

# Návrh na zabezpečení multifunkčního domu

The Security Proposal for a Multifunctional Building

Bc. Libor Kostka

---

Diplomová práce  
2011



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2010/2011

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Libor KOSTKA**  
Osobní číslo: **A09376**  
Studijní program: **N 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Návrh na zabezpečení multifunkčního domu**

Zásady pro vypracování:

1. Zpracujte bezpečnostní analýzu objektu.
2. Stanovte legislativní rámec na vybrané bezpečnostní systémy.
3. Vyberte a charakterizujte jednotlivé komponenty zabezpečení.
4. Zpracujte konkrétní návrh zabezpečení včetně grafické dokumentace.
5. Sestavte rozpočet celkového zabezpečení.

Seznam odborné literatury:

1. KŘEČEK, Stanislav. Příručka zabezpečovací techniky. 3. Blatná : Blatenská tiskárna, 2006. 313 s. ISBN 80-902938-2-4.
2. TKOTZ, Klaus, et al. Příručka pro elektrotechnika. 2. Praha : Europa-Sobotáles, 2006. 624 s. ISBN 80-86706-13-3, DT 621.3/075.3.
3. KREJČÍŘÍK, Alexandr. SMS-Střežení a ovládání objektů pomocí mobilu a sms. Praha : BEN-technická literatura, 2004. 304 s. ISBN 80-7300-02-2.
4. Česko. Zákon ze dne 24.ledna 1997 o technických požadavcích na výrobky a o změně a doplnění některých zákonů. In Sběrka zákonů, Česká republika. 1. částka 6, č. 22, s. 128-136. Dostupný také z WWW: . ISSN 1211-1244.
5. UHLÁŘ, Jan . Technická ochrana objektů. II.díl : Elektrické zabezpečovací systémy. 1. Praha : Policejní akademie české republiky, 2005. 229 s. ISBN 80-7251-1-1.
6. IVANKA, Ján . Systemizace bezpečnostního průmyslu II . 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 86 s. ISBN 978-80-7318-863-4.

Vedoucí diplomové práce:

Ing. Petr Neumann, Ph.D.

Ústav elektroniky a měření

Datum zadání diplomové práce:

25. února 2011

Termín odevzdání diplomové práce:

27. května 2011

Ve Zlíně dne 25. února 2011

  
prof. Ing. Vladimír Vašek, CSc.  
děkan

L.S.

  
doc. RNDr. Vojtěch Křesálek  
ředitel ústavu

## **ABSTRAKT**

Cílem této diplomové práce je navrhnout zabezpečení multifunkčního domu především proti neoprávněnému vniknutí, ale také proti jiným hrozbám. Práce je rozdělena do dvou částí na část teoretickou a praktickou. V teoretické části jsou popsány vybrané bezpečnostní systémy, včetně požadavků, které se na ně vztahují a také obecný postup návrhu těchto systémů. V praktické části je proveden návrh zabezpečení objektu včetně bezpečnostního posouzení, popisu jednotlivých komponentů a celkové ceny zabezpečení, doplněné o grafickou dokumentaci.

Klíčová slova: poplachové zabezpečovací systémy, mechanické zábranné systémy, bezpečnostní analýza, bezpečnostní posouzení.

## **ABSTRACT**

The goal of this thesis is to propose a multi-house security particularly against unauthorized intrusion, but also against other threats. The work is divided into two parts: a theoretical and practical. The theoretical part describes selected safety systems, including requirements that apply to them and the general process design of these systems. In practical part is implemented security proposal facility including security assessment, a description of the individual components and total price security, complemented by video documentation.

Keywords: security alarm systems, mechanical security systems, security analysis, security assessment.

Tímto bych chtěl poděkovat panu Ing. Petru Neumannovi, Ph.D. především za vstřícnost a trpělivost, kterou mi věnoval a za odborné vedení při psaní mé diplomové práce. Také děkuji za rady a poskytnutí materiálů lidem zastupující firmy, jejichž výrobky v mé práci uvádím a charakterizuji.

**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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- 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 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

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD .....</b>	<b>11</b>
<b>I TEORETICKÁ ČÁST .....</b>	<b>13</b>
<b>1 OCHRANA OBJEKTU .....</b>	<b>14</b>
1.1 PROSTOROVÉ ČLENĚNÍ TECHNICKÉ OCHRANY .....	15
1.2 ZPŮSOBY VLOUPÁNÍ DO BYTŮ A RODINNÝCH DOMŮ .....	17
<b>2 MECHANICKÉ ZÁBRANNÉ SYSTÉMY .....</b>	<b>19</b>
2.1 STUPEŇ RIZIKA OHROŽENÝCH OBJEKTŮ .....	20
2.2 ROZDĚLENÍ MECHANICKÝCH ZÁBRANNÝCH SYSTÉMŮ .....	20
2.3 POŽADAVKY NA MECHANICKÉ ZÁBRANNÉ SYSTÉMY .....	21
2.3.1 Pyramida bezpečnosti .....	22
2.4 NÁVRH MZS .....	23
<b>3 POPLACHOVÉ ZABEZPEČOVACÍ SYSTÉMY .....</b>	<b>24</b>
3.1 ZMĚNA NORMY 50131-1 ED.2 PROTI PŘEDCHOZÍM NORMÁM .....	24
3.2 POPIS A ÚČEL POPLACHOVÉHO ZABEZPEČOVACÍHO SYSTÉMU .....	25
3.2.1 Ústředny PZS .....	26
3.2.1.1 Analogové ústředny .....	26
3.2.1.2 Sběrníkové ústředny (ústředny s přímou adresací čidel) .....	26
3.2.1.3 Koncentrátorové ústředny .....	27
3.2.1.4 Ústředny s bezdrátovým přenosem .....	27
3.2.2 Detektory PZS .....	27
3.2.2.1 Rozdělení detektorů PZS .....	27
3.2.3 Detektory prostředí .....	28
3.2.4 Signalizační zařízení .....	29
3.2.5 Poplachová přenosová systémy .....	30
3.2.6 Ovládací zařízení .....	31
3.2.7 Napájecí zdroje .....	31
3.2.8 Kabeláž .....	32
3.3 VYBRANÉ SYSTÉMOVÉ POŽADAVKY NA PZS DLE NORMY ČSN EN 50131-1 ED.2 .....	33
3.3.1 Stupně zabezpečení .....	33
3.3.2 Třídy prostředí .....	33
3.3.3 Přístupové úrovně .....	34
3.3.4 Ochrana proti sabotáži .....	35
3.3.5 Požadavky na napájení .....	36
3.3.6 Zřizování PZS .....	37
3.4 NÁVRH PZS .....	38
3.4.1 Bezpečnostní analýza .....	39
3.4.1.1 Bezpečnostní analýza jako součást bezpečnostní politiky .....	40
3.4.1.2 Analýza rizik .....	41
3.4.2 Bezpečnostní posouzení .....	42
3.4.3 Volba a umístění komponