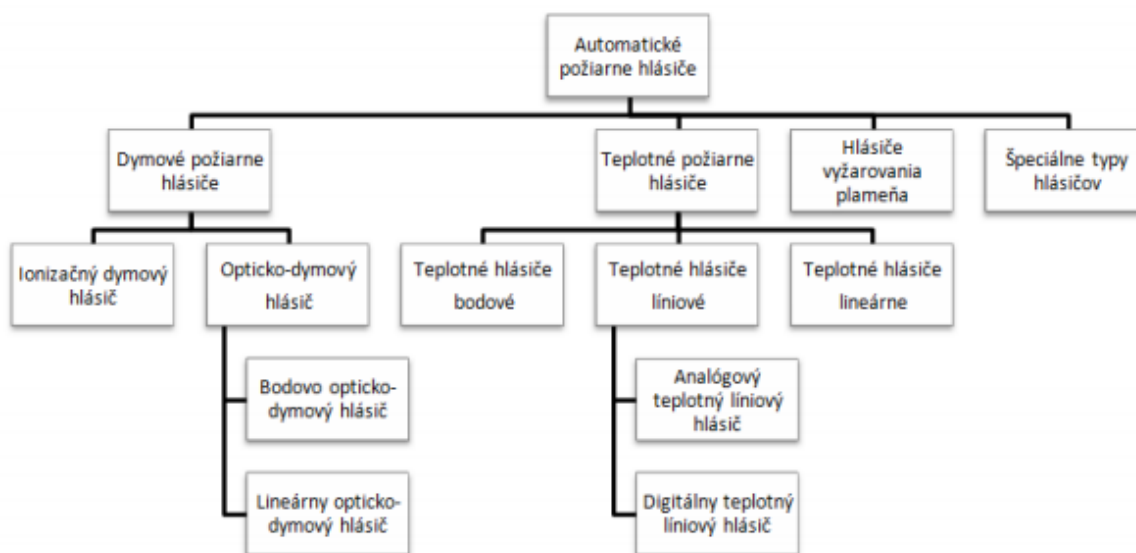
### 2.2.1 Dělení hlásičů

Podle principu jsou hlásiče rozděleny do dvou velkých skupin [9]:

1. Tlačítkové požární hlásiče.
  2. Samočinné požární hlásiče.
- **Tlačítkové požární hlásiče** jsou převážně umístovány do prostor, kde je stálá přítomnost personálu. Lze je dle způsobu aktivace rozdělit na dva druhy, tlačítkové hlásiče s přímou obsluhou a nepřímou obsluhou. U hlásičů s přímou obsluhou dochází ke spuštění poplachu následujícím způsobem – osoba, která zjistí vznik požáru nebo jiné nebezpečí, rozbije sklo a tím dochází k samočinnému sepnutí funkčního tlačítka, pomocí kterého je vyvolán poplach U hlásičů s nepřímou obsluhou, je poplach vyvolán stiskem tlačítka po rozbití skla. Rozdíl mezi přímou a nepřímou obsluhou je takový, že u hlásičů přímé obslu-

hy dochází k aktivaci spínače ihned s rozbitím skla, zatímco u hlásičů s nepřímou obsluhou musí být nejdříve rozbito sklo a poté teprve stisknuto tlačítko. Pokud byl spínač stlačen, byl automaticky vyslán poplachový signál na ústřednu. Aby ústředna mohla zjistit, který hlásič byl stisknut, jsou tyto hlásiče přímo adresovatelné. [9], [10], [23]

- **Samočinné hlásiče požáru** jsou založeny na sledování fyzikálních veličin a při určité změně fyzikálních parametrů souvisejících se vznikem požáru v místě instalace, nezávisle na lidském činiteli, jsou uvedeny v poplach. Jsou založeny na reakci změny teploty dýmu, plamene nebo jejich vzájemnou kombinaci. Jak už název napovídá, k aktivaci hlásičů není potřeba lidský faktor. Samočinné hlásiče jsou následně rozděleny podle celé řady kritérií, což je znázorněno na obrázku 5. [1], [8]



Obrázek 5 Dělení samočinných požárních hlásičů [8]

- Hlásiče kouře – ionizační

Detekce kouře je založena na vyhodnocení změny vodivosti ionizovaného plynného prostředí detekční komůrky. Je vhodný pro zjišťování požárů, které při hoření produkují viditelné i neviditelné zplodiny. Při ionizačním procesu je přeměněn neutrální atom nebo molekula na iont. V běžném stavu je vzduch ionizovaný, což je vlivem elektrického pole mezi elektrodami. V případě požáru, když se dostane dým mezi elektrody, dochází ke zpomalení iontů a následnému snížení proudu. [10], [23]

- Hlásiče kouře – optické

Konstrukce optický hlásičů je navržena dle efektu přítomnosti pevných částic kouře, které jsou vygenerovány průběhem požáru, dvěma způsoby. První způsob je založen na vyhod-

nocování rozptylu optického paprsku a druhý na vyhodnocování pohlcování optického paprsku. Existují optické hlásiče lineární a bodové. [23], [10]

Bodové optické hlásiče kouře jsou založeny právě na principu rozptylu světla. Ve stavu bez kouře laserový paprsek nedopadá na citlivý paprsek, který je oddělen labyrintem. Při požáru vniká kouř do labyrintu, což má za následek rozptyl paprsku, který dopadá na fotodiody, při opakovaném dopadu na diodu je vyhlášen poplach. [10], [9]

Lineární hlásiče jsou založeny na principu vyhodnocení změny intenzity světla paprsku. Skládá se z přijímače a vysílače, který tvoří infračervený laser. Vzdálenost mezi přijímačem a vysílačem může být až 100 m. [9]

- Hlásiče teplot

Princip teplotních hlásičů je založen na vyhodnocení změny teploty v místech instalace, vyvolaných uvolněným teplem v důsledku hoření. Teplotní hlásiče jsou rozděleny na bodové, lineární a liniové (analogové a digitální). [10]

Bodové hlásiče teplot jsou založeny na měření a vyhodnocení změn teplot v místě instalace pomocí termistoru. Vyhodnocení signálu se provádí z hlediska překročení maximální teploty v prostoru, pomocí statického hlásiče, nebo z překročení maximální přípustné rychlosti nárůstu teploty, což obstarává diferenciální hlásič. [9], [10]

Lineární hlásiče teplot jsou založeny na vyhodnocování modulační frekvence IR paprsku, který prochází přes střežený prostor z vysílače do přijímače. Reaguje tedy na rozdíl teplot a hustotu indexu lomu vzduchu. Tyto změny má za následek turbulentní proudění. [10]

- Hlásiče plamene

Jsou založeny na principu detekce požáru na základě vyhodnocování jistých vlastností radiace plamene při požáru. Při detekci plamene pracují s těmito parametry – vyzařování, spektrální charakter vyzařování a frekvence oscilace plamene. Výhodou těchto hlásičů je doba reakce na vzniklý požár za podmínek, že jsou hlásiče správně instalovány. [10]

Hlásiče plamene lze podle oblastí elektromagnetického spektra rozdělit do několika kategorií [10]:

- infračervené (IR) hlásiče plamene,
- ultrafialové (UV) hlásiče plamene,
- kombinace IR s UV hlásiče plamene.



### 2.3 Kamerové systémy

Kamerový systém je tvořen kamerovou soustavou, zobrazovacích a přídavných zařízení, které jsou důležité zejména kvůli přenosu signálu a na obsluhu při monitorování určených chráněných zón. Kamerová soustava v sobě zahrnuje kameru, která má svůj vlastní objektiv a další potřebná příslušenství. Za kameru je považován optický snímač, ať už CCD (Charge Coupled Device) nebo CMOS (Complementary Metal Oxide Semiconductor), který vytváří videosignál z optického obrazu. O dalších prvcích kamerového systému bude psáno později. [11], [23]

Kamerové systémy a jejich prvky jsou zařazeny dle jednotlivých stupňů podle požadované bezpečnosti, která je vyžadována. Jak již bylo zmíněno v předcházející kapitole, existují čtyři stupně zabezpečení, které se označují jako nízké, nízké až střední, střední až vysoké a vysoké riziko. Na kamerové systémy jsou kladeny požadavky, podle toho, do kterého stupně jsou řazeny. Jde o následující požadavky [11]:

- ukládání dat,
- archivace a zálohování,
- záznam událostí,
- monitorování připojení,
- detekci sabotáže,
- přístupové úrovně,
- autorizační kód,
- přístup k datům,
- přístup systémovým protokolům,
- přístup k nastavení systému,
- identifikaci dat.

Mezi další požadavky, které musí kamerové systémy splňovat, patří řád norem, tak jako je to u všech elektrických zařízení jsou to požadavky na [11]:

- elektrickou bezpečnost,
- elektromagnetickou kompatibilitu,
- odolnost proti klimatickým a mechanickým vlivům prostředí.

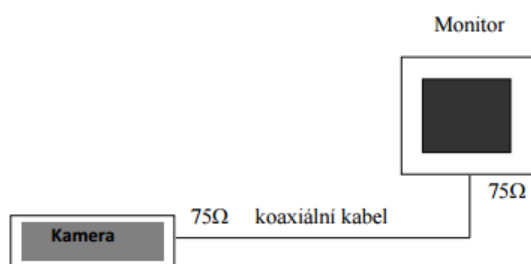
Kamerové systémy byly v počátku zejména navrženy podle toho, aby plnily čtyři funkce – identifikaci, rekognaskaci, monitorování a detekci osob a předmětů. V současnosti jsou

však inteligentní kamerové systémy schopny plnit mnohem širší úhel možností. Zejména jde o detekci podezřelého chování osob, přičemž kamery jsou zaměřeny na nesprávný směr pohybu, rychlou chůzi, výtržnictví. Jako další možnost využití je biometrická verifikace osob, sledování osob, jejich teplot na letištích, rozpoznávání předmětů, identifikaci evidenčních čísel vozidel, sledování a vyhodnocování nehod. [11], [20]

### 2.3.1 Přenosy signálu

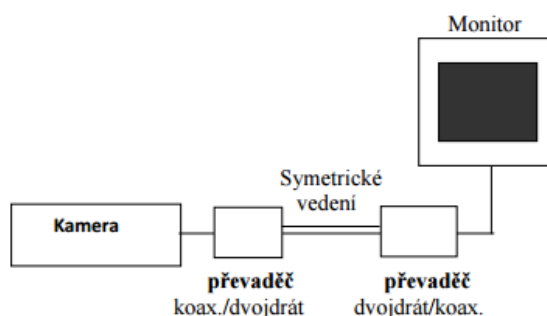
Kamerové systémy jsou navrženy dle několika základních druhů a typů přenosu, které jsou popsány a pro lepší představu znázorněny pomocí obrázků níže.

- Přenos pomocí koaxiálního kabelu (nesymetrický) – přenos pomocí koaxiálního kabelu je nejčastější způsob přenosu, který má však několik nevýhod. Nevýhodou může být omezený přenos na 70 až 300 m, také galvanické propojení vzdálených prvků, kde se může vyskytovat brumový pás. [12]



Obrázek 6 Nesymetrický přenos bez korekčního zesilovače [12]

- Přenos přes kroucený pár (symetrický) – na rozdíl od nesymetrického vedení, je přenos u symetrického rozšířen až na desítky kilometrů. Jde o dvojici vodičů telekomunikačního kabelu, který je kroucený. I zde jsou podobné nevýhody, jako u nesymetrického přenosu, avšak symetrický přenos se může pyšnit vyšší odolností proti rušení. [12], [20]



Obrázek 7 Symetrický přenos [12]

- Bezdrátový přenos – je schválen podle normy na tři pásma – pásmo telemetrie, které pracuje na frekvenci mezi 433 až 868 MHz, druhé pásmo pracuje na frekvenci 868 MHz až 2,45 GHz, zde je větší směrová účinnost a třetí pásmo, které využívají například antény YAGI, pracuje na frekvenci 10 GHz a větších. [12]
- Infračervený přenos – IR přenos je určen jen na malou vzdálenost, který ovlivňují povětrnostní podmínky. [12]
- Přenos po optickém vlákně – výhodou optického přenosu jsou nízké ztráty a dochází zde jen zřídka k elektrickým narušením. Přenos po optice je možný až do vzdálenosti 50 km, další výhodou je nízká pořizovací cena. [12]

### 2.3.2 Snímače obrazu

V současnosti jsou kamerové systémy využívány hojně k ochraně osob a majetku, neodmyslitelně jsou kamery nejdůležitějším prvkem těchto systémů. Princip kamery je takový, že světlo prochází objektivem a dopadá na snímací čip, což je způsobeno soustavou zrcadel. Snímací čipy jsou polovodičové a to zejména CCD, CMOS a DPS, přičemž pracují na odlišném principu, což je popsáno uvnitř podkapitoly. [14], [12], [11]

- **CCD snímače**

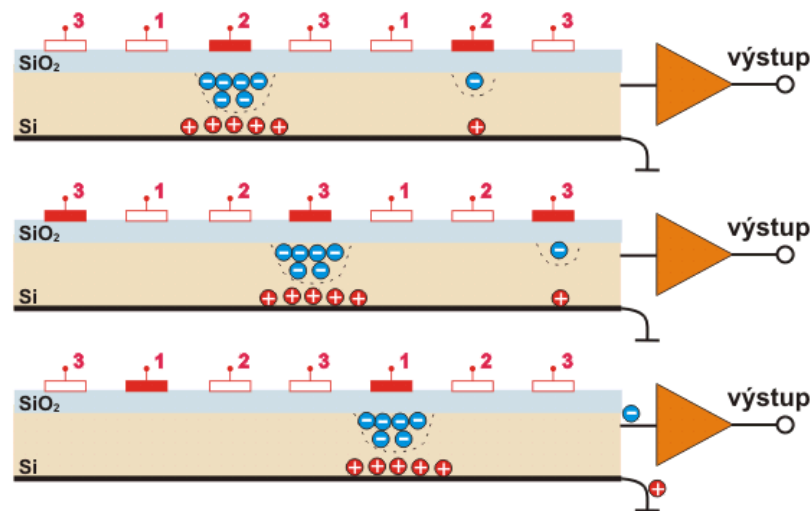
Počátky používání těchto snímačů jsou zakotveny na začátek 80. let, kdy si od nich firmy slibovaly menší rozměry, delší životnost a vysokou citlivost. Z anglického „Charge Coupled Device“, je fotocitlivý polovodičový prvek, ve kterém je přeměna dopadajícího světla na elektrický náboj, který je po následném měření převeden do digitální podoby. [11], [14]

Princip činnosti snímačů je založen na fotoelektrickém jevu, kde jsou díky dopadajícímu elektromagnetickému záření uvolňovány elektrony z látek. Uvolněné elektrody jsou pomocí vodivých elektrod schopny se podílet na elektrické vodivosti. Na přiložených elektrodách je tenká vrstva oxidu křemičitého, který se chová jako skvělý izolant v polovodičích. Ten zabraňuje v odvedení elektronů, které byly uvolněny v důsledku fotoelektrického jevu, pryč. To vše se děje proto, že je tím docíleno k akumulaci náboje, přičemž jeho velikost je závislá na intenzitě dopadajícího světla a dobou, po kterou světlo dopadá na snímač. [12]

Činnost CCD snímače je možná shrnout do třech kroků a jeho princip je zobrazen na obrázku 8 [11], [14]:

1. Přípravná fáze – fáze, kdy na CCD nedopadá světlo.

2. Expozice obrazu – elektrody jsou pod napětím a CCD snímač vystaven světlu. Následně jsou uvolněny elektrony, přitažené ke kladným elektrodám.
3. Snímání obrazu – po konci 2. kroku, je přiveden na 1., 2. a 3. elektrodu tří hodinový signál – zvyšování napětí na 2. elektrodě a snižování na 1. elektrodě. To samé je potom i mezi 2. a 3. elektrodou a mezi 3. a 1.



Obrázek 8 Princip snímání obrazu [13]

- **CMOS snímače**

Snímače CMOS, z anglického „Complementary Metal Oxide Semiconductor“, jsou principem velmi podobné CCD snímačům. Kde je každá buňka snímače, která je u CMOS tvořena fotodiodou, citlivá na dopadající světlo, kterému je vystavena a je generován náboj, který je přímo úměrný paprskům, které dopadají na fotodiodu. [11], [12], [23]

Původní požadavky na CMOS snímače byly takové, aby byly jednoduše navrženy a hlavně pořiditelné za nižší cenu, znamenalo to tedy nízké výrobní náklady, s malými rozměry jednoduchá konstrukce a důraz na nízkou spotřebu energie. Na druhou stranu to znamenalo menší kvalitu, což se podepsalo v masivním rozšíření používání, které se omezilo na web kamery a kamery v mobilních zařízeních. Pokud je používá některý výrobce u profesionálních kamer, tak jsou buňky doplněny o obvody, které potlačují šum. [11], [14]

- **DPS snímače**

Snímač DPS, z anglického „Digital Pixel System“, ke své činnosti používá systém pro snímání a zpracování obrazu, který na rozdíl od CMOS snímačů, poskytuje velmi vysokou kvalitu obrazu, která je zlepšená dynamickým rozsahem (WDR – Wide Dynamic Range). To má velký význam ve využívání v bezpečnostních oblastech, kde je zapotřebí přenášet

kvalitní obraz i v malých prostorách, které mohou být málo osvětleny. Základem DPS snímačů je A/D převodník, který je pro každou buňku samostatný. Převodník převádí signál do digitální podoby, ihned po nasnímání a načtení obrazu. Tato výhoda spočívá v tom, že je snížen šum v obraze. Kamery, které jsou založeny na principu DPS snímačů, jsou složeny z několika tisíců kamer, poskytující ten nejlepší obraz. [14], [12], [24]

### 2.3.3 Technické parametry kamer

Mezi technické parametry kamer je možno zařadit rozlišovací schopnost, poměr stran obrazu, citlivost, dynamický rozsah, napájení kamer a řídicí vstupy kamer. Parametry jsou popsány uvnitř podkapitoly. [11]

- Rozlišovací schopnost

Závisí na velikosti senzoru a počtem pixelů (aktivních buněk). Kvalita obrazu a snižování šumu je právě závislé na rozlišovací schopnosti. Udává se buď v pixelech, nebo v televizních rádcích a platí, že čím větší rozlišovací schopnost, tím větší detaily je schopné zobrazit. Rozlišovací schopnost je možné rozdělit na standardní a vysokou rozlišovací schopnost. [12]

- Poměr stran obrazu

Jedná se o poměr mezi vodorovnou a svislou stranou obrazu. K běžně používaným poměrům stran (3:2, 4:3 a 5:4) se přidaly další formáty (16:9 a 15:9). Nejčastější rozlišení a jejich poměry stran jsou následující – u rozlišení 640 x 480, 800 x 600, 1024 x 768 a 1600 x 1200 je poměr stran 4:3. Poměr stran 5:4 je u rozlišení 1280 x 1024. U poměru stran 15:9, který patří mezi novější formáty, je u rozlišení 1024 x 576. Rozlišení 1280 x 720 má poměr stran 15:9 i 16:9. [14], [11]

- Citlivost

Základní jednotkou citlivosti je lux a citlivost nám vyjadřuje hodnotu osvětlení, která je potřebná k vytvoření výstupního signálu. Minimální osvětlení není přesně dáno. Citlivost je dána vztahem, který vyjadřuje, že čím je větší citlivost, tím větší je i šum signálu. [11]

- Dynamický rozsah

Parametr, který zobrazuje rozdíl mezi nejsvětlejším a nejtmavším místem na snímaném obrazu. Zobrazuje počet odstínů od černé po bílou barvu, který může snímač rozlišit. Dynamický rozsah je určen v jednotkách EV, a znamená rozdíl mezi nejtmavším a nejsvětlej-

ším místem. Jestliže je 16 EV světel a 10 EV stínů, tak dynamický rozsah je rozdíl těchto EV, tudíž 6. [14]

- Napájení kamer

Napájení je určeno výhradně výrobcem kamer, běžně je použito 12V stejnosměrného napětí a 12 nebo 24V střídavého napětí. Pokud jsou to kamery, které jsou pevně instalovány, používá se u nich napětí 230V/50Hz. [12]

- Řídící vstupy kamer

Ke komunikaci se vstupy kamer, které převážně slouží k ovládní objektivu kamery, jsou využívány počítačové konektory kabelů RS 232, RS 422 a RS 485. Nejčastěji je využíván kabel RS 232, protože konektor potřebný k jeho připojení obsahuje každý počítač, avšak je zde omezena vzdálenost na 15 m. Zbývají linky, jsou používány především na větší vzdálenosti, až do 1,5 km a další výhodou je, že se mohou větvit. [14]

## 2.4 Přístupový systém

Přístupový systém vstupu ACS (ACCESS), někdy je také nazýván jako systém kontroly vstupu (SKV), a je možno si pod tímto pojmem představit skupinu opatření, která jsou používána ke kontrole vstupu a taky pohybu osob uvnitř chráněného prostoru. Do skupiny opatření jsou zařazeny systémové, fyzické, elektronické a mechanické. Kontrola vstupů umožňuje velké objekty dělit do zón a zaměstnancům díky tomu poskytovat vstup jen tam, kde mají určeno vstoupit a další velkou výhodou je možnost zjištění jak dlouho se v dané zóně pohybují. [1], [7]

U přístupového systému jde hlavně o identifikaci osob, které chtějí vstoupit do prostoru. Access má tyto základní funkce [1]:

- identifikaci,
- zpracování dat,
- ovládní přístupového místa,
- programovatelnost,
- stav hlášení,
- komunikace,
- napájení,
- samo ochrana.

V souvislosti s přístupovým systémem je nutno rozlišit jej s pojmem docházkový systém. U obou systémů jde o identitu zaměstnanců, avšak u docházkového systému je hlavní funkcí monitorování zaměstnanců, hlavně pak pracovní doby a povinné přestávky. Oba systémy mohou být integrovány v jeden ucelený systém, kdežto přístupových bodů je v chráněném prostoru několik, zatímco docházkový bod je převážně jen u hlavního vstupu do střeženého prostoru. [16], [23]

#### 2.4.1 Identifikace uživatele

Jestliže má být zaměstnanec, nebo osoba identifikována, lze to učinit následujícím způsobem [16]:

- Na základě paměti – heslem, kódem, otázkou (autentizace heslem).
- Na základě předmětu – kartou, přívěškem, ovladačem RF (autentizace předmětem).
- Na základě osobních rysů – biometrie (biometrická autentizace).

V dnešní době s rychlým růstem moderních technologií existuje několik prvků, které se dělí podle různých kritérií, hledisek, snímacích zařízení (kontaktní nebo bezkontaktní), principů. Níže jsou popsány nejčastěji používané identifikační prvky [16], [1]:

- Manuální – vypínače, kódové zámky. Manuální prvky potřebují manuální vstup osoby
- Čipové – dělí se na kontaktní, bezkontaktní a kombinované, umožňují čtení i zápis.
  - Kontaktní – SmartCards, iButton.
  - Bezkontaktní – čipové karty, přívěšky, RFID karty.
  - Kombinované – kombinace kontaktu a bez kontaktu v prvku – přívěsek, klíč, karta.
- Magnetické – karty, které obsahují magnetický pruh.
- Optické – čárové kódy, CCD a laserové čtečky.
- Radiofrekvenční – bluetooth, pracují v pásmech 434 a 868 MHz a 2,4 GHz
- Biometrické – otisk prstu, krevní řečiště, duhovka, sítnice.



Obrázek 9 SmartCard [17]

Podle následujících tříd identifikace v tabulce 4, která znázorňuje rozdělení a příklady prvků, je určen stupeň zabezpečení pro každý prostor, kde se nachází přístupový bod.

Tabulka 4 Třídy identifikace [1]

| Třída identifikace | Identifikace založená na:              | Příklad identifikačního prvku                           |
|--------------------|--|---|
| <b>0</b>           | nepřímé identifikaci                   | Tlačítko, kontakt, pohybový detektor                    |
| <b>1</b>           | datech v paměti                        | Heslo, číslo zaměstnance                                |
| <b>2</b>           | identifikačních prvcích, vč. biometrie | Karty, přívěšky, čip, otisk prstu, krevní řečiště, atd. |
| <b>3</b>           | kombinace 1. a 2. třídy                | Biometrický prvek + heslo                               |

#### 2.4.2 Způsoby přístupu

Tak jako jsou popsány v podkapitole „Identifikační prvky“ prvky pomocí kterých se zaměstnanci identifikují, je nutné se zmínit o způsobech přístupu, které povolí, nebo zamítnou přístup jednotlivých osobám, podle toho jestli správně, či nesprávně prokáží svou identitu. Způsoby přístupu jsou následující [16]:

1. klávesnice,
2. karty,
3. čipové vstupy,
4. hands free,
5. vstupní a signalizační čidla,
6. kamery,
7. biometrie.

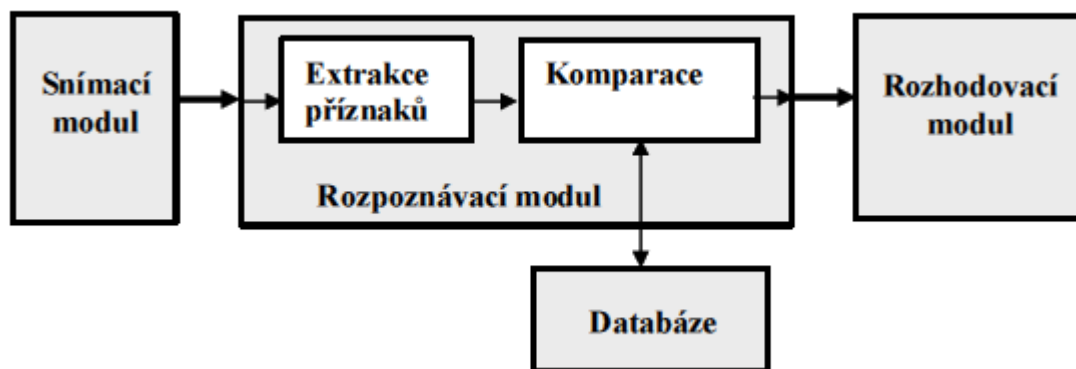


Přičemž nejčastější způsob přístupu v praxi je používán kartový systém, který se dělí dle funkce, způsobu použití a podle typu karet.

- Dle funkčního média [16]:
  - karty s magnetickým kódem,
  - karty s čárovým kódem,
  - karty s čárovým kódem dvojrozměrným,
  - karty s mikročipovým kódem.
- Podle použití [1]:
  - kontaktní,
  - bezkontaktní.
- Podle typu karet [1]:
  - A – platební,
  - T – telefonní,
  - Z – kontroly přístupu.

### 2.4.3 Biometrické systémy

Patří mezi nejmladší identifikační systémy, které jsou založeny na identifikaci osob jejich charakteristických znaků, které znázorňují jedinečnost a osobitost každého člověka. Tyto fyziologické, či behaviorální znaky jsou snímány, zpracovány, porovnány s uloženými daty v databázi a nakonec vyhodnoceny. Biometrické systémy jsou schopny pracovat ve dvou módech, identifikační a verifikační. U identifikačního jsou znaky snímány a porovnány se všemi daty uloženými v databázi, aby byla zjištěna identita osoby. U verifikačního módu osoba zadá svou identitu a po následném získání znaků jej systém porovná s uloženými, a buď přístup odmítne, nebo povolí. Na obrázku 10 je znázorněn princip biometrických systémů podle bloků, které znázorňují jednotlivé moduly systémů. [16], [20]



Obrázek 10 Princip biometrických systémů [18]

Přístupové a docházkové systémy, které ke své funkci a větší bezpečnosti využívají biometriku, k ověření nejsou potřebné žádné nosné předměty (karty, klíče, čipy). V tom je velká výhoda, protože u systémů, které k ověření a přístupu vyžadují některý z uvedených předmětů, je velká možnost ztráty předmětů. Naopak nevýhoda systémů, které kombinují biometriku, je ve velkém výkonu systémů a vysoké pořizovací ceny. Proto se přístupové systémy s biometrikou používají převážně u nejvyššího stupně ochrany. [16], [24]

- Rozdělení biometrických znaků

Snímání biometrických znaků je rozděleno do dvou kategorií, fyziologické a behaviorální znaky (tabulka 5). Fyziologické znaky má člověk od narození a jsou neměnné, zatímco behaviorální znaky jsou rysy chování člověka a u každého jedince se vyvíjí časem. [16]

Tabulka 5 Rozdělení biometrických znaků [16]

| Fyziologické znaky  |                                  | Behaviorální znaky     |
|---------------------|----------------------------------|------------------------|
| Otisk prstu         | Krevní řečiště                   | Dynamika chůze         |
| Geometrie ruky      | Rýhování nehtů                   | Hlas                   |
| Rozpoznání obličeje | Tvar ucha                        | Dynamika podpisu       |
| Oční duhovka        | Pach                             | Dynamika stisku kláves |
| Oční sítnice        | Deoxyribonukleová kyselina (DNA) | Dynamika pohybu myši   |

### 3 ZABEZPEČOVACÍ SYSTÉMY

Účelem zřizování zabezpečovacích systémů je poskytování ochrany požadovaného objektu. Pod ochranou se rozumí pevné prostředí, v kterém jednotlivé osoby, nebo skupiny mohou bez jakéhokoliv narušení, ohrožení a hrozbou násilí, vykonávat svou práci svědomitě a poctivě. V dnešní době je trend zřizování integrovaných systémů, pod které spadají technické prvky, které jsou vzájemně propojeny. Mezi tyto technické prvky jsou řazeny mechanické zábranné systémy a monitorovací a signalizační zařízení, které byly popsány v kapitolách 1 a 2. Mezi ně spadá i organizační opatření s ostrahou. [19], [23]

Systémy poskytují jakýsi soubor opatření, jež jsou vymezovány pro zajištění určité bezpečnosti. Do již zmíněného souboru patří organizační a technicko-taktické opatření, což je vlastně zmiňovaný zabezpečovací systém. Na zabezpečovací systémy je možno nahlížet ze dvou úhlů pohledů, které jsou vzájemně ovlivněny. [19], [24]

- Operační hledisko.
- Technické hledisko.

#### 3.1 Operační hledisko

Operační hledisko, pokud jde o zabezpečovací systémy, je u těchto systémů pro dané subjekty, jež jsou zainteresovány na vybudování zabezpečovacího systému, jiné. To znamená, že nejde přesně popsat cílovou funkci operačního hlediska, protože je pro každý subjekt jiná. Jako zjednodušená cílová funkce operačního hlediska se bere v potaz „vše, co má bezpečnostní systém splňovat“. Proto je na operační hledisko nahlíženo s otázkou, která řeší úroveň propustnosti a okamžité zmírnění škody v pokusech o překonávání systému, tak i s otázkou tykající se ekonomické, společenské a technické efektivnosti. [23], [19]

Je-li zabezpečovací systém soubor již výše zmíněných opatření pro zajištění ochrany nspecifikovaných hodnot před rizikem napadení, je obtížné definovat požadavky na funkci integrovaného zabezpečovacího systému, které mohou ovlivnit efektivnost těchto systémů v boji proti trestné činnosti. Kromě prvotního požadavku systémů – zabránění krádeži, vloupání, zničení nebo poškození, může být zabezpečovací systém ovlivněn dalšími požadavky, kterými jsou [23], [19]:

- posílení obranyschopnosti zabezpečovacího systému,
- vytvoření ideálních podmínek pro dopadení násilníka na místě činu či jeho okolí,
- zajištění dostatečných důkazů (fotografie, videa),

- možnost znovunalezení zcizených hodnot (historické, kulturní památky).

Z uvedených požadavků ovlivňujících efektivnost zabezpečovacích systémů je možné vyvodit dva znaky, jež jsou charakteristické pro každý zabezpečovací systém [19], [24]:

1. Existence ohrožených hodnot, které jsou vystaveny nebezpečí, za předem známých okolností.
2. Existence vnějších omezení, dostupnými možnostmi.

Proces poskytování ochrany chráněného objektu lze zobrazit blokovým schématem, jež je možné vidět na obrázku 11.



Obrázek 11 Schéma poskytování ochrany zabezpečovacích systémů [19]

Zabezpečovací systémy mají určitou strukturu, která se liší z organizačního a taktického hlediska. Operační prvky ze struktury jsou vymezeny svou činností k funkčnosti systémů. Mezi ně patří ochranný vliv na [19], [24]:

- Prevenci pachatele

Schopnost zabránit v napadení chráněného zájmu pachatelem, zejména mentálně, společensky nebo ekonomicky.

- Detekování

Zjištění změny sledovaných vlastností v objektu za pomoci zabezpečovacích čidel, alespoň změna jedné vlastnosti objektu.

- Diskriminovaná detekce

Proces vyhodnocení mezi skutečným a údajným nebezpečím hrozící objektu. Cílem diskriminované detekce je identifikovat veškeré události, které mohou být nebezpečné pro chráněný objekt.

- Poplach

Poplachy jsou děleny do dvou kategorií, na plané a falešné. Většinou jsou tyto pojmy používány jako synonyma ke stejnému jevu, avšak podle funkce čidel jsou rozlišovány.

- Planý – může být způsobený zásahem do běžné činnosti systému, ne však vloupáním. Možnou příčinou je chyba obsluhy, nebo citlivost čidel na vnější vlivy (průvan, teplo, větrání). [19]
- Falešný – je způsoben buď špatnou funkcí systému (vliv elektromagnetického rušení), rozbitou elektronickou součástí, nebo jinou poruchou (špatný sabotážní kontakt). Není však zaviněný obsluhou. [19], [24]

- Reakce systému

Reakce systémů na určité vlastnosti ohrožení objektu je několik druhů, které začínají instalací mechanické zábrany a končí zásahem do organizované a vytrénované jednotky. Za každých okolností operační prvek musí rychle a opakovaně přerušit nebezpečí, které hrozí chráněnému objektu. [19]

- Spolehlivost systému

Schopnost systému plnit požadovanou funkci za stanovených podmínek a po určitou dobu. U zabezpečovacích systémů vystupují do popředí specifické požadavky, než je to u jiných systémů. Zejména jde o míru zranitelnosti systému, nebo-li stupeň odolnosti proti nebezpečí. Díky funkci signalizace provozuschopnosti se zde mluví o diskvalifikačním poplachu, který informuje obsluhu o změně vnějších podmínek, za kterých nemůže čidlo pracovat správně. [24]

- Efektivnost systému

Efektivita zabezpečovacích prostředků se dělí na společenskou, ekonomickou, technickou a provozní, jež je hodnocena dle výsledků činnosti systémů. [19]

- Společenská – je odrazem účinnosti boje proti trestné činnosti v praxi.
- Ekonomická – jedná se o poměr na snižování ekonomických ztrát a vynaloženými prostředky na zabezpečovací systémy.
- Technická – úzce spojena s vědecko-technickým rozvojem zabezpečovací techniky, díky čemuž je zvýšena efektivnost proti trestné činnosti.
- Provozní – integrace ekonomické a technické efektivnosti, která je zaměřena na složitost obsluhy, poruchovost systému a výskytu planých poplachů.

### 3.2 Technické hledisko

Hlavním úkolem technického hlediska je rozbor cílové funkce zabezpečovacích systémů. Prvky a prostředky, které jsou použity, slouží primárně ke sběru informací o stavu, v jakém se chráněný objekt nachází. Nebezpečí, které hrozí chráněnému zájmu, jež je neustále střežen, musí být převedeno na elektrické signály, o které se starají detektory. Všechny technické prvky jsou založeny za pomoci fyzikálních jevů a používají jejich charakteristiky. V důsledku této skutečnosti je třeba detekovat bezpečnostní pojmy, ale až poté, co jsou převedeny. Pro představu jde o změnu teploty, pohyb hmoty v chráněném prostoru, nebo neoprávněnou manipulaci s předmětem, který je pod ochranou kapacitními detektory. [19]

Operační prvky využívané pro zabezpečovací systémy nemají pro technický subsystém žádný význam, nejsou-li zastupovány fyzikálními signály. Nebezpečí, které hrozí, vždy souvisí s jediným souborem těchto signálů, které však nejsou schopny určit reálné nebezpečí. Z toho důvodu je nutné brát vztah mezi technickým a operačním hlediskem takový, že technické řešení zabezpečovacích systémů jen jedním z funkčních vlastností operačního popisu. [19], [24]

Jestliže je u zabezpečovacího systému brána v potaz ochrana objektu před neoprávněným vstupem, ač se to nezdá, tato funkce je precizně zprovozněna jistým subsystémem, který je schopen detekovat všechny narušitele, kteří se pokoušejí dostat do operačního prostoru. I když se z technického hlediska nejedná o žádné pochybení systému, tak díky nástupu reakce prvku, která hraje důležitou roli. Musí během chvíle dojít k zákroku na napadeném místě, jestliže se tak nestane, je tím celá funkce zabezpečovacího systému nulována. Bohužel se to v praxi stává a pachatel má tudíž možnost z místa činu utéct, aniž by mu v útěku něco překáželo. Jak již bylo zmíněno, reakce je důležitá role. Je-li čas k provedení zákroku na napadeném objektu větší, než čas, potřebný k provedení krádeže a odcizení majetku, je nutné zavádět tzv. zpožďovací prvky, které využívají mechanické zábranné systémy. Ty pachatele zdrží v rychlém pronikání k jeho cíli. Prvky zabezpečovacích systémů je nutné instalovat podle toho, aby nebyly vystaveny vnějším vlivům, které na ně mohou působit a vyvolávat tím plané poplachy, či zhoršit samotnou funkci prvku. [23], [19]

Plané poplachy však mohou být vyvolány i skrz použití velmi citlivých prostředků, které citlivě reagují na bezvýznamné rušivé podněty. Zásahová jednotka, která reaguje na poplachy, neví, že se jedná o planý poplach, a časem se její činnost stává laxní, což má za následek podcenění výkonu, po kterém může následovat i ohrožení samotné zásahové jednotky.

Dalším důsledkem vyvolaný planými poplachy může být nepřítomnost zásahové jednotky tam, kde se o planý poplach nejedná a její činnost je důležitější, než na místě vzniklé planým poplachem. [19]

## 4 ANALÝZA RIZIK A BEZPEČNOSTNÍ ANALÝZY

V následujících podkapitolách je rozepsána analýza rizik, její důvody a podmínky ke stanovení. Na analýzu rizik budou navazovat jednotlivé bezpečnostní analýzy, či metody, které jsou rozděleny do dvou velkých kategorií, tj. kvalitativní a kvantitativní analýzy.

### 4.1 Analýza rizik

Pod pojmem analýza rizik je možno si představit určitý proces, při kterém jde o podrobné hledání a zkoumání hrozeb, které mohou při nedostatečném opatření negativně působit na určitý objekt, kterému mohou způsobit, podle závažnosti určité hrozby, malé či velké škody na majetku. Každá hrozba představuje určité riziko a velikost rizika, které se přiřazuje hodnota podle pravděpodobnosti výskytu a následku, který popřípadě nastane. [21], [20]

Jak již bylo zmíněno, analýza rizik představuje ucelený proces, do kterého patří určité části, fáze, kroky, jež jsou následující [21]:

- **identifikování aktiv** – prohlídkou daného objektu je proveden opis aktiv, které patří pod firmu,
- **určení hodnoty aktiv** – jsou zde stanoveny hodnoty aktiv podle významu pro firmu, kterými disponuje, ohodnoceno škodné případné ztráty, změny, poškození či zcizení,
- **stanovení hrozeb a slabin** – jsou zde určeny slabé prostory, které neodolají působením hrozeb a určení jevů, které když nastanou, negativně ovlivní hodnotu aktiv, proto kroky výše s aktivy,
- **určení závažností** – stanovuje se zde pravděpodobnost výskytu hrozby a úroveň újmy objektu v závislosti na hrozbách.

Přímo pro analýzu rizik byly vytvořeny skupiny metod, které se navzájem prolínají (obrázek 12).





Obrázek 12 Metody pro analýzu rizik [21]

- Induktivní metody

Jsou založeny na způsobu předvídání možných ohrožení na bezpečnost objektu, přičemž jsou zejména analyzovány skutečnosti, které stojí za případným ohrožením. Díky těmto metodám je možné přibližně určit počet událostí, vyhodnotit jejich následky a na základě toho navrhnout opatření k jejich eliminaci. Induktivní metody jsou realizovány pomocí dvou skupin – pravděpodobnostní model a expertní odhady. [21], [11]

- Deduktivní metody

Tato skupina metod pracuje s výskytem událostí v minulosti, podle kterých hledá příčiny, jež způsobily nepříjemnou událost objektu. Význam metod je důležitý při vytváření scénářů, které jsou vyvozeny podle příčin vzniku událostí a projevů rizik na daný objekt. To dává bezpečnostním systémům podnět se lépe na tyto scénáře připravit, když jsou známy možné scénáře. Využitelnost těchto metod je u již zmíněných vytvořených scénářů, avšak při neznámých událostí je jejich účinnost použití jen zřídka. [11], [21]

- Porovnávací metody

Jsou založeny na zkoumání jevů, na které se poukazuje na základě stanovené shody mezi těmito dvěma, či více jevy. Jsou velmi často používány z důvodu jednoduché aplikace. Je možné je použít jen tam, kde se vyskytují dva jevy se společnými parametry, tím vlastně dochází k již zmíněné shodě. [11], [21]

## 4.2 Vybrané kvalitativní analýzy

Výhodou kvalitativních analýz je jednoduchost v závislosti na rychlosti, ale každé své výhody přináší i nevýhody, v tomto případě jde o subjektivitu výsledků. Kvalitativní analýzy se používají v kombinaci s kvantitativními a to s cílem dosáhnout přesnějších výsledků,

protože kvalitativní neposkytují dostatečně potřebnou hodnotu. Jejich další možné využití je při stanovení priorit mezi možnými riziky a určení úrovně ohrožení a zranitelnosti. Kvalitativní analýzy jsou založeny na vyhodnocení strukturovaných rozhovorů a dotazníků, nebo na hodnocení, které sahá i do širší škály oborů, než jen do oboru, který řeší problém a to specialisty v oboru. Mezi kvalitativní metody patří i SWOT analýza, která bude podrobněji popsána, protože posloužila jako inspirace v praktické části.

- **Delfská metoda**

Nejčastěji používána analýza pro zjištění rizik, která je svým charakterem založena na expertních odhadech. Jak se říká „výjimka potvrzuje pravidlo“, protože výše bylo zmíněno, že kvalitativní metody se vyznačují svou rychlostí, to však neplatí u této metody, která je naopak časově náročná. Vyjadřuje, co může nastat a za jakých podmínek. Celá metoda je založena na principu, kdy jsou v kontaktu tři složky (experti, hodnotící skupina a představitelé hodnoceného objektu). Počet expertů je u této metody různý v závislosti na velikosti řešeného problému, ale většinou se dbá na to, aby expertů bylo deset. Metoda je postavena na kladení otázek, které jsou diskutovány hodnotící skupinou, kterou tvoří pevná, předem stanovená část a variabilní část, která se podle potřeby mění. Pravidlem je zde udržení anonymity. [20], [22]

- **Kontrolní seznam**

Jednoduchá kvalitativní analýza, která za pomoci kontrolního seznamu dává odpovědi na otázky, které jsou zaměřené na nedostatky a odlišnosti na provozní postup. Tím pádem napomáhá k bezpečnostnímu zlepšení. Musí-li expert vytvořit nový kontrolní seznam děje se tak podle norem a příslušných předpisů, jestliže je seznam vytvořený celým týmem, je zajištěna lepší kvalita, než kdyby jej sestavoval jeden expert. Rozsáhlost kontrolního seznamu je přímo úměrná účelu a složitosti zařízení, či objektu. Kontrolní seznam lze použít v kterékoliv fázi procesu, avšak nejčastější využití je při projektování jako kontrola se standardními podmínkami. Kontrolní seznam lze kombinovat například s metodou „Co se stane, když...“. [11], [21]

- **Analýza „Co se stane, když...“**

Jedná se o často používanou analýzu, která je založená na brainstormingu, kdy se sejde skupina expertů, kteří jsou dobře obeznámeni se situací a hledají možné situace, které mohou za určitých okolností nastat. Všechny položené otázky jsou zapisovány na tabuli a postupně se snaží přijít na všechny odpovědi. Jestliže je analýza využívána pro velký systém,

je lepší jej rozdělit na několik menších oblastí, částí provozu a ty hodnotit samostatně. Na základě zapsaných a prodiskutovaných odpovědí, lze zlepšit bezpečnostní opatření, aby bylo sníženo riziko. Výhodou je nízká časová náročnost, je možné ji použít v kterékoliv fázi. Novinkou analýzy je, že se nezapisují odpovědi ručně na tabuli, ale je k tomu použit vyhovující software. [11], [21], [22]

- **Předběžná analýza ohrožení**

Tato analýza byla vyvinuta s cílem hodnocení bezpečnosti pro armádu USA. Používá se především ve fázi návrhu projektu. Je určena pro identifikaci a rozřídění ohrožení, nebezpečných situací nebo událostí, ale hlavně jejich příčin a dopadů na zařízení, které se rozdělují dle kritérií. Při analýze se používá několik technik k následnému posouzení rizik. Výstupem je nápověda k podrobněji zaměřeným postupům rizik na daný systém, zejména rizika, u kterých je potřeba najít jiné způsoby minimalizace nebezpečí. Výhodou je brzké obeznámení pracovníků s možnými výskytů nebezpečí a lepším zvládnutím bezpečnosti. [21], [11], [22]

- **Analýza ohrožení a provozuschopnosti**

Analýza, která je založena na mezioborovém týmu, maximálně sedmi expertů, konkrétně na brainstormingu. Je využívána během projektové fáze procesu, nebo ihned po ní. Expertní tým k odhalení nežádoucích odchylek projektu využívá tvořivé a systematické kroky. Analýza ohrožení a provozuschopnosti, která je označována jako HAZOP (Hazard and Operability Study), má přednosti ve své jednoduchosti, díky které se stala jednou z nejpoužívanějších analýz pro zjištění rizik a správné funkce zařízení. Na základně výborných referencí je využívána při posuzování rizik složitých chemických továren. [22], [20], [11]

- **Analýza stromu událostí**

Analýza založena na grafických a statistických nástrojích, která vyjadřuje výsledky havárie plynoucí z vyvolané události. Jako výsledek jsou pak různé poruchy a chyby, které vedou celý systém k havárii. Díky tomu se posuzuje úspěch, nebo porucha funkčnosti.

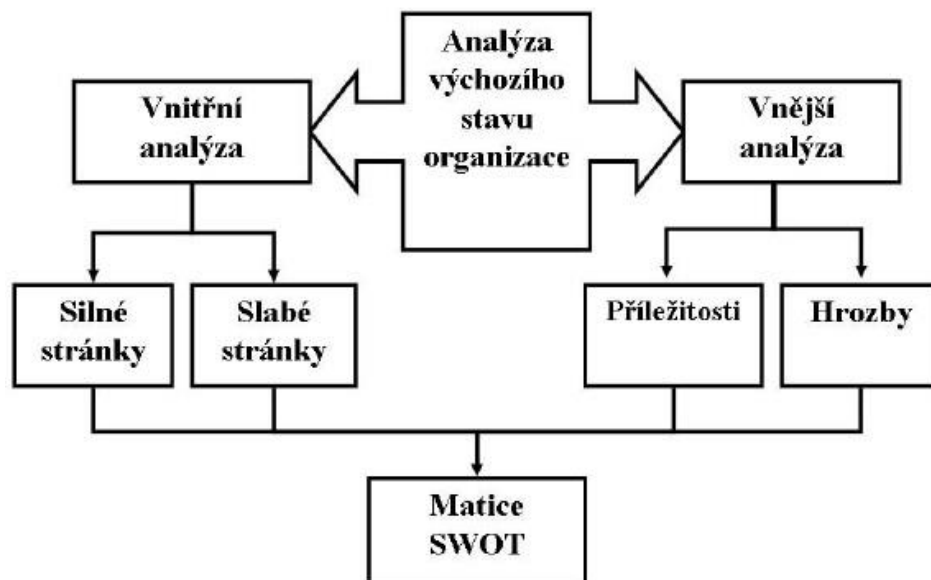
Celá analýza je provedena jedním analytikem pro menší systémy, které zvládne posoudit sám, často se však využívá model s dvěma až čtyřmi experty. Získané výsledky jsou využity k následným doporučením pro snížení rizik, nebo potencionálních poruch. Analýza je vhodná pro testování systémů, které mají svůj bezpečnostní systém, popřípadě systémy bez

bezpečnostního systému, které však mají nouzový havarijný postup k zásahu v případě reakce na určité počítačové události. [11], [21]

- **SWOT analýza**

Metoda SWOT analyzuje objekt, jež je založena na identifikaci základních faktorů, které jsou rozdělené na vnitřní a vnější analýzu, grafické znázornění je na obrázku 13 [21]:

- silné stránky (Strengths),
- slabé stránky (Weakness),
- vnější příležitosti (Opportunities),
- hrozby (Threats),



Obrázek 13 Rámec SWOT analýzy [21]

Tato analýza je založena na využití expertních metod, mezi nejznámější je možno uvést brainstorming, delfskou metodu, brainwriting, nebo metoda psaní scénářů.

Před sestavováním SWOT analýzy je nezbytné provést podrobnou analýzu výchozího stavu, který se stanovuje hned na začátku procesu. Po následném stanovení procesu se zařazuje do jedné ze čtyř základních skupin pomocí metod, které jsou uvedené výše. Pokračuje se vzájemným působením mezi faktory, konkrétně jejich silných a slabých stránek na jedné straně proti příležitostem a hrozbám na straně druhé. Cílem je získání nových informací, které jsou typické pro úroveň vzájemného porovnání. SWOT analýza se nejčastěji používá v marketingu, ale poslední dobou nachází velké uplatnění při tvorbě bezpečnostních poli-

tik. Nesmí se zapomínat ani na fakt, že pomocí SWOT analýzy bývá zlepšeno strategické plánování firmy, protože je možné jí použít pro vyhodnocení fungování společnosti. Na obrázku 14 je příklad SWOT analýzy pro objektovou bezpečnost. [21], [22]

| Silné stránky   | Slabé stránky  |
|---|--|
| <ol style="list-style-type: none"> <li>1. Zabezpečení technologických vstupů</li> <li>2. Kvalitní bezpečnostní vstupní prvky (dveře)</li> </ol> | <ol style="list-style-type: none"> <li>1. Technický stav stand. prvků (okna)</li> <li>2. Fyzická ostraha</li> </ol>                              |
| Příležitosti  | Hrozby   |
| <ol style="list-style-type: none"> <li>1. Změna územního plánu lokality</li> <li>2. Výhodná nabídka bezpečnostní služby</li> </ol>              | <ol style="list-style-type: none"> <li>1. Finanční omezení</li> <li>2. Nedbalost zaměstnanců</li> <li>3. Vysoká kriminalita v oblasti</li> </ol> |

Obrázek 14 Příklad použití SWOT analýzy

SWOT analýza není prováděna s cílem vytvořit rozsáhlý přehled o silných, slabých stránkách, příležitostech a hrozbách, ale použít tyto skutečnosti při provádění následujících činností [22]:

- Určit rizikové oblasti a i ty, které je nutné zlepšit, či je udržet na stejné úrovni.
- Navrhnout si cíl pro určité oblasti (vytváření obecných rozvojových cílů, které zahrnují, jakého stavu má být v oblastech dosaženo).

Pod pojmem „obecné cíle“ se rozumí, že jsou určeny pro dlouhodobý časový úsek. Zatímco „specifické cíle“ jsou brány jako cíle nižšího řádu, které jsou nezbytné k dosažení obecných cílů ve zvoleném časovém úseku. Cíle specifické nemohou být určeny ani po střednědobý, či krátkodobý časový úsek. [22], [11]

Důležité je zde stanovit opatření, které jsou prováděny za účelem splnění nadefinovaných cílů. Cíle charakterizují cílový stav, kdežto opatření stanovují projekty, které musí být splněny pro dosažení nadefinovaných cílů. [21]

### 4.3 Vybrané kvantitativní analýzy

Jde o analýzy nebo metody, které jsou založené na matematických výpočtech rizik z pravidelné četnosti výskytu hrozeb a následných dopadů. Jsou realizovány ze dvou kroků –

z pravděpodobnosti výskytu událost a pravděpodobnosti ztráty. Nevýhodou je jejich náročnost na čas, který se umocňuje s rozsáhlejším objektem, a náročnost na velký objem vstupujících dat. [21]

- **Analýza stromem poruch**

Analýza stromem poruch nejen, že patří mezi kvantitativní metody, tak i mezi deduktivní metody. Používá se pro ni značka FTA, z anglického „Fault Tree Analysis“. Jedná se o grafický model, který je založen na Booleovské algebře (hradla „a“, „nebo“ a jiné). Zná zornuje postupný proces od vyhledávání těch nejmenších poruch vedoucí k vrcholové či nejzávažnější události. Tato analýza se používá i pro rozsáhlejší systémy, protože může určit výčet všech nejmenších poruch. Výsledkem je přiřazení pravděpodobnosti poruch systémů na základě již známých pravděpodobností hlavních příčin vzniku. Je časově závislé na velikosti podniku. [11], [21]

- **Analýza lidského faktoru**

Je založena na postupném hodnocení faktorů, které ovlivňují práci vykonávanou lidskou složkou, zejména se jedná o operátory, údržbáře, techniky a jiné zaměstnance. Cílem je tedy zjistit chyby, kterých se zaměstnanci dopouštějí a následně jejich příčiny a důsledky. Princip spočívá v dotazování otázek na fyzickou kondici, charakteristiku prostředí, na šikovnost, znalosti, inteligenci, psychiku a schopnosti zaměstnanců. Používá se zejména ve spojení s jinými metodami (například se zmíněnou analýzou stromem poruch). Výsledky jsou grafické, nejčastěji ve formě stromu chyb, buď jsou kvalitativní, nebo kvantitativní. Analýza je zejména prováděna odbornými analytiky, kteří jsou seznámeni s tím, jak rozhovory provádět. [11], [21]

- **Analýza rizik procesu**

Jedná se o systém s komplexním přístupem pro předpovídání odhadu pravděpodobnosti výskytu a dopadů událostí na zařízení, nebo systém jako takový. Cílem této analýzy je zcela jasný a nekompromisní, přijít na zdroje rizik a na základě toho navrhnout potřebná opatření, která zohledňují i efektivitu další investice. Metoda je nasazována zejména v bezpečnostních organizacích a procesech nebo projektech s ní spojených. [21], [11]

## **II. PRAKTICKÁ ČÁST**

## 5 ÚVOD DO PRAKTICKÉ ČÁSTI

Cílem praktické části práce bude návrh zabezpečovacího systému firmy Megacorp – Plus, s.r.o., která je zaměřena na strojírenský průmysl. Společnost na trhu působí přes 20 let a ve strojírenství se zaměřuje na oblast výroby lehkých a těžkých ocelových konstrukcí, výroby ocelových dveří a zárubní, zpracování plechů na CNC strojích, výroby jednoúčelových strojů. Při návrhu bude nutné uvažovat specifický provoz a prostory dané firmy. Návrh zabezpečení bude tedy zaměřen na reálný objekt s možným reálným využitím. Proto byla nezbytná konzultace s vedením firmy a to za účelem získat co nejvíce informací potřebných k vypracování této práce. Po dohodě s vedením firmy mohou být v práci uveřejněny i informace vedoucí k přímé identifikaci daného objektu. Dále z jednání vyplynula nutnost při výběru vhodných komponent zabezpečovacího systému zohlednit i finanční stránku dané firmy. Z toho důvodu budou návrhy dva. První bude navržen i s ohledem na potřeby firmy a druhý se bude opírat o osobní zkušenosti získané během studia oboru bezpečnostní technologie, systémy a management na fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně.

Navrhované systémy se budou týkat výše zmíněné firmy. Celý areál je ohraničen plotem, který obklopují rodinné domy. V areálu firmy se nachází 3 budovy a sklad, který slouží pro nepotřebné věci. Hlavní budova bude předmětem zabezpečovacího systému, ke které přilehá bývalá provozovna. Dále se v areálu nachází budova s výrobní halou, ve které jsou různé dílny (lakovna, svářečí dílna, CNC s frézku). Posledním objektem je dům, který má firma pouze ve vlastnictví. Dům není v současné době obýván a stejně jako budova s výrobní halou nebude předmětem návrhů zabezpečovacích systémů.

Dále musím podotknout, že daná firma nedisponuje žádným zabezpečovacím systémem.



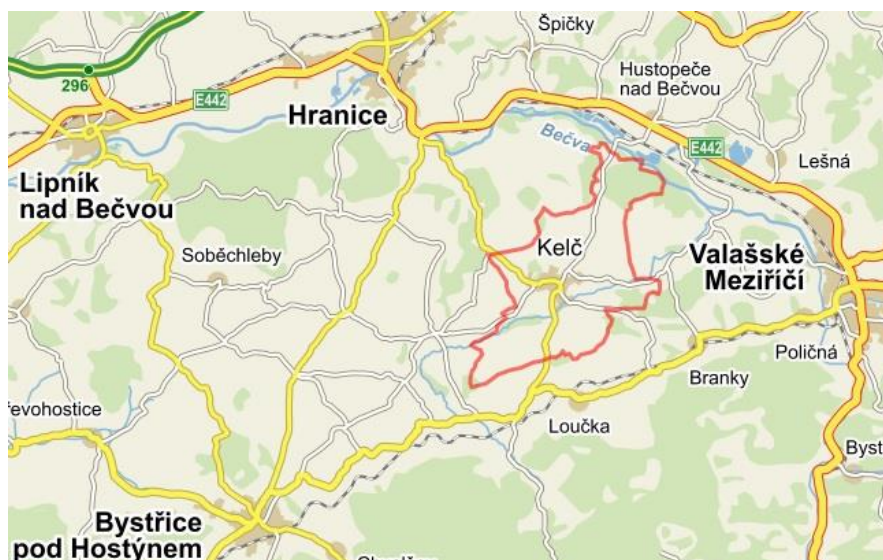
## 6 POPIS OBJEKTU A JEHO BEZPEČNOSTNÍ POSOUZENÍ

Následující kapitola bude zaměřena na areál objektu společnosti, posouzení objektu, kde budou posouzeny zabezpečované hodnoty, zde patří zejména aktiva, kterými firma disponuje. Dále bude provedeno bezpečnostní posouzení budovy a vlivů, které působí ať už zevnitř, nebo zvenčí. Součástí posouzení bude vytvoření bezpečnostní analýzy.

### 6.1 Areál objektu společnosti

Zabezpečovaný objekt se nachází v malém městečku Kelč, které je hraničním městem dvou moravských krajů, tj. Zlínského a Olomouckého a leží v okrese Vsetín. Žije zde okolo 2 500 obyvatel a zajímavostí je zmínka o uložení pokladu na kopci Strážné, který se nachází za městem a byl zde uložen kolem roku 1000.

Objekt společnosti se nachází u hlavní silnice s křižovatkou, ze které je možné se dostat do téměř stejně vzdálených dvou větších měst. Do Hranic na Moravě, které jsou vzdáleny 12 km a ze všech větších měst nejbližší Kelči, je možné se dostat po severozápadní straně. Do Bystřice pod Hostýnem, která je vzdálená 15 km, vede jihozápadně cesta z křižovatkou nad zvolenou firmou. Východním směrem leží město Valašského Meziříčí, které je vzdálené 13 km. V podstatě je možné napsat, že Kelč leží uvnitř trojúhelníku, kde vrcholy jsou tvořeny těmito třemi městy, což je znázorněné na obrázku 15.

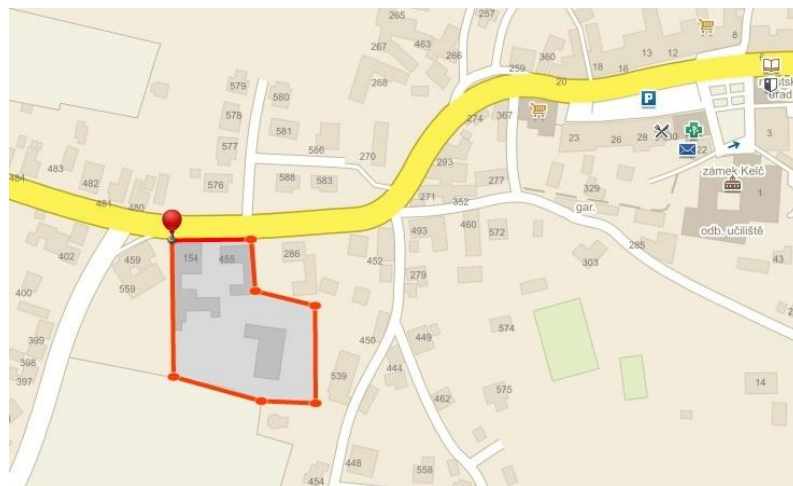


Obrázek 15 Územní plán města Kelč [29]

Pokud bychom se zaměřili na samotné území firmy. Každý by čekal, že bude sousedit s několika dalšími společnostmi v průmyslové zóně. Tím že je Kelč malé město a žádná průmyslová zóna se v něm nenachází, tak zvolená firma sousedí se satelitním městečkem

na severní straně, které je hned přes cestu po výjezdu z firmy a s jeho výstavbou se začalo před 10 lety. V satelitním městečku je několik rodinných domů, především zde bydlí rodiny s malými dětmi. Západní a východní strana firmy je taktéž obklopena rodinnými domy. Jen jižní část perimetru je oddělena zemědělskou půdou. Sousední rodinné domy, vč. satelitního městečka, jsou znázorněny na obrázku 16.

Po 400 metrech ve směru na Hranice na Moravě se nachází firma AKORD Kelč, která se převážně zabývá zateplením budov a revitalizací domů. Opačným směrem, na Valašské Meziříčí, po 500 metrech je náměstí, kde je mnoho obchodů a pod náměstím mají své pobočky policejní a hasičské jednotky. V případě jakékoliv nežádoucí situace je odezva na eliminaci situace státními orgány velmi krátká.



Obrázek 16 Objekt společnosti [30]



Obrázek 17 Letecký pohled na objekt společnosti [30]

Pozemek, na kterém se zabezpečovaný objekt nachází, má výměru okolo 9 500 m<sup>2</sup>, jen pro představu, tak velkou plochu tvoří dvě fotbalová hřiště vedle sebe. Z obrázku 17 je patrné, že všechny čtyři budovy areálu společnosti tvoří menší polovinu z celkové plochy.

Jak již bylo zmíněno, na celkové ploše jsou čtyři objekty – hlavní budova, ke které přilehá bývalá provozovna, budova s výrobní halou. Dům (na obrázku 18 vlevo), jež má firma ve vlastnictví, nemá s chodem firmy nic společného. Může sloužit k pronájmu. Poslední budovou v objektu je sklad nepotřebných věcí, které jsou převážně určené do šrotu. V tabulce 6 jsou budovy uvedeny pro lepší přehlednost.

Tabulka 6 Budovy v areálu společnosti

| Číslo | Budovy v areálu společnosti         |
|-------|-------------------------------------|
| 1     | Hlavní budova s bývalou provozovnou |
| 2     | Budova s výrobní halou              |
| 3     | Dům                                 |
| 4     | Sklad nepotřebných věcí             |

V hlavní budově, která je rozdělena na přízemí a první patro, se v přízemí nachází dílna pro strojní obrábění výrobků a různých opravování elektrickými zařízeními. V prvním patře hlavní budovy (oranžová budova na obrázku 18) je kancelář s šatnou pro vedení a kuchyň s jídelnou pro všechny zaměstnance. V budově výrobní haly (obrázek 19) je několik dílen, které nejsou odděleny dveřmi, z důvodu snadnějšího přístupu do všech dílen.



Obrázek 18 Pohled ze silnice na firmu a dům [25]

## 6.2 Bezpečnostní posouzení objektu

Samotné bezpečnostní posouzení obsahuje čtyři části, které se vztahují na zabezpečovaný objekt. Při návrhu zabezpečovacího systému se jedná o tyto čtyři oblasti - zabezpečované hodnoty, budovy objektu, vnitřní a vnější vlivy. Všechny oblasti je možné klasifikovat do dvou skupin. Analýza rizik zahrnuje zabezpečované hodnoty a budovy objektu, druhá skupina, ostatní vlivy, zahrnuje vnitřní a vnější vlivy.

Analýza rizik se zpracovává s cílem stanovit potřebný stupeň zabezpečení, který popisuje norma ČSN EN 50 131 – 1 a tyto stupně jsou rozděleny do 4 kategorií, jak je uvedeno v tabulce 1. Posouzení vnitřních a vnějších vlivů je zpracováno z důvodu správného výběru prvků zabezpečení.

### 6.2.1 Zabezpečované hodnoty

Druh majetku není pro potenciální zloděje zvenčí nikterak zajímavý, protože se převážně jedná o kovový materiál, hrozbu pro aktiva představuje hlavně poškození na strojích potřebných k výrobě. V budově výrobní haly se nachází lakovna, svářecí dílna a stroje k frézování a CNC obrábění (Computer Numeric Control). Vezmeme-li do úvahy tuto budovu, ve které jsou stroje velmi těžké a pro pachatele nezajímavé. Největší hodnotu v této budově představují stroje určené k frézování a CNC obrábění. Nachází se zde ještě barvy a laky, které jsou speciálně určeny přímo pro výrobu. Co by mohlo být pro majitele ztrátové, kdyby se pachatel dostal do hlavní budovy s bývalou provozovnou, kde se v přízemí nachází dílna, ve které jsou snadno odcizitelné elektrické zařízení, hlavně vrtačky a obráběcí stroje, které mají z dílny největší hodnotu a pro pachatele jsou ideálním předmětem ke krádeži nebo poškození. V prvním patře hlavní budovy je společná kancelář, ve které je nepřeborné množství cenných papírů a hlavně osobní počítače a notebook majitele. Jejich odcizení by představovalo pro firmu velký problém. Zde se počítá hlavně se SW, který je používán pro CNC obrábění a frézování a firma do něj investovala velké finanční prostředky, bohužel však přesná výše ceny nebyla poskytnuta.

Zabezpečovaný objekt společnosti se nachází v okrese Vsetín, ve kterém je kriminalita na nízké úrovni, v porovnání s různými okresy po celé Moravě. Bylo tak zjištěno ze zdrojů Policie ČR. Právě díky nízké kriminalitě společnost nepamatuje žádnou významnou krádež. Byly zde zaznamenány akorát menší vloupání a krádeže v hlavní budově s bývalou provozovnou, kde bylo odcizeno elektrické zařízení. Problémem bylo, že se nikdy nepřišlo

na to, kdo za těmito krádežemi byl, jestli pachatel zvenčí, nebo nejhorší možný pachatel a to zaměstnanec firmy. Firma totiž nedisponuje žádným zabezpečovacím systémem a oplocení, které je kolem objektu sahá do výšky cca 140 cm, tudíž je snadno překonatelné.

Co se týče poškození, do budovy výrobní haly je přístup znesnadněn, protože většina okenních otvorů je ve výšce okolo 5 m (obrázek 19). K překonání dveří nebo vrat by pachatel musel být vybaven určitými prostředky k překonání, je-li brán v potaz útočník, který objekt nezná. Další výhodou před možným útokem je, že budova není viděna od hlavní silnice, tudíž si ji pachatel nemůže prohlédnout a díky tomu se na ni potřebně vybavit. Větší riziko vloupání představuje hlavní budova s bývalou provozovnou, která byla před pár lety po plášti komplet zrekonstruována. Byla vyměněna veškerá okna a dveře za plastová. Společná kancelář pro vedení, byla taktéž zrekonstruována. Hlavní budova představuje větší zájem pro potencionální útoky pachatele, kteří si hlavní budovu mohou dokonale prohlédnout od hlavní silnice. Poškození tak hrozí na veškerých okenních otvorech přízemí, hlavních dveří, či starých, nevyměněných vrat (obrázek 20).



Obrázek 19 Pohled na budovu výrobní haly



Obrázek 20 Pohled na vrata hlavní budovy

### 6.2.2 Budovy objektu

Konstrukce obou budov, na kterých se nachází okna, dveře, vrata, jsou starší, než je datován vznik firmy. Budovy mohou mít kolem 40 – 50 let, avšak v posledních letech se pravidelně rekonstruují. Hlavní budova je komplet zrekonstruována až na hlavní vrata (obrázek 20). V budově výrobní haly je použita panelová konstrukce, která je velmi pevná a odolná vůči otřesům a vibracím způsobených používáním strojů. V budově s výrobní halou jsou vyměněna pouze vrata a dveře, okna byly ponechány staré. V brzké budoucnosti se neuvazuje s jejich rekonstrukcí. Tyto okna však představují větší riziko vloupání, protože jsou snadno překonatelné.

Provoz a režim objektu je jednosměnný, tudíž je zde zavedena jen ranní směna, která pro všechny zaměstnance začíná v 6:00 a končí v 14:30. Objekt je však většinou úplně prázdný až po 15. hodině, než se všichni zaměstnanci převlečou, uklidí a zamknou dílny. O víkendech je společnost zavřena. Objekt společnosti nedisponuje žádným zabezpečovacím systémem, ani fyzickou ostrahou, takže není nijak střežen v době, kdy se v objektu nikdo nenachází.

Držitelé klíčů jsou oba jednatelé a sekretářka, ale také vedoucí výroby. Ostatní zaměstnanci jsou na ně odkázáni. Zabezpečovaný objekt se nachází v městské zástavbě. Okolí objektu tvoří rodinné domy, z jedné strany přes hlavní silnici satelitní městečko, kde se vyskytuje mnoho lidí, hlavně přes den a kolem objektu denně projedou stovky aut. Riziko zde ne-

hrozí od lidí, kteří jsou v podnapilém stavu, protože většina hospod se nachází na opačné straně města. Dá se říct, že objekt se nachází v klidné části.

### 6.2.3 Vnitřní vlivy

V celém komplexu objektu je zhotovené vodovodní potrubí z oceli, tudíž by nemělo při použití mikrovlnných detektorů jakkoliv narušit jejich funkci. Vytápění je v hlavní budově zřízeno jen v prvním patře, kde se nachází kancelář a jídelna s kuchyní. Radiátory jsou v těchto prostorách umístěny klasicky pod okny. Klimatizace a odvětrávání je v budově s výrobní halou.

Co se týče závěsných předmětů, tak v jednotlivých dílnách se jich moc nevyskytuje, snad jen v budově s výrobní halou je umístěna jedna nástěnka co se kdy má udělat. V prvním patře hlavní budovy na chodbě je k vidění jeden velký plakát a ozdoba na protější zdi. Přímo v kanceláři jsou po zdech zarámované obrazy.

Výtahy v zabezpečeném objektu nejsou, co však může negativně působit na komponenty zabezpečovacího systému, jsou vibrace a hluk způsobené elektrickými zařízeními. Jelikož se hlavní budova nachází přímo vedle hlavní silnice, je zde riziko osvětlení projíždějících aut. Osvětlení je v obou budovách pomocí zářivek.

Elektromagnetické rušení může být vyvoláno v budově s výrobní halou svářecími soupravami. Po celém objektu je používáno nepřehledné množství elektrických zařízení, které by však neměly způsobovat elektromagnetické rušení.

V jednotlivých dílnách se vyskytují různé druhy zařízení, které vydávají zvuky charakteristické těmto zařízením, je třeba v návrhu brát v potaz vhodný výběr komponent. Celý objekt sousedí s rodinnými domy, u kterých je možný výskyt domácích zvířat po zahradě, zejména psů. Z pole u areálu objektu se předpokládá výskyt zvířat, zejména srnců, srnek, zajíců, divokých prasat. Uvnitř areálu společnosti se žádné zvířata nevyskytují, tudíž by komponenty zvířaty neměly být nijak ovlivněny.

Ovlivnění činnosti komponent kvůli průvanu hrozí zejména v hlavní budově s bývalou provozovnou, protože se zde nachází mnoho oken a při jejich otevření k němu může snadně docházet. V dílně stejné budovy hrozí pád skladovaných předmětů ze stolů nebo z vícepatrových regálů. Uspořádání obráběcích strojů při správném umístění prvků zabezpečení nikterak nenaruší jejich funkci. Umístění obráběcích strojů v dílně hlavní budovy je na obrázku 21.



Obrázek 21 Umístění obráběcích strojů

#### 6.2.4 Vnější vlivy

Z dlouhodobě působících faktorů je třeba zmínit vysoce frekventovanou hlavní silnici vedle areálu. Objekt je umístěn v městské zástavbě, kde se předpokládá vysoký výskyt procházejících lidí, zejména přes den. Do budoucna se předpokládá se stále se rozšiřujícím satelitním městečkem.

Vlivy vzniklé kvůli počasí nikterak neovlivní funkci detektorů, které budou umístěny uvnitř budovy. Může být ovlivněn výběr kamer. Většina kamer je však odolná proti různým vlivům, ať už se jedná o sněžení, krupobití, déšť nebo vítr.

V okolí objektu se nevyskytují žádné antény, ani radary. Podél hlavní silnice jsou umístěny stožáry s elektrickým vedením. Ke vzniku elektromagnetického rušení by však docházet nemělo. Výskyt těžkých strojů, které mohou způsobovat vibrace, výrazně neovlivní činnost prvků zabezpečení, protože domy jsou v dostatečné vzdálenosti.

Ve zmíněnou pracovní dobu může docházet ke vniknutí přes hlavní bránu různými osobami, počínaje dětmi, konče opilci a vandaly, protože hlavní brána je v rozmezí 6 – 15 hodin otevřena.

### 6.3 Bezpečnostní analýza

Na základně získaných informací o SWOT analýze v teoretické části, mi následně byly nápomocí a inspirací při zpracování bezpečnostní analýzy (tabulka 7). Ta je tvořena silnými a slabými stránkami, příležitostmi a hrozbami. V tabulce (9, 10, 11, 12) jsou tyto čtyři položky rozebrány detailněji, v tabulkách jsou uvedeny pojmy jako váha, která značí důle-



žitost a hodnocení označující spokojenost. U zmíněných pojmů jsou zaznačeny jednotlivé hodnoty. Tyto hodnoty znamenají spokojenost či nespokojenost, přičemž silné stránky a příležitosti jsou bodovány v rozmezí 1 až 5. U slabých stránek a hrozeb je rozmezí od -1 až -5.

Tabulka 7 Bezpečnostní analýza

| Bezpečnostní analýza |  |   |
|----------------------|--|---|
| Silné stránky        |  | Slabé stránky                                 |
| Vnitřní část         | Silné vedení                                 | Zabezpečovací systém                          |
|                      | Klidná lokalita, nízká kriminalita           | Finanční stránka                              |
|                      | Těžko odcizitelná aktiva – nezájem pachatele | Snadno překonatelný perimetr                  |
|                      | Rychlý zásah policie, hasičů                 | Špatný stav hlavních vrat, hluk, vibrace      |
| Příležitosti         |  | Hrozby  |
| Vnější část          | Fyzická nebo kynologická ostraha             | Krádeže zařízení, vandalismus                 |
|                      | Vylepšení perimetrických prvků               | Poškození pláště z hlavní silnice             |
|                      | Výměna pozůstalých starých otvorů            | Nárůst kriminality                            |
|                      | Pořízení zabezpečovacího systému             | Krádeže cenných papírů a SW licence z archívu |

V bezpečnostní analýze byly určeny silné a slabé stránky, stejně tak jako příležitosti nebo hrozby, které mohou mít negativní vliv na další fungování společnosti. Z uvedených silných stránek se dá považovat za významnou stránku charakter aktiv, kdy společnost vlastní mnoho zařízení, které svou hmotností a parametry znesnadňují odcizení. Za největší slabinu firmy je považována absence jakéhokoliv zabezpečovacího systému, dále pak finanční stránka, která je způsobena nízkou poptávkou.

Z příležitostí, které jsou pro firmu k dispozici, je stěžejní pořízení zabezpečovacího systému. Pro firmu jsou s příležitostmi spojeny i hrozby, vč. nárůstu kriminality ve městě a s tím spojené krádeže jednoduchých přenosných zařízení, nebo cenných papírů z kanceláře, vč. SW licence programů.

Detailnější rozbor jednotlivých hodnot spokojenosti a nespokojenosti je uveden v tabulce 8. Díky tomu je možné si udělat lepší představu o silných a slabých stránkách, ale i příležitostech nebo hrozbách. Hodnoty jsou následně přiděleny položkám a znásobeny uvedenou váhou podle důležitosti. Kladné hodnoty jsou uděleny silným stránkám a příležitostem, záporné hodnoty ke slabým stránkám a hrozbám.

Tabulka 8 Detailnější rozbor hodnocení

| Body | Hodnocení (spokojenost) | Body | Hodnocení (nespokojenost) |
|------|-------------------------|------|---------------------------|
| 1    | Nízká                   | -1   | Zanedbatelná              |
| 2    | Mírná                   | -2   | Přijatelná                |
| 3    | Přijatelná              | -3   | Střední                   |
| 4    | Dostačující             | -4   | Nevyhovující              |
| 5    | Vysoká                  | -5   | Nepřijatelná              |

Váha značí důležitost a řídí se následujícími pravidly - součet vah u silných, slabých stránek, příležitostí a hrozeb dává vždy součet 1 a čím vyšší číslo, tím větší je důležitá položka.

Tabulka 9 Hodnocení silných stránek

| Silné stránky                                       | Váha | Hodnocení | Celkem     |
|---|------|-----------|------------|
| <b>Silné vedení</b>                                 | 0,2  | 3         | 0,6        |
| <b>Klidná lokalita, nízká kriminalita</b>           | 0,2  | 2         | 0,4        |
| <b>Těžko odcizitelná aktiva – nezájem pachatele</b> | 0,3  | 4         | 1,2        |
| <b>Rychlý zásah policie, hasičů</b>                 | 0,3  | 4         | 1,2        |
|   |      |           | <b>3,4</b> |

Tabulka 10 Hodnocení slabých stránek

| Slabé stránky                                   | Váha | Hodnocení | Celkem       |
|---|------|-----------|--------------|
| <b>Zabezpečovací systém</b>                     | 0,4  | -4        | -1,6         |
| <b>Finanční zázemí</b>                          | 0,3  | -3        | -0,9         |
| <b>Snadno překonatelný perimetr</b>             | 0,15 | -1        | -0,15        |
| <b>Špatný stav hlavních vrat, hluk, vibrace</b> | 0,15 | -2        | -0,3         |
|   |      |           | <b>-2,95</b> |

Tabulka 11 Hodnocení příležitostí

| Příležitosti                             | Váha | Hodnocení | Celkem   |
|--|------|-----------|----------|
| <b>Fyzická nebo kynologická ostraha</b>  | 0,2  | 2         | 0,4      |
| <b>Vylepšení perimetrických prvků</b>    | 0,15 | 2         | 0,3      |
| <b>Výměna pozůstalých starých otvorů</b> | 0,15 | 2         | 0,3      |
| <b>Pořízení zabezpečovacího systému</b>  | 0,5  | 4         | 2        |
|  |      |           | <b>3</b> |

Tabulka 12 Hodnocení hrozeb

| Hrozby   | Váha | Hodnocení | Celkem       |
|--|------|-----------|--------------|
| <b>Krádeže zařízení, vandalismus</b>                 | 0,25 | -3        | -0,75        |
| <b>Poškození pláště z hlavní silnice</b>             | 0,2  | -2        | -0,4         |
| <b>Nárůst kriminality</b>                            | 0,15 | -2        | -0,3         |
| <b>Krádeže cenných papírů a SW licence z archívu</b> | 0,4  | -3        | -1,2         |
|  |      |           | <b>-2,65</b> |

Následně je možné z předchozích tabulek 9, 10, 11 a 12 sečíst silné a slabé stránky ve vnitřní části a příležitosti s hrozbami ve vnější části. Výsledek po sečtení vnitřní části je kladný, konkrétně 0,45. Hodnota vnější části je po sečtení 0,35. Z toho plyne, že silné stránky a příležitosti převažují, avšak výsledné hodnoty jsou zanedbatelné.

Z výše uvedených tabulek vyplývá, že je třeba pořídit zabezpečovací systém, který představuje největší slabinu pro firmu. Pro firmu představují značné riziko nejpravděpodobnější hrozby uvedené v tabulce 13. Je třeba dbát důraz na protiopatření k hrozbám při návrhu zabezpečovacího systému. Hrozby jsou mj. i krádeže přenosných elektrických zařízení klíčových pro firmu, nebo vloupání do kanceláře a zcizení cenných papírů, notebooku majitele s nahranou SW licencí programů určené k frézování a CNC obrábění.

### 6.3.1 Vyhodnocení bezpečnostní analýzy

Na základě informací uvedených v předchozích tabulkách bezpečnostní analýzy lze navrhnout protiopatření k zjištěným hrozbám, což je cílem analýzy (tabulka 13). Výstup bezpečnostní analýzy je dalším stěžejním požadavkem potřebným k zohlednění při samotném návrhu zabezpečovacího systému. Z navržených opatření bude při návrhu zabezpečovacího systému nutná realizace PZTS, ale i CCTV. Hrozbu pro objekt představuje i požár, tudíž bude nutné počítat s pořízením chybějících hasicích přístrojů a kombinovaného detektoru kouře a teploty.

Tabulka 13 Protiopatření k hrozbám

| Hrozby                                | Protiopatření   |
|---------------------------------------|---|
| <b>Krádeže</b>                        | PZTS, CCTV  |
| <b>Vandalismus, rozbití oken</b>      | CCTV, MZS, PZTS   |
| <b>Pracovní úraz a poruchy strojů</b> | Dodržovat bezpečnost a ochranu zdraví při práci, revize, kontroly |
| <b>Vloupání</b>                       | CCTV, PZTS  |
| <b>Požár</b>                          | Detektor kouře, hasicí přístroje                                  |

## 7 NÁVRH ZABEZPEČOVACÍHO SYSTÉMU – VERZE 1

V následující kapitole bude proveden první návrh zabezpečovacího systému, který bude odpovídat stanovenému stupni zabezpečení a třídě prostředí. Nedílnou součástí návrhu zabezpečení budou protiopatření zjištěných hrozeb. Jak již bylo uvedeno v úvodu do praktické části práce, budou zohledněny i potřeby firmy, konkrétně stanovené částkou 60 000 Kč na vybrané zabezpečovací prvky bez montáže a zednických prací. V kapitole bude zmíněn i rozpis použitých prvků, vč. cenového rozpočtu, konfigurace a způsobu zásahu. Při návrhu zabezpečovacích systémů byly důležité konzultace s vedením firmy. Při konzultacích s vedením firmy, ve kterých nebyla předmětem přesná cena aktiv, jež byla na základě získaných poznatků vyčíslena okolo 3 000 000 Kč. Mezi aktiva firmy patří obráběcí stroje, elektrické zařízení, dokumenty, software licence programů a nábytek zabezpečované hlavní budovy s bývalou provozovnou.

### 7.1 Požadavky na návrh zabezpečení – verze 1

Cílený požadavek na návrh zabezpečovacího systému verze 1 je zajistit protiopatření k eliminaci hrozeb, zohledněna bude i finanční stránka, která je uvedena v úvodu kapitoly. Dále by měl být návrh adekvátně zabezpečen z pohledu aktiv, kterými firma disponuje, přičemž jejich odhadovaná suma činí 3 000 000 Kč a to pouze v hlavní budově s bývalou provozovnou. Suma byla odhadnuta na základě získaných znalostí provozu a prostor firmy. Bývala provozovna, která přilehá k hlavní budově, nebude předmětem zabezpečení.

Zabezpečovaná hlavní budova a celý areál společnosti nedisponuje žádným zabezpečovacím systémem. Což je jeden z požadavků pořízení zabezpečovacího systému v podobě CCTV a PZTS sloužící jako protiopatření k možným hrozbám. EPS není mezi jednotlivými požadavky na zabezpečovací systém. Pokud by do budoucna byl požadavek na rozšíření zabezpečovacího systému o případnou EPS, bude se tím zabývat projektant se zaměřením na požární ochranu. Na obrázku 22 je ukázka zrekonstruované společné kanceláře.



Obrázek 22 Pohled do kanceláře ze dveří

## 7.2 Stupeň zabezpečení a třída prostředí

Z bezpečnostního posouzení, které bylo zpracováno v kapitole 5 a z výsledků bezpečnostní analýzy, je hlavní budova zařazena do druhého stupně zabezpečení podle tabulky 1 ve druhé kapitole. Druhý stupeň zabezpečení znamená nízké až střední riziko a je třeba u něj zabezpečit dveře, okna a ostatní otvory, vč. místností. Lze u něj předpokládat, že potenciální pachatel má určitou znalost PZTS a ke své činnosti používá nástroje a přenosné přístroje, které mu dopomáhají ke snadnému vniknutí do objektu.

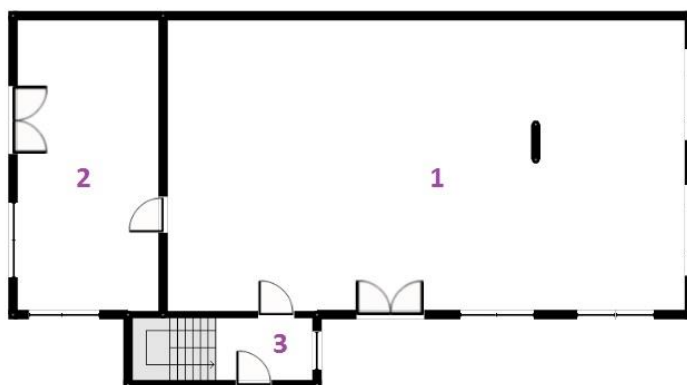
Třída prostředí je zvolena dle tabulky 2 v druhé kapitole podle normy ČSN EN 50 131 – 1, kde je i detailnější popis všech možných tříd. Platí, že pro všechny komponenty uvnitř je použita druhá třída – vnitřní všeobecné. Pro komponenty vně je použita čtvrtá třída – venkovní všeobecné. V tabulce 14 je uvedeno rozdělení tříd prostředí jednotlivých místností, stejně tak je k nim přiřazeno charakteristické číslo zaznačené v půdorysech (obrázek 23, 25).

Tabulka 14 Rozdělení místností do tříd prostředí

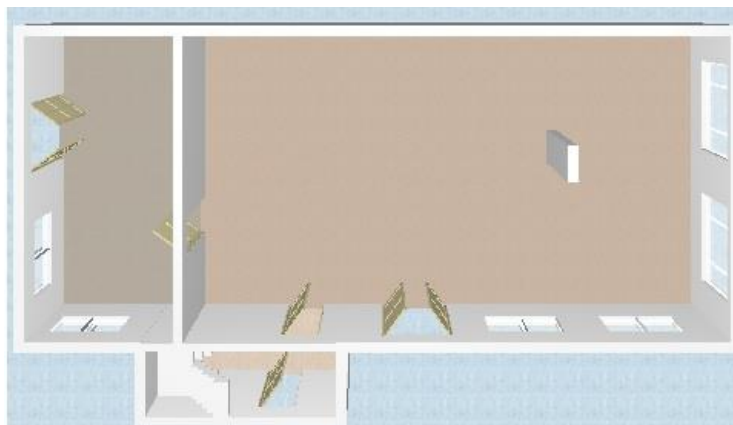
| Třída prostředí | Místnost              | Číslo místnosti | Třída prostředí | Místnost          | Číslo místnosti |
|-----------------|-----------------------|-----------------|-----------------|-------------------|-----------------|
| II.             | Dílna                 | 1               | II.             | Pánské WC         | 6               |
| II.             | Šatna pro zaměstnance | 2               | II.             | Společná kancelář | 7               |
| II.             | Chodba s poschodím    | 3               | II.             | Šatna pro vedení  | 8               |
| II.             | Chodba v 1. patře     | 4               | II.             | Kuchyň s jídelnou | 9               |
| II.             | Dámské WC             | 5               |                 |                   |                 |

### 7.3 Půdorysy zabezpečené budovy

Zabezpečená hlavní budova je dvoupodlažní – přízemí a první patro. Jejich půdorysy jsou znázorněny na obrázcích níže a pro oba návrhy zabezpečení jsou půdorysy totožné. Pro přízemí i první patro jsou půdorysy vyobrazeny v 2D, ve kterých jsou umístěny hodnoty 1 až 9. Význam hodnot je určen ve zmíněné tabulce 14. Popis použitého SW, který posloužil pro nákres půdorysů přízemí a prvního patra zabezpečené hlavní budovy, je pod půdorysy. Na obrázku 23 je půdorys přízemí hlavní budovy rozdělen do dvou místností, ke kterým přilehá vstupní chodba. Pro lepší představu je půdorys přízemí vyobrazen i v 3D prostoru (obrázek 24).



Obrázek 23 Půdorys přízemí hlavní budovy v 2D

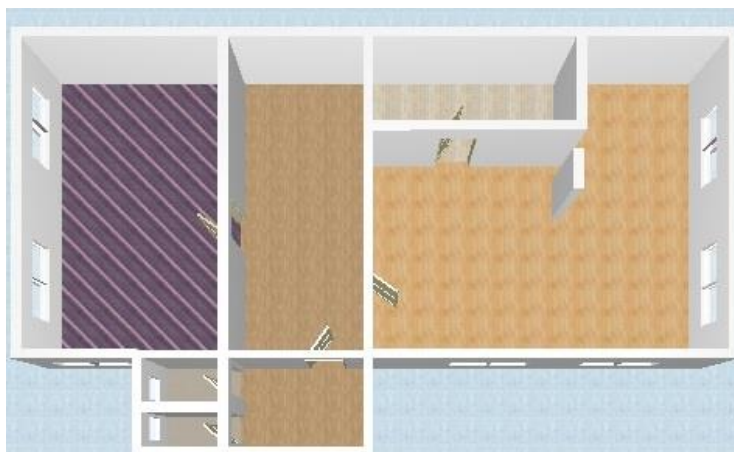


Obrázek 24 Půdorys přízemí hlavní budovy v 3D

Na obrázku 25 je znázorněn půdorys prvního patra, které je rozděleno do čtyř místností – šatna pro vedení, společná kancelář, chodba v prvním patře a společná kuchyně s jídelnou. V mezi podlaží se nachází dámské a pánské toalety. Stejně jako u půdorysu přízemí, je půdorys prvního patra znázorněn v 3D prostoru. (obrázek 26).



Obrázek 25 Půdorys hlavní budovy prvního patra v 2D

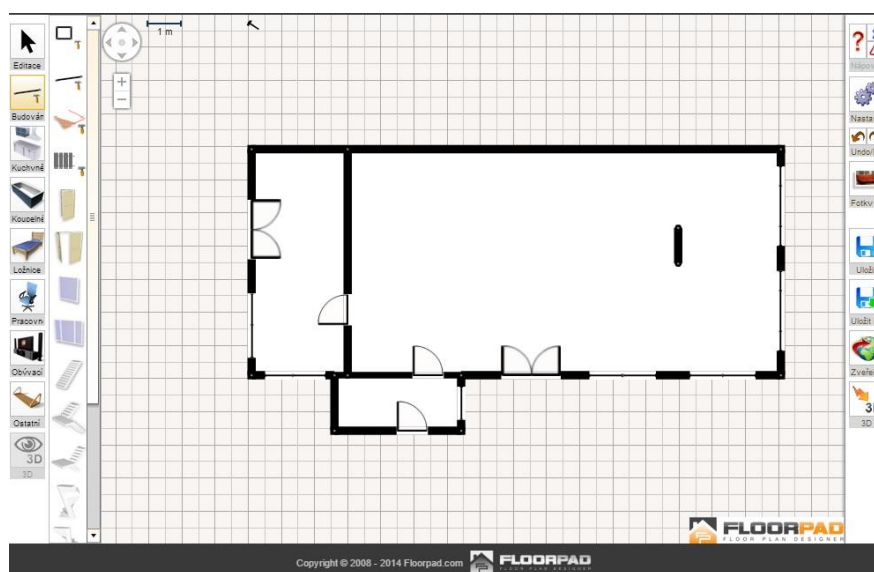


Obrázek 26 Půdorys hlavní budovy prvního patra v 3D



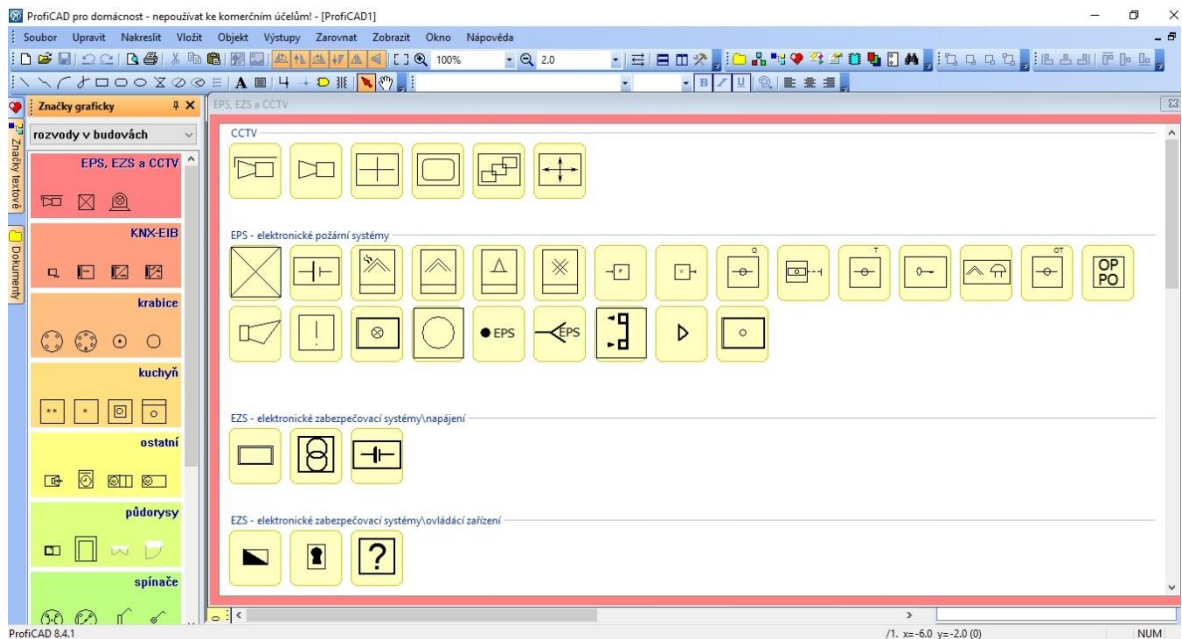
### 7.3.1 Použitý SW pro vytvoření půdorysů objektu

Ke tvorbě půdorysů byly použity 2 programy, FloorPAD a ProfiCAD. V programu FloorPAD byly vytvořeny jednotlivé půdorysy v dvourozměrném i trojrozměrném prostoru. Výhodou programu je čeština a jeho jednoduchost, kdy ovládání zvládne úplně každý za pár minut. Další výhodou programu je free verze, která však přináší i nevýhody, jako třeba omezení uložení jen jednoho půdorysu. Skvělou vlastností je 3D vizualizace pro lepší představivost, kde je možné si projít celý objekt.



Obrázek 27 Ukázka v programu FloorPAD

Pro rozvody a použití značek do půdorysů posloužil program ProfiCAD, který je určen zejména pro oblast elektro, ale je využíván i pro hydraulické a pneumatické dokumentace. Práce v ProfiCADu je poněkud náročnější, hlavně na trpělivost. Je v něm více ikoněk a možností, tudíž bylo s programem náročnější sžití. Obsahuje více než 2000 značek, pokud by však v knihovně nebyla požadovaná značka, tak má program funkci editor značek, ve kterém je snadné si vytvořit svou vlastní. Některé vlastnosti mi přišly zbytečné, zejména se jednalo o veškeré číslování čar, vč. značek. Velkou výhodou je v tomto programu možnost uložení výkresů ve formátu DXF, který značí kompatibilitnost se všemi programy CAD. Na obrázku 28 je ukázka značek CCTV i PZTS.



Obrázek 28 Ukázka značek v ProfiCADu

#### 7.4 Výběr vhodných prvků pro návrh zabezpečení – verze 1

Výběr vhodných prvků zabezpečovacího systému první verze je zvolen dle požadavků na protipatření hrozeb z výsledků bezpečnostní analýzy a finančních potřeb firmy, jak již bylo uvedeno v úvodu do praktické části. Na základě získaných teoretických informací při studiu oboru bezpečnostní technologie, systémy a management na Univerzitě Tomáše Bati ve Zlíně, jsem se rozhodl použít prvky od firmy Jablotron, a.s. Vzhledem k rozlehlosti areálu, kdy firma dodává prvky pro menší objekty. V úvahu připadaly i prvky od jiných výrobců, např. Digiplex, který poskytuje prvky zabezpečení pro střední a rozsáhlejší objekty nebo Magellan, který dodává jen bezdrátové provedení. Konkrétně budou použity prvky zabezpečení řady Jablotron 100, která poskytuje 100 % kompatibilitu. Celý návrh zabezpečovacího systému bude proveden sběrnice. Veškeré technické informace byly použity z katalogu produktů firmy [33], který uvádím v úvodu kapitoly, abych se na něj nemusel odkazovat samostatně u každého prvku. Pro sběrnice systém bylo přihlédnuto i kvůli požadavku na finanční stránku pořízení prvků, protože jsou levnější než u bezdrátové verze. Výhodou sběrnice návrhu je větší odolnost prvků a odpadá zde jakákoliv výměna a kontrola baterií u jednotlivých komponentů zabezpečení. Nevýhodou je náročnější montáž a instalace kabeláže.

- **Ústředna JA-101K**

Zvolená ústředna je určena pro menší firmy, což je vhodné pro zvolenou firmu, ale i pro rodinné domy, nebo kanceláře. Ústředna disponuje vestavěným komunikátorem GSM/GPRS, který umožňuje hlasovou, textovou nebo GPRS komunikaci s uživateli, či střediskem PCO (pult centralizované ochrany) podle přání majitele. K ústředně je možno připojit maximálně 50 prvků a obsahuje 1 svorkovnici pro případ rozšíření o sběrníkové prvky. Je rovněž vybavena modulem JA-110R, který slouží pro bezdrátové připojení prvků.



Obrázek 29 Ústředna JA-101K [26]

Základní nabídka ústředny je:

- 50 sběrníkových zón,
- 50 uživatelských kódů,
- 6 sekcí a 8 programovatelných výstupů,
- SMS reporty pro 8 uživatelů,
- Pro 5 uživatelů lze využívat hlasové reporty,
- 5 protokolů pro PCO a 4 nastavitelné PCO.
- 20 vzájemně nezávislých kalendářů.

- **Modul telefonního komunikátoru JA-190X**

Komunikátor byl zvolen pro možnost vzdálené komunikace s PCO. Mezi základní vybavení modulu patří přepět'ová ochrana. Digitální přenos na PCO je založen pomocí protokolů CID (Contact ID) a SIA. Splňuje druhý stupeň zabezpečení a třídu prostředí 2.



Obrázek 30 Modul telefonního komunikátoru JA-190X [26]

- **Klávesnice JA-113E a ovládací segment JA-192E**

Zvolený typ klávesnice byl z důvodu zlaté střední cesty poměru cena – výkon. Obsahuje RFID čtečku karet k ovládání zabezpečovacího systému. Klávesnice disponuje jedním ovládacím segmentem, ale v případě rozšíření může být vybavena až 20 segmenty typu JA-192E.

Ovládací segment umožňuje snadné ovládání funkcí systémů, tj. ovládaní sekcí, výstupů, tísňových volání a zobrazování stavu systému.



Obrázek 31 Klávesnice a ovládací segment [26]

- **Sběrníkový PIR detektor pohybu JA-110P**

Detektor pohybu byl zvolen k detekci v místnostech a i díky jeho dostatečné vzdálenosti detekce. Reakce na zjištěný pohyb osob je buď okamžitá, nebo zpožděná. Charakter detekce lze změnit použitím výměnných čoček pro ochranu dlouhých chodeb, pro vyloučení spuštění alarmu zvířetem nebo hlídání vertikální záclonou (JS-7904 chodbová, JS-7910 zvířecí a JS-7902 záclonová).



Obrázek 32 PIR detektor pohybu [26]

Napájení detektoru pohybu je ze sběrnice ústředny. Prvek je zařazen do druhé třídy prostředí a ideální výška instalace je ve 2,5 m a umožňuje detekci pohybu až do 12 m při úhlu detekce 120°.

- **Sběrníkový detektor rozbití skla JA-110B**

Pro ochranu skleněných ploch byl zvolen tento typ detektoru, který je vhodný pro objekty zabezpečení menších rozměrů. Je určen k vyhodnocení poplachu rozbitím skleněné výplně dveří, oken nebo výloh. Citlivost detektoru je nastavitelná a je napájen z ústředny. Splňuje požadavky pro zařazení mezi druhou třídu prostředí a taktéž druhý stupeň zabezpečení. Detekční dosah u detektoru rozbití skla je 9 m.



Obrázek 33 Detektor rozbití skla [26]

- **Sběrníkový magnetický detektor JA-111M**

Byl zvolen na základě plnohodnotné kompatibility a sabotáži krytu, která je aktivována při manipulaci s ochranným krytem. Je určen k detekci otevírání dveří nebo oken po oddálení permanentního magnetu od senzoru. Je schopen spustit poplach při vstupu narušitele okamžitě nebo s nastaveným zpožděním. Tak jako již zmíněné prvky splňuje zvolený 2. stupeň zabezpečení, vč. druhé třídy prostředí.



Obrázek 34 Sběrníkový magnetický detektor [26]

- **Sběrníkový kombinovaný detektor kouře a teploty JA-110ST**

Jelikož je třeba ošetřit hrozbu vzniku požáru, k čemuž byl vybrán detektor kouře a teploty. Umožňuje 3 základní funkce detekce. První funkcí je detekce kouře a zvýšení teploty, druhou funkcí je detekce kouře nebo zvýšení teploty a třetí funkcí je detekce jen kouře nebo jen zvýšení teploty. Detektor splňuje požadavky vyhlášky č. 23/2008 Sb., o požární ochraně staveb. Poplach je vyhlášen, pokud teplota dosáhne 60°C až 70°C.



Obrázek 35 Detektor kouře a teploty [26]

- **Venkovní siréna JA-111A**

Slouží k signalizaci poplachu ve venkovním prostředí. Siréna je vybavena sabotážními senzory, komunikace je založena po sběrnici na protokolu „Jablotron“ a je napájena z ústředny. Obsahuje záložní akumulátor 4,8 V/ 1800 mAh, jehož životnost je cca 3 roky. Splňuje požadavky 4. třídy prostředí – venkovní všeobecné. Hlasitost vyhlášení poplachu lze nastavit až na 110 dB.



Obrázek 36 Venkovní siréna [26]

- **Vrchní kryt sirény JA-111A**

Zvolená sběrnice siréna je dodávána bez krytu, tudíž je nutné pořídit pro ni kryt. Zvolený typ je určen ke zvolenému typu sirény.



Obrázek 37 Kryt venkovní sirény [26]

- **Bezdotyková RFID karta JA-190J**

Jako ovládací prvek byla zvolena RFID karta, která obsahuje jedinečný kód Jablotronu, pomocí kterého může být provedeno odstřežení nebo zastřežení systému. Bezdotyková přístupová karta RFID je kompatibilní se systémem Jablotron řady 100. Pracuje na frekvenci 125 kHz.



Obrázek 38 Přístupová karta RFID [26]

- **Záložní akumulátor SA214-18**

Bezúdržbový záložní akumulátor slouží převážně v době, když by došlo k výpadku sítě. Ústředna je k tomuto akumulátoru, který má napětí 12 V a disponuje kapacitou 18 Ah, připojena. Akumulátor tohoto typu není určen výhradně pro prvky firmy Jablotron, a.s.



Obrázek 39 Záložní akumulátor [26]



- **GSM kamera EYE-02**

Zvolením GSM bezpečnostní kamery je možno sledovat okolí objektu vzdáleně přes PCO. Komunikuje s ústřednou pomocí GSM sítě. Díky dodávanému software JabloTool lze sledovat záběry živě na všech dostupných prohlížečích. Připojením kamery na PCO je možné mít objekt 24 hodin pod kontrolou. Obsahuje 5 detektorů – pohybový PIR, zvukový, detektor rozbití skla, náklonový a vibrační, detektor pohybu v obraze. Kameru je možno ovládat pomocí dálkového ovladače, sms příkazů, volání nebo internetu. Komunikace může být až na 10 zvolených čísel nebo emailů. Podle příslušného nastavení zasílá poplach ve formě mms, sms, volání, emailu nebo na PCO.



Obrázek 40 GSM kamera EYE-02 [26]

- **Záznamové zařízení**

Jako záznamové zařízení pro archivaci videí poslouží NVR (Network Video Recorder) rekordér typu NVR 104C ELN, ke kterému lze připojit až 4 kamery a 1 interní disk o maximální velikosti 4 TB.



Obrázek 41 Rekordér [27]

- **Pevný disk Western Digital SATA**

Pevný disk Western Digital Purple s kapacitou 1 TB byl vyvinut pro kamerové a sledovací systémy. Je navržen pro náročný nepřetržitý provoz s vysokým rozlišením. S pořízením tohoto typu je zaručena větší spolehlivost a jistota uložených záznamů.



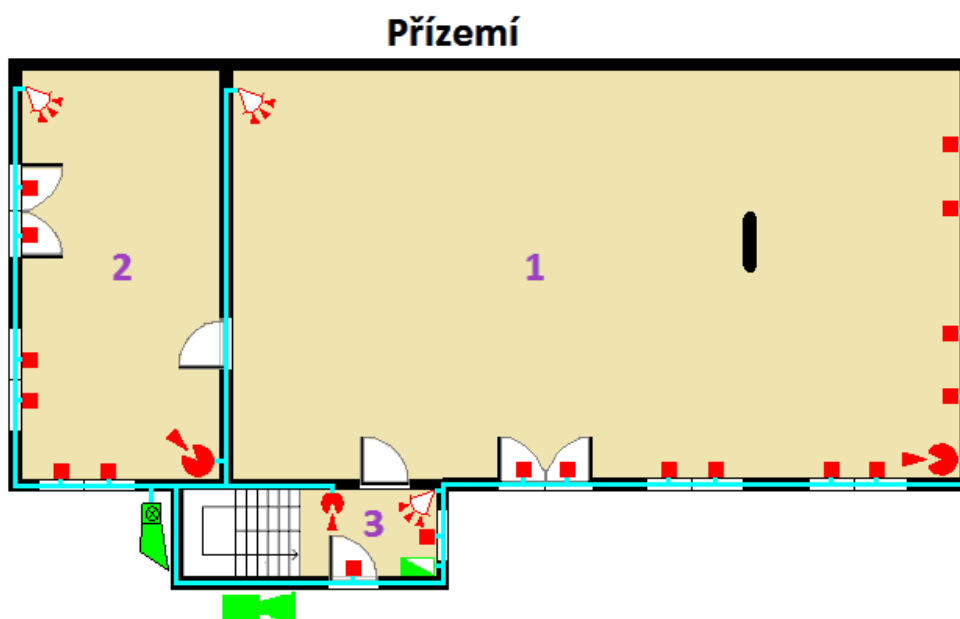
Obrázek 42 Pevný disk WD Purple [28]

- **Kabeláž**

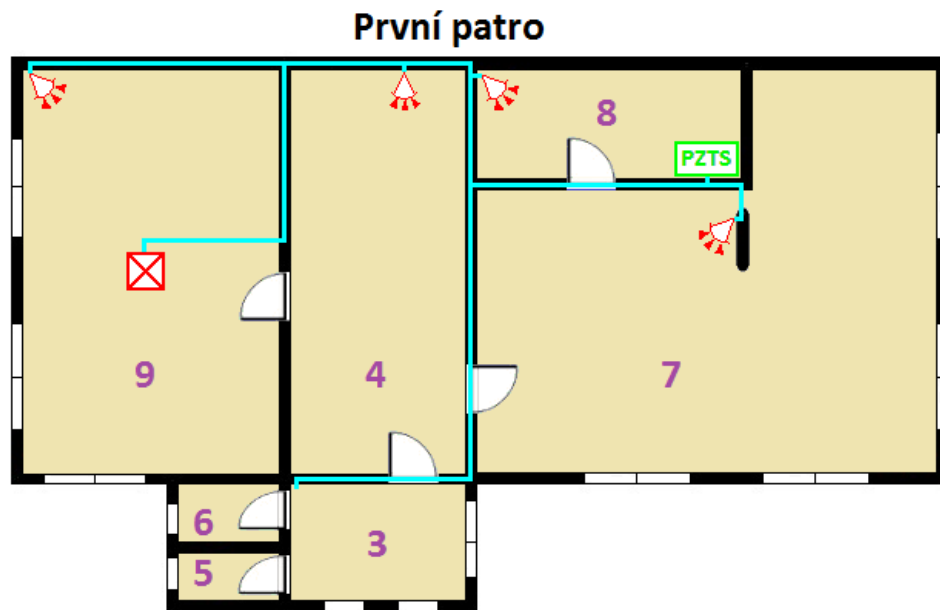
Typ kabeláže byl zvolen SYKFY 6x0,5 mm<sup>2</sup>. Tento typ bohatě postačí, protože pro všechny zabezpečovací prvky postačí průřez 0,5 mm<sup>2</sup>. Šesti-žilový kabel byl zvolen z důvodu venkovní sířeny, která potřebuje více vodičů. Kabeláž je stíněná. Je určen pro slaboproudé rozvody PZTS přičemž každý vodič je barevně odlišen.

## 7.5 Rozmístění prvků zabezpečení do půdorysů – verze 1

V následující podkapitole jsou umístěny návrhy zabezpečení s rozmístěním prvků, vč. legendy použitých značek. Na půdorysu přízemí hlavní budovy (obrázek 43) je ochrana řešena prostorově, ale i plášťově. Zatímco zabezpečení prvního patra (obrázek 44) je řešeno jen prostorově.




Obrázek 43 Umístění prvků v přízemí – verze 1



Obrázek 44 Umístění prvků v prvním patře – verze 1

V následující tabulce 15 jsou uvedeny vysvětlivky ke všem použitým značkám v půdorysech přízemí a prvního patra. Typy schématických značek v legendě jsou podle přílohy PI, kde jsou základní značky uvedeny dle normy ČSN EN 50 131.

Tabulka 15 Legenda použitých značek – verze 1

| Značka  | Popis značky             |
|---|--------------------------|
|  | Detektor rozbití skla    |
|  | Detektor pohybu          |
|  | Magnetický detektor      |
|  | Detektor kouře a teploty |
|  | Ústředna                 |
|  | Klávesnice               |
|  | Kamera                   |
|  | Venkovní siréna          |

## 7.6 Konfigurace systému a zóny zabezpečovacího systému – verze 1

Ochrana přízemí hlavní budovy je řešena prostorově, ale i plášťově z důvodu nízkého umístění oken a přístupných vrat, vč. dveří. Nalevo zvenčí od hlavních dveří je umístěna kamera, která je připojena na PCO, který sleduje zabezpečovaný objekt v době, když je prázdný. Zatímco zabezpečení prvního patra (obrázek 44) je řešeno jen prostorově, protože okna jsou umístěna ve výšce cca 5 m a nepředpokládá se, že pachatel vyšplhá po kolmých stěnách. Samozřejmě je zde hrozba použití žebříku. Potom se sice dostane do prvního patra přes okna, ale následný pohyb je zaznamenán pohybovými PIR detektory umístěnými uvnitř prostor a vyhlášením poplachu. V kuchyni s jídelnou je jediný detektor kouře a teploty, protože je zde největší riziko vzniku požáru. Dámské a pánské záchody v mezi podlaží nejsou zabezpečeny, protože skrz malé rozměry oken se pachatel dovnitř nedostane. Pokud se na záchody dostane skrz chodbu, je jeho pohyb zachycen pohybovým detektorem umístěným ve vstupní chodbě s poschodím.

Zabezpečovací systém je navržen do dvou režimů. Režim 1A, u kterého se jedná o zastřežení objektu plášťově i prostorově. Tento režim bude v provozu, když se v objektu nenachází žádný ze zaměstnanců a ústředna je uvedena do stavu hlídání. Režim je spuštěn po pracovní době, o víkendech nebo o svátcích. Stav zastřežení je uveden do provozu vedením firmy nebo vedoucím výroby. Po uvedení zabezpečovacího systému do stavu zastřežení má tento zaměstnanec 40 vteřin na uzamknutí a opuštění budovy.

Režim 1B je ve stavu odstřežení, do kterého je uveden vedoucím výroby, nebo vedením firmy. Jen tito zaměstnanci mají možnost obsluhovat zabezpečovací systém. Stav odstřežení je uveden přiložením karty a následným zadáním kódu z důvodu zvýšení úrovně bezpečnosti, ke klávesnici s čtečkou. Klávesnice je umístěna při vstupu do hlavní budovy po pravé straně, takže čas potřebný k odstřežení, který je 20 vteřin, je dostačující. Pokud by v tomto časovém intervalu nedošlo ke správnému zadání kódu, bude vyhlášen poplach. Zóna tamper určená pro ústřednu a 24 hodinová zóna, která obsahuje detektor kouře a teploty, pracují v obou režimech.

Systém je navržen do několika zón, které jsou rozděleny podle místností, tak aby v případě vyhlášení poplachu bylo jednodušší zjistit, kde byl poplach vyvolán. Kamerový systém bude pracovat jen v režimu 1A, tedy stavu zastřežení a bude napojen na PCO, protože je zbytečné, aby kamera jela i v režimu 1B, kdy je většina zaměstnanců v budově. Záznam z kamer je ukládán na záznamové zařízení po dobu 3 dnů.

Rozdělení jednotlivých zón je v tabulce 16, ve které je označení pro zónu, místnost, prvky nacházející se v místnosti a jejich počet, vč. typu zóny. Pod tabulkou jsou jednotlivé zóny vysvětleny.

Tabulka 16 Rozdělení zón – verze 1

| Označení zóny | Místnost              | Prvky v místnosti (počet)  | Zóna                   |
|---------------|-----------------------|--|------------------------|
| 1             | Chodba s poschodím    | Detektor pohybový (1), magnetický (2), tříštění skla (1), klávesnice (1) | Zpožděná               |
| 2             | Dílna                 | Detektor pohybový (1), magnetický (10), tříštění skla (1)                | Okamžitá               |
| 3             | Šatna pro zaměstnance | Detektor pohybový (1), magnetický (6), tříštění skla (1)                 | Okamžitá               |
| 4             | Chodba v 1. patře     | Detektor pohybový (1)  | Okamžitá               |
| 5             | Kancelář              | Detektor pohybový (1)  | Okamžitá               |
| 6             | Šatna pro vedení      | Detektor pohybový (1) a ústředna (1)                                     | Okamžitá + tamper      |
| 7             | Kuchyň s jídelnou     | Detektor pohybový (1) a detektor kouře a teploty (1)                     | Okamžitá + 24 hodinová |

- Zóna zpožděná – zóna pracuje tak, že po vstupu hlavními dveřmi do budovy je aktivován magnetický a pohybový detektor a automaticky je spuštěn čas, který je potřebný k odstřežení systému, v tomto případě 20 vteřin. Po uvedení systému do stavu zastřežení při odchodu má zaměstnanec 40 vteřin pro opuštění a uzamknutí budovy. Pokud zaměstnanec v tomto časovém úseku nestihne zadat kód pro odstřežení, je vyhlášen poplach. Stejný případ pokud nestihne v časovém intervale opustit budovu po zastřežení.
- Zóna okamžitá – pokud je systém v režimu odstřežení, tak nedojde k vyhlášení poplachu, i když se v chráněných prostorách pohybují zaměstnanci. Ve stavu zastřežení při narušení prostor dojde již k vyhlášení poplachu.
- Zóna 24 hodin a tamper – je určena pro detektor kouře a teploty a zóna tamper výhradně pro ústřednu. Obě zóny pracují i ve stavu odstřežení.

## 7.7 Cenová kalkulace vybraných zabezpečovacích prvků – verze 1

Ceny, které jsou uvedeny v tabulce 17, jsou včetně daně z přidané hodnoty (DPH). Zmíněné hodnoty prvků jsou průměrem několika cen předních výrobců zabezpečovacích systémů. Do cenové kalkulace není započtena montáž, zednické práce a servis, protože každá firma si za tyto služby účtuje rozdílné ceny.

Tabulka 17 Cenová kalkulace – verze 1

| Název   | Počet kusů | Cena/kus/m [Kč] | Cena celkem [Kč] |
|---|------------|-----------------|------------------|
| Ústředna JA-101K                              | 1          | 8 875           | 8 875            |
| Modul telefonního komunikátoru JA-190X        | 1          | 1 220           | 1 220            |
| Klávesnice JA-113E                            | 1          | 1 683           | 1 683            |
| PIR detektor pohybu JA-110P                   | 7          | 569             | 3 983            |
| Detektor rozbití skla JA-110B                 | 3          | 827             | 2 481            |
| Magnetický detektor JA-111M                   | 18         | 367             | 6 606            |
| Kombinovaný detektor kouře a teploty JA-110ST | 1          | 1 058           | 1 058            |
| Venkovní siréna JA-111A                       | 1          | 1 295           | 1 295            |
| Kryt na sirénu JA-111A                        | 1          | 592             | 592              |
| Bezdotyková RFID karta JA-190J                | 11         | 73              | 803              |
| Záložní akumulátor SA214-18                   | 1          | 1 139           | 1 139            |
| GSM kamera EYE-02                             | 1          | 8 076           | 8 076            |
| Záznamové zařízení NVR 104C ELN               | 1          | 2 923           | 2 923            |
| Pevný disk Western Digital Purple             | 1          | 1 639           | 1 639            |
| Stíněný kabel SYKFY 6x0,5 mm                  | 300        | 8               | 2 400            |
| <b>Cena celkem</b>                            |            |                 | <b>44 773 Kč</b> |

## 7.8 Způsob hlášení poplachu a zásah

Vyhlášený poplach bude signalizován opticky na klávesnici pomocí LED, jež oznamuje zónu, ve které byl poplach vyhlášen. Tak i akusticky venkovní sirénou, která dosahuje hlasitosti 110 dB. Jelikož ústředna disponuje vestavěným GSM/GPRS komunikátorem, tak při vyhlášení poplachu dojde k vytočení čísla majitele.

Zpráva o poplachu bude přenesena i na PCO, který objekt monitoruje ve stavu zastřežení u prvního návrhu zabezpečení, tak i ve stavu odstřežení u druhé verze návrhu. Zásah je zajištěn bezpečnostní agenturou, která bude dodávat zabezpečované prvky. Je možné se s firmou domluvit i na montáži návrhu zabezpečovacího systému pro tento reálný objekt. Agentura má sídlo ve Valašském Meziříčí, které je vzdálené 13 km od firmy, jak již bylo zmíněno v kapitole 6. Dojezd zásahové jednotky na místo trvá okolo 15 minut, která následně provede patřičné kroky při vyhlášeném poplachu.

## 7.9 Údržba systému

Bezpečnostní agentura bude provádět i údržbu systému. Zabezpečovaná firma, zmíněná v úvodu do praktické části, bude s touto agenturou smluvně vázána. Ve smlouvě budou uvedeny pravidelné kontroly zabezpečovacího systému a samotných prvků, u kterých v případě nefunkčnosti bude provedena oprava. Požadavek na přezkoušení kompletního systému je jednou za půl roku a s kontrolou údržby zabezpečovacího systému se počítá jednou ročně.

## 7.10 Legislativa a normy

Všechny použité komponenty zabezpečovacího systému, které jsou zmíněny výše v kapitole, splňují požadavky pro daný stupeň zabezpečení a třídu prostředí. Požadavky na komponenty jsou obsaženy v následujících právních předpisech:

- ČSN EN 50 131 – Poplachové zabezpečovací a tísňové systémy,
- ČSN EN 50 132 – Kamerové systémy,
- nařízení vlády č. 616/2006 Sb. o technických požadavcích na výrobky podle hlediska elektromagnetické kompatibility,
- zákon č. 22/1997 Sb. o technických požadavcích na výrobky.

Prvky zabezpečení taktéž splňují prohlášení o shodě, vč. příslušných certifikátů, které jsou uvedeny v přílohách PII, PIII a PIV, konkrétně jde o certifikáty firmy Jablotron.

## 8 NÁVRH ZABEZPEČOVACÍHO SYSTÉMU – VERZE 2

Kapitola je zaměřena na návrh zabezpečovacího systému, který vychází z předchozí verze a je vhodně rozšířený o doplňující prvky zabezpečení. Hlavním rozdílem je zde použití mechanických zábranných systémů, tj. bezpečnostních dveří a folii na okna, vč. trezoru. Stupeň zabezpečení s třídou prostředí je stejný jako u prvního zabezpečovacího systému. Půdorysy zabezpečované budovy a software použitý při jejich vytváření je taktéž stejný. Způsob vyhlášení poplachu, údržba systému a legislativa, vč. norem, také nebude zmíněn ve verzi 2, protože je stejný s první verzí.

Ve druhé verzi jsou zmíněny požadavky na zabezpečení hlavní budovy, které se oproti první verzi liší. Také rozšiřující a doplňující prvky zabezpečení jsou uvedeny v následující kapitole. Rozmístění prvků do půdorysů návrhu zabezpečení a konfigurace zabezpečovacího systému, vč. zón a cenové kalkulace zabezpečovacích komponent, je taktéž uvedena ve druhém návrhu zabezpečení.

### 8.1 Požadavky na návrh zabezpečení – verze 2

První verze zabezpečovacího systému vytvořená v kapitole 7 byla navržena podle určitých požadavků, ze kterých se vycházelo. Na základě svých zkušeností získaných při studiu oboru bezpečnostní technologie, systémy a management na Univerzitě Tomáše Bati ve Zlíně, fakulty aplikované informatiky, jsem se rozhodl při návrhu zabezpečení verze 2, vycházet z předchozího zabezpečení a vhodně jej rozšířit a doplnit o prvky zabezpečení, vč. již mechanických zábranných prvků.

### 8.2 Doplňující vybrané prvky pro návrh zabezpečení – verze 2

V této kapitole jsou zmíněny jen prvky zabezpečení, které jsou použity v rozšiřujícím návrhu zabezpečení druhé verze, ale nebyly použity v první. Zvolené technické prvky a jejich parametry byly převzaty z katalogu prvků [33] firmy Jablotron Alarms.

- **Sběrníkový PIR detektor pohybu s kamerou JA-120PC**

Detektor obsahuje vestavěný kamerový modul a umožňuje detekovat pohyb včetně vizuální signalizace poplachu, který bude umístěn v kanceláři, aby měl majitel důkazy při vloupání. Při zaznamenání a spuštění poplachu jsou pořízeny sekvence fotografií v JPEG formátu a rozlišení 640x480 bodů. Fotografie jsou uloženy ve vnitřní paměti detektoru a na



ústřednu jsou přenášeny v komprimované podobě, odkud jsou posílány na PCO. Úhel detekce je 12 m při úhlu 50°. MicroSD karta může disponovat paměti 1 TB až 2 TB.



Obrázek 45 PIR detektor s kamerou [26]

- **Sběrníkový duální PIR a MW detektor pohybu JA-120PW**

Detektor tohoto typu je určen k prostorové detekci pohybu osob uvnitř budov. Díky kombinaci PIR a MW detekce, je vysoce odolný proti možnému výskytu falešných poplachů, proto jsem se rozhodl jej použít v ostatních místnostech hlavní budovy. Při vyhlášení poplachu musí být aktivován MW detektor, který reaguje na předešlou aktivaci PIR. Vlastnosti jsou stejné jako u předešlých detektorů, dosah detekce je 12 m pod úhlem 110° se základní čočkou.



Obrázek 46 Duální detektor PIR/MW [26]

- **Sběrníkový detektor pohybu a rozbití skla JA-120PB**

Detektor byl zvolen na základě větší ochrany zabezpečení, který bude rozšiřovat plášťovou ochranu ve společné kanceláři prvního patra. Detektor je vybaven dvěma senzory, přičemž jeden z nich detekuje pohyb osob v prostoru a druhý senzor detekuje tříštění skla. Detekční

vzdálenost detektoru je 9 m, při ideální instalaci ve výšce 2,5 m. Splňuje druhý stupeň zabezpečení a druhou třídu prostředí.



Obrázek 47 Detektor pohybu a rozbití skla [26]

- **Sběrníkový záplavový detektor JA-110F**

Zvolením záplavového detektoru je ošetřena hrozba zaplavení, jež bude umístěn v kuchyni s jídelnou. Detektor obsahuje dvě elektrody, které při zaplavení vyšlou signál aktivace. Do stavu klidu je detektor uveden, jakmile zaplavení jeho elektrod odezní. Neobsahuje tamper a je třeba jej instalovat pár cm nad podlahu pro včasnou aktivaci poplachu. Používá se do místností, kde se teplota pohybuje v rozmezí -10 až 40 °C.



Obrázek 48 Záplavový detektor [26]

- **Bezpečnostní dveře Magnum**

Bezpečnostní protipožární dveře typu Magnum jsou zařazeny do bezpečnostní třídy 3. kategorie. Jejich protihluková izolace je 44 dB. Tepelná propustnost u dveří Magnum je 1,4. Čím nižší hodnota u propustnosti, tím méně tepla dveře propouští pryč. Disponují dvojitým těsněním s tloušťkou křídla 56 mm. Obsahují 15 zamykacích bodů, které jsou při větším

počtu zamykacích bodů chráněny před vysunutím z pantů. Protipožární odolnost je EI 30, tedy 30 minut. Vnitřní vodorovné výztuže jsou zhotoveny z kalené oceli. Disponují oboustranným ocelovým pláštěm. Dveře i s montáží stojí 22 990 Kč, vč. DPH.



Obrázek 49 Bezpečnostní dveře Magnum [31]

- **Bezpečnostní folie SCX**

Bezpečnostní folie SCX je třívrstvá. Ze všech bezpečnostních folií dodávané nejmenovanou firmou je nejsilnější. Obsahuje atest P2A a samotná tloušťka folie je 0,35 mm. Instalací folií jsou okna chráněna před prohozením nebezpečných předmětů, zejména kamenů. Folie také chrání zaměstnance před úrazem skla, například před poraněním o střepy rozbitého skla.

- **Stěnový trezor ST-132E/I**

Trezor o hmotnosti 35 kg s vnitřními rozměry 395x330x220 mm. Pro zabezpečenou firmu bude sloužit k úschově finanční hotovosti a cenných dokumentů, které se ve firmě nachází volně na polici. Je určen k instalaci do zdi a obsahuje přestavitelnou polici. Trezor má certifikát normy EN 1143-1 pro bezpečnostní třídu I, jež je určena pro domácnosti a menší podniky. Také certifikát NBÚ, který ověřuje způsobilost technických prostředků typu 3 – tajné.



Obrázek 50 Stěnový trezor [32]

- **Sběrnice tísňové tlačítka JA-112J**

Při jakémkoliv nebezpečí, které není vyhlášeno ústřednou, jsou v objektu umístěny 2 tísňové tlačítka pro možnost vyvolat poplach zaměstnancem. Napájení tlačítka je z ústředny pomocí sběrnice. Splňuje požadavky pro druhou třídu prostředí i druhý stupeň zabezpečení. Tísňové tlačítka jsou vybavena indikační LED diodou, která svítí zeleně, nebo červeně.



Obrázek 51 Tísňové tlačítka [26]

- **Ochranný kryt KAC-EYE**

Venkovní plastový kryt, určený pro bezpečnostní monitorovací kameru GSM EYE-02 před působením vnějších vlivů.



Obrázek 52 Ochranný kryt pro kameru [26]

- **Záložní akumulátor SA214-26**

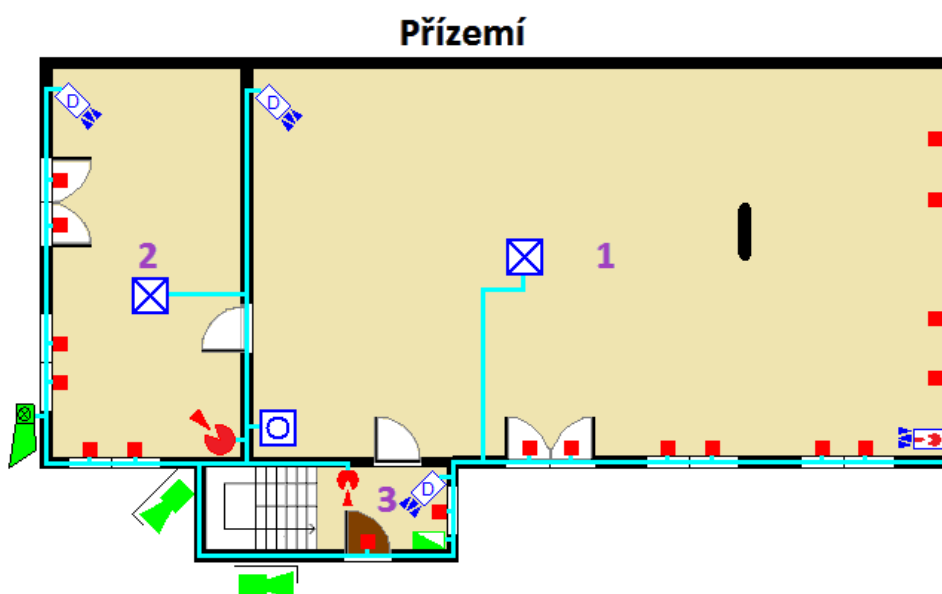
Z důvodu většího počtu použitých prvků a jejich odběru v mA, musí být použit výkonnější akumulátor. Tento typ záložního akumulátoru při výpadku elektrické energie disponuje kapacitou 26 Ah.



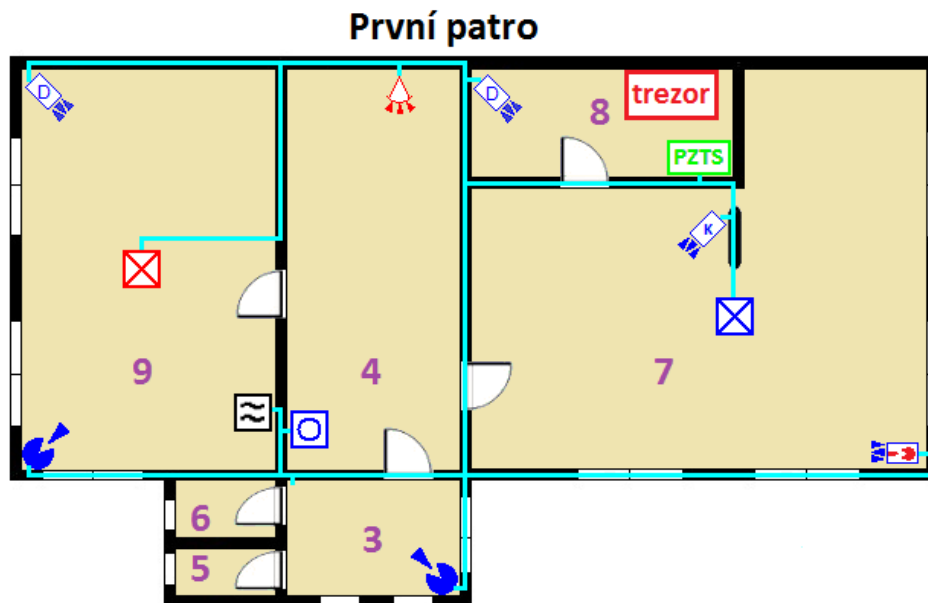
Obrázek 53 Záložní akumulátor SA214-26 [26]

### 8.3 Rozmístění prvků zabezpečení do půdorysů – verze 2

V následující kapitole jsou umístěny půdorysy návrhu zabezpečení s rozmístěním prvků, vč. legendy použitých značek. Na půdorysech přízemí hlavní budovy (obrázek 54) a prvního patra (obrázek 55) je ochrana řešena prostorově, ale i plášťově. Rozmístění jednotlivých prvků v půdorysech vychází z předchozího návrhu zabezpečení, který je rozšířen a doplněn o výše zmíněné prvky, nebo jsou některé prvky z první verze zabezpečovacího systému vyměněny za spolehlivější a odolnější vůči planým poplachům.
















Obrázek 54 Umístění prvků v přízemí – verze 2



Obrázek 55 Umístění prvků v prvním patře – verze 2

Jelikož je druhý návrh zabezpečovacího systému rozšířen o další prvky zabezpečení, je rozšířena i legenda použitých značek znázorněna v tabulce 18.

Tabulka 18 Legenda použitých značek – verze 2

| Značka  | Popis značky                            |
|---|---|
|  | Magnetický detektor                     |
|  | Detektor tříštění skla                  |
|  | Duální PIR, MW detektor                 |
|  | Detektor pohybu s kamerou               |
|  | Pohybový detektor                       |
|  | Záplavový detektor                      |
|  | Detektor tříštění skla s PIR detektorem |
|  | Detektor kouře a teploty                |
|  | Tišňové tlačítko                        |
|  | Venkovní siréna                         |
|  | Kamera s ochranným krytem               |
|  | Klávesnice                              |
|  | Ústředna                                |

## 8.4 Konfigurace systému a zóny zabezpečovacího systému – verze 2

Podle použitých prvků v přízemí hlavní budovy (obrázek 54) je ochrana řešena prostorově i plášťově, přičemž plášťová ochrana je zesílena vyměněním vchodových dveří za bezpečnostní dveře a na všechny okenní otvory je instalována bezpečnostní folie. Prostorová ochrana je díky duálním detektorům umístěným v chodbě, dílně a šatně pro zaměstnance, odolnější vůči planým poplachům. V návrhu zabezpečení verze 2 je v přízemí ošetřena hrozba vzniku požáru detektory kouře a teploty umístěnými v šatně a dílně, kde se také nachází jedno ze dvou tísňových tlačítek.

Zabezpečení prvního patra (obrázek 55) ve verzi 2 je rozšířeno o plášťovou ochranu pomocí detektorů tříštění skel, aby byla ošetřena hrozba použití žebříku při snaze dostat se do prvního patra. Prostorová ochrana je rozšířena o tísňové tlačítko na chodbě a záplavový detektor v kuchyni. Největší důraz je kladen na zabezpečení kanceláře, kde hrozí významné finanční ztráty. Kancelář je rozšířena o detektor pohybu v kombinaci s detektorem tříštění skla a o duální detektor pohybu s kamerou. Šatna je vybavena trezorem na uschování dokumentů a peněžní hotovosti. I na okna prvního patra jsou umístěny bezpečnostní folie, tak aby měl pachatel v co největší možné míře znesnadněn přístup dovnitř budovy. V kuchyni s jídelnou, kanceláři, vč. šatny pro vedení, jsou základní pohybové PIR detektory vyměněny za duální detektory, přičemž zabezpečení kanceláře je ještě více zesíleno detektorem kouře a teploty.

Konfigurace systému druhého návrhu zabezpečení vychází z konfigurace předchozí verze. Zabezpečovací systém je navržen do dvou režimů. Režim 2A znamená stav zastřežení, který je nastaven po pracovní době, o víkendech a o svátcích. Při zastřežení je budova chráněna plášťově i prostorově. Režim 2B je ve stavu odstřežení, který je uveden do chodu v pracovní době od 6:00 do 15:00, když se v objektu pohybují zaměstnanci. Zóna tamper určená pro ústřednu a 24 hodinová zóna obsahující všechny 4 detektory, pracují v obou režimech.

Ve zpožděné zóně zabezpečovacího systému druhé verze je časový interval nastaven na 20 vteřin, který je určen pro opuštění budovy po uvedení systému do zastřeženého stavu. Stejný čas je potřebný pro zadání kódu do uvedení odstřeženého stavu po vstupu do budovy. Pokud by v časovém intervalu nedošlo k zadání kódu, bude vyhlášen poplach. Pro odstřežení nebo zastřežení systému je oprávněn jen vedoucí výroby nebo vedení firmy.

Zabezpečovaný systém druhé verze je rozdělen do několika zón, který se od předchozího návrhu liší umístěnými prvky v jednotlivých místnostech, tedy zónách. Kamerový systém, který je napojen na PCO bude pracovat v obou režimech a záznam z kamer je ukládán po dobu 3 dnů.

Tabulka 19 Rozdělení zón – verze 2

| Označení zóny | Místnost                                       | Prvky v místnosti (počet)   | Zóna              |
|---------------|--|---|-------------------|
| 1             | Chodba s poschodím                             | Detektor duální PIR, MW (1), magnetický (2), tříštění skla (1), siréna (1), klávesnice (1)  | Zpožděná          |
| 2             | Dílna  | Detektor duální PIR, MW (1), magnetický (10), tříštění skla s PIR (1), tísňové tlačítko (1) | Okamžitá          |
| 3             | Šatna pro zaměstnance                          | Detektor duální PIR, MW (1), magnetický (6), tříštění skla (1)                              | Okamžitá          |
| 4             | Chodba v 1. patře                              | Detektor pohybový (1), tříštění skla (1), tísňové tlačítko (1)                              | Okamžitá          |
| 5             | Kancelář                                       | Detektor duální PIR s kamerou (1), duální tříštění skla s PIR (1)                           | Okamžitá          |
| 6             | Šatna pro vedení                               | Detektor duální PIR, MW (1), ústředna (1)   | Okamžitá + tamper |
| 7             | Kuchyň s jídelnou                              | Detektor pohybový (1), záplavový (1) a tříštění skla (1)                                    | Okamžitá          |
| 8             | Kuchyň, kancelář, dílna, šatna pro zaměstnance | Detektor kouře a teploty (4)  | 24 hodinová       |

Popis zón je stejný jako u návrhu zabezpečovacího systému verze 1 v kapitole 7. Jediný rozdíl je u zpožděné zóny, kdy čas potřebný k zadání kódu na klávesnici pro odstřežení nebo k opuštění budovy po zastřežení, je 20 vteřin. U první verze návrhu zabezpečovacího



systemu měl zaměstnanec odpovědný za obsluhu systému 40 vteřin pro opuštění budovy po zadání kódu do stavu zastřežení.

## 8.5 Cenová kalkulace vybraných zabezpečovacích prvků – verze 2

V cenové kalkulaci jsou ceny zabezpečovacích prvků uvedeny včetně DPH. Hodnota použitých prvků zabezpečení vyjadřuje průměr cen od více dodavatelů, protože ty se u většiny z nich liší. V celkové hodnotě návrhu zabezpečení druhé verze, není započtena jakákoliv montáž, demontáž a jiné práce spojeny s uvedením systému do funkčního stavu. Montáž a veškeré práce spojené s ní si každá firma úrokuje podle sebe.

Tabulka 20 Cenová kalkulace – verze 2

| Název prvku                                   | Počet kusů | Cena/kus/m<br>[Kč] | Cena celkem [Kč] |
|---|------------|--------------------|------------------|
| Ústředna JA-101K                              | 1          | 8 875              | 8 875            |
| Modul telefonního komunikátoru<br>JA-190X     | 1          | 1 220              | 1 220            |
| Klávesnice JA-113E                            | 1          | 1 683              | 1 683            |
| PIR detektor pohybu JA-110P                   | 1          | 569                | 569              |
| Detektor rozbití skla JA-110B                 | 4          | 827                | 3 308            |
| Magnetický detektor JA-111M                   | 18         | 367                | 6 606            |
| Kombinovaný detektor kouře a teploty JA-110ST | 4          | 1 058              | 4 232            |
| Venkovní siréna JA-111A                       | 1          | 1 295              | 1 295            |
| Kryt na sirénu JA-111A                        | 1          | 592                | 592              |
| Bezdotyková RFID karta JA-190J                | 11         | 73                 | 803              |
| Záložní akumulátor SA214-26                   | 1          | 1 981              | 1 981            |
| GSM kamera EYE-02                             | 2          | 8 076              | 16 152           |
| Záznamové zařízení NVR 104C<br>ELN            | 1          | 2 923              | 2 923            |

|  |     |        |                   |
|--|-----|--------|-------------------|
| <b>Pevný disk Western Digital Purple</b>                   | 1   | 1 639  | 1 639             |
| <b>Stíněný kabel SYKFY 6x0,5 mm</b>                        | 400 | 8      | 3 200             |
| <b>Sběrníkový PIR detektor pohybu s kamerou JA-120PC</b>   | 1   | 2 335  | 2 335             |
| <b>Sběrníkový duální PIR a MW detektor pohybu JA-120PW</b> | 5   | 1 920  | 9 600             |
| <b>Sběrníkový detektor pohybu a rozbití skla JA-120PB</b>  | 2   | 1 250  | 2 500             |
| <b>Sběrníkový záplavový detektor JA-110F</b>               | 1   | 415    | 415               |
| <b>Bezpečnostní dveře Magnum</b>                           | 1   | 22 990 | 22 990            |
| <b>Bezpečnostní folie SCX</b>                              | 50  | 690    | 34 500            |
| <b>Stěnový trezor ST-132E/I</b>                            | 1   | 16 320 | 16 320            |
| <b>Sběrníkové tísňové tlačítko JA-112J</b>                 | 2   | 500    | 1 000             |
| <b>Ochranný kryt pro kameru, KAC-EYE</b>                   | 2   | 1 100  | 2 200             |
| <b>Celkem</b>  |     |        | <b>146 938 Kč</b> |

## 9 POROVNÁNÍ NAVRŽENÝCH SYSTÉMŮ ZABEZPEČENÍ

V diplomové práci jsou navrženy dva zabezpečovací systémy pro hlavní budovu firmy, která se specializuje ve strojírenském průmyslu, jak již bylo uvedeno v úvodu do praktické části. Z důvodu možnosti reálného využití nebo inspirace při následné realizaci systému zabezpečení první návrh zohlednil i potřeby dané firmy, vč. finančního hlediska. Druhý koncept byl založen na zkušenostech získaných při studiu oboru bezpečnostní technologie, systémy a management na Univerzitě Tomáše Bati ve Zlíně, fakulty aplikované informatiky.

Navržený zabezpečovací systém první verze obsahuje minimální množství prvků, které však poskytují požadovanou úroveň zabezpečení firmy. V první verzi jsou použity prvky poplachových zabezpečovacích a tísňových systémů, vč. kamerového systému. Při návrhu zabezpečení jsou prvky v co největší míře omezeny, tak aby byl splněn finanční požadavek na pořízení prvků, proto nejsou použity mechanické zábranné systémy.

Druhý návrh zabezpečení vychází z první verze a je rozšířen a doplněn o další prvky. Disponuje již mechanickými zábrannými prvky, vč. poplachových zabezpečovacích a tísňových systémů s kamerovým systémem. Celková finanční hodnota prvků v prvním návrhu je 44 773 Kč, zatímco u druhého je cena 146 938 Kč.

Ve druhé verzi zabezpečení je PZTS rozšířen o několik prvků, které nejsou obsaženy v prvním návrhu. Byly zejména vyměněny základní pohybové PIR detektory za duální, ať už kombinace detektorů PIR a MW, PIR s kamerou nebo kombinace PIR detektoru s detektorem tříštění skla. Duální detektory jsou odolnější vůči planým poplachům a poskytují větší spolehlivost, proto byly použity. V přízemí a prvním patře jsou umístěny tísňové tlačítka pro případ výskytu jakékoliv nebezpečné situace, které nejsou zmíněnými detektory vyhlášeny jako poplach. Oproti první verzi zabezpečení je druhá rozšířena o tři detektory kouře a teploty umístěné v kanceláři, šatně pro zaměstnance a v dílně. Větším počtem těchto detektorů je eliminována hrozba vzniku požáru po celé budově. Také je rozšířena o záplavový detektor, který jsem umístil do kuchyně pár cm nad podlahu, tak aby byl poplach včas vyvolán v případě zaplavení.

Kamerový systém byl rozšířen o jednu kameru, tak aby byl přístup k objektu monitorován od hlavní silnice a z opačné strany od budovy s výrobní halou. Obě kamery byly vybaveny krytem, který poskytuje větší odolnost vůči vnějším vlivům. U dražší verze jsou kamery v chodu v obou stavech, tj. zastřeženém i odstřeženém.

Mechanické zábranné prvky, které byly použity ve druhé verzi návrhu zabezpečení, se na rozdíl výsledných cen podílely nejvíc. Bezpečnostní dveře, kterými byly nahrazeny hlavní dveře, aby byl ztížen přístup pachatele do objektu. Použitím bezpečnostních folií na všech oknech se nejen zvýšila ochrana zaměstnanců před střepy rozbitím nebo vysypáním skla, ale převážně je pro pachatele zvýšena průniková odolnost do prostor budovy. Trezor jsem použil proto, aby bylo možné nejcennější dokumenty a finanční hotovost uschovat na bezpečném místě. Pro lepší přehlednost použitých prvků jsou obě verze porovnány v tabulce 21. Zabezpečovaný objekt nedisponoval jakýmkoliv zabezpečením, byl pouze ohraničen plotem. Při konzultacích s vedením firmy, které byly zmíněny v úvodu do praktické části, bylo zjištěno, že pořízení zabezpečovacího systému je důležitým požadavkem pro společnost.

Tabulka 21 Porovnání systémů

|  | Návrh systému – verze 1 |                          | Návrh systému – verze 2 |                            |
|--|-------------------------|--------------------------|-------------------------|----------------------------|
| <b>Poplachové zabezpečovací a tísňové systémy (PZTS)</b> | 7x                      | PIR detektor             | 1x                      | PIR detektor               |
|  | 18x                     | Magnetický detektor      | 18x                     | Magnetický detektor        |
|  | 3x                      | Detektor tříštění skla   | 4x                      | Detektor tříštění skla     |
|  | 1x                      | Detektor kouře a teploty | 4x                      | Detektor kouře a teploty   |
|  |                         |                          | 5x                      | PIR/MW detektor            |
|  |                         |                          | 2x                      | PIR/tříštění skla detektor |
|  |                         |                          | 1x                      | PIR/kamera detektor        |
|  |                         |                          | 1x                      | Záplavový detektor         |
|  |                         | 2x                       | Tísňové tlačítko        |                            |
| <b>Kamerové systémy (CCTV)</b>                           | 1x                      | Kamera bez krytu         | 2x                      | Kamera s krytem            |
| <b>Mechanické zábranné systémy (MZS)</b>                 | Nejsou použity          |                          | 1x                      | Bezpečnostní dveře         |
|  |                         |                          | 1x                      | Trezor                     |
|  |                         |                          | 50m                     | Bezpečnostní folie         |
| <b>Cena</b>  | <b>44 773 Kč</b>        |                          | <b>146 938 Kč</b>       |                            |

## ZÁVĚR

Cílem této diplomové práce byl návrh dvou verzí zabezpečovacích systémů pro strojírenskou společnost. První návrh se opíral o potřeby firmy a požadavek na protipatření hrozeb působící na společnost. Při druhém návrhu jsem vycházel z teoretických zkušeností získaných při studiu oboru bezpečnostní technologie, systémy a management na fakultě aplikované informatiky, Univerzity Tomáše Bati ve Zlíně.

V teoretické části jsou uvedeny mechanické zábranné systémy a to podle jednotlivých ochran, tj. obvodové, plášťové a předmětové. Na mechanické zábranné systémy navazovaly elektrické signalizační a monitorovací prvky, kde byly zmíněny poplachové zabezpečovací a tísňové systémy. Dále kamerové i přístupové systémy a elektrická požární signalizace. Nemalá část je také věnována zabezpečovacím systémům z pohledu na operační a technickou část. Poslední kapitola v této části práce je zaměřena na kvalitativní a kvantitativní bezpečnostní analýzu.

Praktická část práce se zabývá samotným návrhem zabezpečení firmy se strojírenským zaměřením. Jedná se tedy o objekt se specifickým provozem. Vzhledem k reálnému objektu a možnostem reálného využití byly potřebné konzultace s vedením firmy za účelem získání potřebných informací. Na základě konzultací a potřeb firmy na návrh zabezpečení první verze, vč. výsledků bezpečnostní analýzy, byl navržen zabezpečovací systém s minimem prvků, které však poskytují potřebnou ochranu zabezpečení. Po stanovení stupně zabezpečení a třídy prostředí, byly v odpovídajících programech zhotoveny půdorysy přízemí a prvního patra. Po výběru vhodných prvků zabezpečení dodávané výše zmíněnou firmou, byly následně ve zmíněných půdorysech rozmístěny. Přičemž zabezpečení přízemí je řešeno prostorově, ale i plášťově. První patro předchozí verze je zabezpečeno pouze z hlediska prostorové ochrany. Konfigurace systému, u které je stěžejní informací ovládání systému vedoucím výroby, nebo vedením firmy.

Při druhém návrhu zabezpečení jsem vycházel z předešlé, jednodušší první verze a z teoretických zkušeností získaných při studiu oboru bezpečnostní technologie, systémy a management na Univerzitě Tomáše Bati ve Zlíně, fakulty aplikované informatiky, jak již bylo zmíněno v úvodu do praktické části. Tato verze byla rozšířena o doplňující prvky zabezpečení, zejména se pak jednalo o mechanické zábranné prvky, tj. bezpečnostní dveře a bezpečnostní folie. Zabezpečení prvního patra u této verze je rozšířeno o plášťovou ochra-

nu. V neposlední řadě byl při tomto návrhu pořízen trezor na uschování dokumentů a finanční hotovosti.

Na závěr diplomové práce byly oba navržené systémy zhodnoceny a porovnány. Přičemž první verze návrhu byla vyčíslena na 44 773 Kč, kdežto druhá verze na 146 938 Kč. Hlavní důvod tak velkého rozdílu výsledné ceny byl odvozen z finančních potřeb a rozšíření druhé verze o mechanické zábranné prvky.

Osobně bych doporučil druhou verzi návrhu zabezpečovacího systému, tedy tu nákladnější variantu. Mohlo by se na první pohled zdát, že cena je příliš vysoká, ale při dlouhodobém pohledu na věc se tato investice určitě vyplatí. Na druhou stranu, pokud je firma ve svých začátcích a nedisponuje příliš velkým kapitálem, postačí i levnější verze návrhu.

**SEZNAM POUŽITÉ LITERATURY**

- [1] KINDL, Jiří. *Projektování bezpečnostních systémů*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007. ISBN 978-80-7318-554-1.
- [2] IVANKA, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.
- [3] UHLÁŘ, Jan. *Technická ochrana objektů II*. Praha: Vydavatelství PA ČR, 2005. ISBN 80-7251-189-0.
- [4] BRABEC, František. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. ISBN 80-86445-04-6.
- [5] BRABEC, František. *Ochrana bezpečnosti podniku*. Praha: Eurounion, 1996. ISBN 80-85858-29-0.
- [6] VALOUCH, Jan. *Projektování integrovaných systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-296-1. Dostupné také z: <http://hdl.handle.net/10563/25814>
- [7] BEBČÁK, Petr. *Požárně bezpečnostní zařízení*. 2. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2004. SPBI Spektrum. Červená řada. ISBN 80-86634-34-5. Dostupné také z: [http://toc.nkp.cz/NKC/200704/contents/nkc20071704904\\_1.pdf](http://toc.nkp.cz/NKC/200704/contents/nkc20071704904_1.pdf)
- [8] Alcam profi s.r.o. *Elektrická požární signalizace - EPS* [online]. 2011 [cit. 2016-05-09]. Dostupné z: <http://www.alcamprofi.cz/elektricka-pozarni-signalizace-eps-evakuacni-rozhlas-er.html>
- [9] KOLEKTIV, Luděk Lukáš. *Bezpečnostní technologie, systémy a management I*. Zlín: VeRBuM, 2011-. ISBN 978-80-87500-05-7.
- [10] KOLEKTIV, Luděk Lukáš. *Bezpečnostní technologie, systémy a management III*. 1. vyd. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.
- [11] KOLEKTIV, Luděk Lukáš. *Bezpečnostní technologie, systémy a management II*. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-808-7500-194.
- [12] IVANKA, Ján. *Systemizace bezpečnostního průmyslu*. Vyd. 5. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2014, 219 s. ISBN 978-80-7454-410-1. Dostupné také z: <http://hdl.handle.net/10563/27488>.

- [13] KRUEGLE, Herman. *CCTV surveillance: analog and digital video practices and technology*. Second edition. Amsterdam: Elsevier, BH, 2007. ISBN 978-0-7506-7768-4. Dostupné také z: <http://www.loc.gov/catdir/toc/ecip0517/2005022280.html>
- [14] LOVEČEK, Tomáš; NAGY, Peter. *Bezpečnostné systémy: kamerové bezpečnostné systémy*. Vyd. 1. Žilina: Žilinská univerzita, 2008, 283 s. ISBN 978-80-8070-893-1.
- [15] *Ústředny EZS* [online]. Praha, 2015 [cit. 2016-05-09]. Dostupné z: <http://www.micro.feld.cvut.cz/home/x34ezs/prednasky/04%20Ustredny%20EZS.pdf>
- [16] JAIN, Anil K., Arun A. ROSS a Karthik NANDAKUMAR. *Introduction to biometrics*. New York: Springer, c2011. ISBN 978-0-387-77326-1. Dostupné také z: <http://www.springerlink.com/content/978-0-387-77325-4/contents/>
- [17] Redox Technologies. *Smart Card Plug-In* [online]. 2004 [cit. 2016-05-09]. Dostupné z: [http://www.redoxtechnologies.com/Smart\\_Card\\_Plug\\_in.htm](http://www.redoxtechnologies.com/Smart_Card_Plug_in.htm)
- [18] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forezních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.
- [19] UHLÁŘ, Jan. *Technická ochrana objektů III*. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8.
- [20] VALOUCH, Jan. *Projektování bezpečnostních systémů*. Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2012, 152 s. ISBN 978-80-7454-230-5. Dostupné také z: <http://dspace.k.utb.cz/handle/10563/18663>
- [21] ŠEVČÍK, Jiří. *Bezpečnostní posouzení objektu* [online]. Zlín, 2010 [cit. 2016-05-09]. Dostupné z: <http://hdl.handle.net/10563/16101>. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.
- [22] *Seznam – Přehled metodik pro analýzu rizik* [Pomůcka, metodika]. Praha: Ministerstvo vnitra, Generální ředitelství HZS ČR, č.j.: PO-58-7/PLA-2004. Dostupné také z: [www.mvcr.cz](http://www.mvcr.cz)



- [23] ČANDÍK, Marek. *Objektová bezpečnost II*. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2004, 100 s. ISBN 8073182173.
- [24] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 80-902938-2-4.
- [25] Seznam.cz. *Mapy* [online]. 2016 [cit. 2016-05-09]. Dostupné z: <https://mapy.cz/zakladni?x=17.8104870&y=49.4775196&z=17&l=2&pano=1&pid=34751541&yaw=3.377&fov=1.571&pitch=0.157&source=firm&id=441990>
- [26] Jablotron Alarms. *Zabezpečovací systém Jablotron JA-100 sběrnice*. [online]. 2014 [cit. 2016-05-09]. Dostupné z: <http://www.jabloshop.cz/system-ja-100-sbernice>
- [27] Elnika plus. *NVR 104C ELM – IP DVR rekordér pro 4 IP kamery* [online]. 2016 [cit. 2016-05-09]. Dostupné z: <http://www.elnika.cz/elnika.php?detail=25303>
- [28] Alza.cz. *WD Purple 1TB 64 MB cache* [online]. 2016 [cit. 2016-05-09]. Dostupné z: <https://www.alza.cz/western-digital-purple-1000gb-64mb-cache-d602230.htm?catid=18849533>
- [29] Seznam.cz. *Mapy* [online]. 2016 [cit. 2016-05-09]. Dostupné z: <https://mapy.cz/zakladni?x=17.7530459&y=49.4681152&z=11&source=muni&id=530>
- [30] Seznam.cz. *Mapy* [online]. 2016 [cit. 2016-05-09]. Dostupné z: <https://mapy.cz/zakladni?planovani-tra-sy&x=17.8124797&y=49.4788473&z=16&rc=9o5PcxUZKt&rs=firm&rs=&ri=441990&ri=&mrp=%7B%22c%22%3A1%2C%22tt%22%3A1%7D&mrp=&rt=&rt=>
- [31] HT dveře. *Bezpečnostní dveře Magnum* [online]. 2009 [cit. 2016-05-09]. Dostupné z: <http://najisto.centrum.cz/3117438/ht-dvere-sro/produkty/287474/dvere-magnum/>

- [32] Trezory Key-mart. *Stěnový trezor ST-132E/1* [online]. c1990-2016 [cit. 2016-05-09]. Dostupné z: <http://www.trezory-keymart.cz/detail.php?produkt=Stenovyy-trezor-ST-132EI&id=889>
- [33] Jablotron Alarms. *Katalog produktů* [online]. 2016 [cit. 2016-05-09]. Dostupné z: <http://www.jablotron.com/cz/katalog-produktu/>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

|      |  |
|------|--|
| °C   | Základní jednotka teploty                |
| 2D   | Dvourozměrný prostor                     |
| 3D   | Trojrozměrný prostor                     |
| A/D  | Analogový / digitální převodník          |
| ACS  | Access, přístupový systém                |
| Ah   | Ampérhodina                              |
| CAD  | Computer Assisted Drafting               |
| CCD  | Charge-coupled Device                    |
| CCTV | Closed Circuit Television                |
| CID  | Contact ID                               |
| cm   | Centimetr                                |
| CMOS | Complementary Metal Oxide Semiconductor  |
| CNC  | Computer Numeric Control                 |
| ČR   | Česká republika                          |
| ČSN  | České technické normy                    |
| dB   | Decibel                                  |
| DNA  | Deoxyribonucleic Acid                    |
| DPH  | Daň z přidané hodnoty                    |
| DPPC | Dohledové poplachové a přijímací centrum |
| DPS  | Digital Pixel System                     |
| DXF  | Drawing Exchange Format                  |
| EPS  | Elektrická požární signalizace           |
| EZS  | Elektrická zabezpečovací signalizace     |
| EV   | Citlivost zaostřovacího systému          |

---

|       |  |
|-------|--|
| FTA   | Fault Tree Analysis                          |
| GHz   | Gigahertz                                    |
| GPRS  | General Packet Radio Service                 |
| GSM   | Global System for Mobile Communications      |
| HAZOP | Hazard and Operability Study                 |
| Hz    | Hertz  |
| HZS   | Hasičský záchranný sbor                      |
| I&HAS | Intruder and Hold-up Alarm System            |
| IR    | Infrared, infračervený                       |
| JPEG  | Joint Photographic Experts Group             |
| kg    | Kilogram                                     |
| kHz   | Kilohertz                                    |
| km    | Kilometr                                     |
| LED   | Light-Emitting Diode                         |
| m/s   | Metr za sekundu                              |
| m     | Metr   |
| mm    | Milimetr                                     |
| MHz   | Megahertz                                    |
| MZS   | Mechanický zabezpečovací systém              |
| NBÚ   | Národní bezpečnostní úřad                    |
| NVR   | Network Video Recorder                       |
| P2A   | Bezpečnostní atest, kategorie odolnosti skel |
| PCO   | Pult centralizované ochrany                  |
| PIR   | Pasiv Infra Red                              |
| PZS   | Poplachový zabezpečovací systém              |
| PZTS  | Poplachový zabezpečovací a tísňový systém    |

---

|        |  |
|--------|--|
| RF     | Radio Frequency  |
| RFID   | Radio Frequency Identification                                   |
| SIA    | Security Industry Association                                    |
| SKV    | System kontrolly vstupu  |
| SMS    | Short Message Service  |
| s.r.o. | Společnost s ručením omezeným                                    |
| SW     | Software   |
| SWOT   | Strenghts Weaknesses Opportunities Threats, bezpečnostní analýza |
| TB     | Terabyte   |
| USA    | United States of America   |
| UV     | Ultraviolet, ultrafialové  |
| V      | Volt   |
| WC     | Water closet, záchod   |
| WDR    | Wide Dynamic Rande   |

**SEZNAM OBRÁZKŮ**

|  |    |
|--|----|
| Obrázek 1 Grafické znázornění procesů bezpečnosti v MZS [2] .....        | 11 |
| Obrázek 2 Schéma PZTS [6] .....  | 16 |
| Obrázek 3 Uspořádání paprsků bariéry [12] .....                          | 20 |
| Obrázek 4 Ukázka ústředny smyčkové a s přímou adresací [15] .....        | 21 |
| Obrázek 5 Dělení samočinných požárních hlásičů [8] .....                 | 23 |
| Obrázek 6 Nesymetrický přenos bez korekčního zesilovače [12] .....       | 26 |
| Obrázek 7 Symetrický přenos [12] .....                                   | 26 |
| Obrázek 8 Princip snímání obrazu [13] .....                              | 28 |
| Obrázek 9 SmartCard [17] .....   | 32 |
| Obrázek 10 Princip biometrických systémů [18] .....                      | 34 |
| Obrázek 11 Schéma poskytování ochrany zabezpečovacích systémů [19] ..... | 36 |
| Obrázek 12 Metody pro analýzu rizik [21] .....                           | 41 |
| Obrázek 13 Rámec SWOT analýzy [21] .....                                 | 44 |
| Obrázek 14 Příklad použití SWOT analýzy .....                            | 45 |
| Obrázek 15 Územní plán města Kelč [29] .....                             | 49 |
| Obrázek 16 Objekt společnosti [30] .....                                 | 50 |
| Obrázek 17 Letecký pohled na objekt společnost [30] .....                | 50 |
| Obrázek 18 Pohled ze silnice na firmu a dům [25] .....                   | 51 |
| Obrázek 19 Pohled na budovu výrobní haly .....                           | 53 |
| Obrázek 20 Pohled na vrata hlavní budovy .....                           | 54 |
| Obrázek 21 Umístění obráběcích strojů .....                              | 56 |
| Obrázek 22 Pohled do kanceláře ze dveří .....                            | 62 |
| Obrázek 23 Půdorys přízemí hlavní budovy v 2D .....                      | 63 |
| Obrázek 24 Půdorys přízemí hlavní budovy v 3D .....                      | 64 |
| Obrázek 25 Půdorys hlavní budovy prvního patra v 2D .....                | 64 |
| Obrázek 26 Půdorys hlavní budovy prvního patra v 3D .....                | 64 |
| Obrázek 27 Ukázka v programu FloorPAD .....                              | 65 |
| Obrázek 28 Ukázka značek v ProfiCADu .....                               | 66 |
| Obrázek 29 Ústředna JA-101K [26] .....                                   | 67 |
| Obrázek 30 Modul telefonního komunikátoru JA-190X [26] .....             | 68 |
| Obrázek 31 Klávesnice a ovládací segment [26] .....                      | 68 |
| Obrázek 32 PIR detektor pohybu [26] .....                                | 69 |

|  |    |
|--|----|
| Obrázek 33 Detektor rozbití skla [26] .....              | 70 |
| Obrázek 34 Sběrníkový magnetický detektor [26] .....     | 70 |
| Obrázek 35 Detektor kouře a teploty [26] .....           | 71 |
| Obrázek 36 Venkovní siréna [26] .....                    | 71 |
| Obrázek 37 Kryt venkovní sirény [26] .....               | 72 |
| Obrázek 38 Přístupová karta RFID [26] .....              | 72 |
| Obrázek 39 Záložní akumulátor [26] .....                 | 72 |
| Obrázek 40 GSM kamera EYE-02 [26] .....                  | 73 |
| Obrázek 41 Rekordér [27] .....                           | 73 |
| Obrázek 42 Pevný disk WD Purple [28] .....               | 74 |
| Obrázek 43 Umístění prvků v přízemí – verze 1 .....      | 74 |
| Obrázek 44 Umístění prvků v prvním patře – verze 1 ..... | 75 |
| Obrázek 45 PIR detektor s kamerou [26] .....             | 81 |
| Obrázek 46 Duální detektor PIR/MW [26] .....             | 81 |
| Obrázek 47 Detektor pohybu a rozbití skla [26] .....     | 82 |
| Obrázek 48 Záplavový detektor [26] .....                 | 82 |
| Obrázek 49 Bezpečnostní dveře Magnum [31] .....          | 83 |
| Obrázek 50 Stěnový trezor [32] .....                     | 84 |
| Obrázek 51 Tísňové tlačítko [26] .....                   | 84 |
| Obrázek 52 Ochranný kryt pro kameru [26] .....           | 84 |
| Obrázek 53 Záložní akumulátor SA214-26 [26] .....        | 85 |
| Obrázek 54 Umístění prvků v přízemí – verze 2 .....      | 85 |
| Obrázek 55 Umístění prvků v prvním patře – verze 2 ..... | 86 |

**SEZNAM TABULEK**

|   |    |
|---|----|
| Tabulka 1 Stupně zabezpečení [20] .....               | 17 |
| Tabulka 2 Třídy prostředí [20].....                   | 17 |
| Tabulka 3 Jednotlivé prvky používané u PZTS [7] ..... | 18 |
| Tabulka 4 Třídy identifikace [1] .....                | 32 |
| Tabulka 5 Rozdělení biometrických znaků [16].....     | 34 |
| Tabulka 6 Budovy v areálu společnosti.....            | 51 |
| Tabulka 7 Bezpečnostní analýza.....                   | 57 |
| Tabulka 8 Detailnější rozbor hodnocení .....          | 58 |
| Tabulka 9 Hodnocení silných stránek.....              | 58 |
| Tabulka 10 Hodnocení slabých stránek .....            | 59 |
| Tabulka 11 Hodnocení příležitostí.....                | 59 |
| Tabulka 12 Hodnocení hrozeb .....                     | 59 |
| Tabulka 13 Protiopatření k hrozbám .....              | 60 |
| Tabulka 14 Rozdělení místností do tříd prostředí..... | 63 |
| Tabulka 15 Legenda použitých značek – verze 1 .....   | 75 |
| Tabulka 16 Rozdělení zón – verze 1 .....              | 77 |
| Tabulka 17 Cenová kalkulace – verze 1 .....           | 78 |
| Tabulka 18 Legenda použitých značek – verze 2 .....   | 86 |
| Tabulka 19 Rozdělení zón – verze 2.....               | 88 |
| Tabulka 20 Cenová kalkulace – verze 2 .....           | 89 |
| Tabulka 21 Porovnání systémů.....                     | 92 |


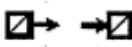























## SEZNAM PŘÍLOH

- PI Legenda schématických značek
- PII Certifikát o prohlášení o aplikovatelnosti
- PIII Certifikát pro vývoj, výrobu a prodej zdravotnických zařízení
- PIV Certifikát pro vývoj, výrobu a prodej elektronických poplachových systémů

## PŘÍLOHA PI: LEGENDA SCHÉMATICKÝCH ZNAČEK ČSN 50131

| Sch. značka<br>dle ČSN 50131 | Zjednodušená<br>sch. značka | Popis prvku                             | Sch. značka<br>dle ČSN 50131 | Zjednodušená<br>sch. značka        | Popis prvku                               |
|------------------------------|-----------------------------|---|------------------------------|------------------------------------|---|
|                              |                             | Magnetický detektor                     |                              |                                    | Kombinovaný detektor<br>PIR střípní a GBS |
|                              |                             | Magnetický detektor<br>- odolný         |                              |                                    | Kombinovaný detektor<br>PIR a GBS (JS-25) |
|                              |                             | Detektor tříštění<br>skla               |                              |                                    | Mikrovlnný<br>detektor                    |
|                              |                             | Detektor tříštění<br>skla - antimasking |                              |                                    | Duální detektor<br>mikrovlna, PIR         |
|                              |                             | Kontaktní detektor<br>plezo             |                              |                                    | Duální stropní detek.<br>mikrovlna, PIR   |
|                              |                             | PIR vějíř                               |                              |                                    | Ořesový detektor                          |
|                              |                             | PIR vějíř<br>venkovní                   |                              |                                    | Detektor<br>poslední bankovky             |
|                              |                             | PIR vějíř<br>antimasking                |                              |                                    | Tisňový hlásič PANIC<br>tlačítka          |
|                              |                             | PIR dlouhý<br>dosah                     |                              |                                    | Tisňový hlásič PANIC<br>lišta             |
|                              |                             | PIR s vlastní<br>adresou                |                              |                                    | Technologický<br>hlásič                   |
|                              |                             | PIR záclona                             |                              |                                    | Detektor<br>hořlavých plynů               |
|                              | PIR záclona<br>antimasking  |   |                              | Požární hlásič                     |   |
|                              | PIR záclona<br>dveří        |   |                              | Signalizace optická                |   |
|                              | Infrazávora                 |   |                              | Signalizace optická<br>a akustická |   |
|                              | Infrazávora<br>vysílač      |   |                              | Vnitřní siréna<br>s blikáčem       |   |
|                              | Infrazávora<br>přijímač     |   |                              | Vnitřní siréna                     |   |
|                              | Ultrazvukový detektor       |   |                              | Venkovní siréna<br>s blikáčem      |   |
|                              | PIR stropní                 |   |                              | Venkovní siréna                    |   |

| Sch. značka<br>dle ČSN 50131  | Zjednodušená<br>sch. značka   | Popis prvku                           | Sch. značka<br>dle ČSN 50131   | Zjednodušená<br>sch. značka   | Popis prvku                     |
|---|---|---------------------------------------|--|---|---------------------------------|
|  |   | Výstražné zařízení<br>maják           |  |   | Bezdrátový<br>vysílač, přijímač |
|  |    | Ústředna EZS                          |   |   | Klíčový<br>spínač               |
|  |   | Napájecí zdroj                        |   |   | Propouštěcí<br>zámek            |
|  |   | Expandér, link. modul<br>koncentrátor |   |   | Ovladač,<br>klávesnice          |
|  |   | Tablo EZS                             |   |   | Vstupně-výstupní<br>modul       |
|  |   | Přenosové zařízení<br>komunkátor      |   |   | Reléový modul                   |
|  |   | Transformátor<br>220/16 V             |  |    | Detektor kouře                  |
|  |   | Záložní<br>akumulátor                 |  |   | Vysílač GSM                     |
|   |  | Přijímač řady UC<br>(216, 220, ...)   |  |  | Vysílač PCO                     |
|   |  | Expandér<br>řady UC 280               |  |  | Záplavový detektor              |
|   |  | Detektor kouře                        |  |  | Vývod kabelu                    |

# PŘÍLOHA PII: CERTIFIKÁT O PROHLÁŠENÍ APLIKOVATELNOSTI

**CQS - Sdružení pro certifikaci systémů jakosti**  
**Pod Lisem 129, 171 02 Praha 8 - Troja**  
**Česká republika**

CQS je certifikačním orgánem, akreditovaným podle normy ČSN EN ISO/IEC 17021:2011 Českým institutem pro akreditaci, o.p.s. pod registračním číslem 3029 pro certifikaci systémů managementu bezpečnosti informací



## CERTIFIKÁT

číslo: CQS 26/2015

CQS - Sdružení pro certifikaci systémů jakosti na základě kladného výsledku certifikačního auditu prohlašuje, že

**system managementu bezpečnosti informací v organizaci**

**JABLOTRON ALARMS a.s.**  
**Pod Skalkou 4567/33, 466 01 Jablonec nad Nisou, Česká republika**

byl prověřen a shledán v souladu s požadavky

**ČSN ISO/IEC 27001 : 2014**

Tento certifikát platí pro celou společnost v souladu s „Prohlášením o aplikovatelnosti“ z 27.01.2015 pro obor (služby):

- **CLOUD JABLOTRON - vývoj a provoz**

\*\*\*\*\*

Platnost certifikátu omezena do: 19. 02. 2018  
Rozhodnutí o certifikaci: 19. 02. 2015  
Datum vydání: 19. 02. 2015

  
Ing. Jana Olšanská  
Vedoucí certifikačního orgánu



# PŘÍLOHA PIII: CERTIFIKÁT PRO VÝVOJ, VÝROBU A PRODEJ ZDRAVOTNICKÝCH ZAŘÍZENÍ

**CQS - Sdružení pro certifikaci systémů jakosti**  
**Pod Lisem 129, 171 02 Praha 8 - Troja**  
**Česká republika**

CQS je certifikačním orgánem, akreditovaným podle normy ČSN EN ISO/IEC 17021:2011 Českým institutem pro akreditaci, o.p.s. pod registračním číslem 3029 pro certifikaci systémů managementu kvality



## CERTIFIKÁT

číslo: CQS 173/2014

CQS - Sdružení pro certifikaci systémů jakosti na základě kladného výsledku certifikačního auditu prohlašuje, že systém managementu kvality

**JABLOTRON ALARMS a.s.**  
**Pod Skalkou 4567/33, 466 01 Jablonec nad Nisou, Česká republika**  
**a sklad: Průmyslová zóna Liberec Sever, Hala H3, Svárovská 699, 463 03 Stráž nad Nisou**

byl prověřen a sledán v souladu s požadavky

**ČSN EN ISO 13485 : 2012**

Tento certifikát platí pro následující procesy; technické oblasti jsou uvedeny ve zprávě z auditu ze dne 15.12.2014

- **Vývoj, výroba a prodej aktivních neimplantabilních zdravotnických prostředků**

\*\*\*\*\*

Platnost certifikátu omezena do: 15. 12. 2017  
Rozhodnutí o certifikaci: 15. 12. 2014  
Datum vydání: 15. 12. 2014  
Datum udělení prvního certifikátu: 18. 12. 2002

  
**Ing. Jana Olšanská**  
Vedoucí certifikačního orgánu



# PŘÍLOHA PIV: CERTIFIKÁT PRO VÝVOJ, VÝROBU A PRODEJ ELEKTRONICKÝCH POPLACHOVÝCH SYSTÉMŮ

**CQS - Sdružení pro certifikaci systémů jakosti**  
**Pod Lisem 129, 171 02 Praha 8 - Troja**  
**Česká republika**

CQS je certifikačním orgánem, akreditovaným podle normy ČSN EN ISO/IEC 17021:2011 Českým institutem pro akreditaci, o.p.s. pod registračním číslem 3029 pro certifikaci systémů managementu kvality



## CERTIFIKÁT

číslo: CQS 2204/2014

CQS - Sdružení pro certifikaci systémů jakosti  
na základě kladného výsledku certifikačního auditu  
prohlašuje, že systém managementu kvality

**JABLOTRON ALARMS a.s.**  
**Pod Skalkou 4567/33, 466 01 Jablonec nad Nisou, Česká republika**  
**a sklad: Průmyslová zóna Liberec Sever, Hala H3, Svárovská 699, 463 03 Stráž nad Nisou**

byl prověřen a shledán v souladu s požadavky

**ČSN EN ISO 9001 : 2009**

Tento certifikát platí pro procesy:

- **Vývoj, výroba a prodej elektronických poplachových systémů**

\*\*\*\*\*

Platnost certifikátu omezena do: 15. 12. 2017

Rozhodnutí o certifikaci: 15. 12. 2014

Datum vydání: 15. 12. 2014

Datum udělení prvního certifikátu: 25. 05. 1999

A handwritten signature in blue ink, appearing to read 'Jana Olšanská', written over a dotted line.

**Ing. Jana Olšanská**

**Vedoucí certifikačního orgánu**

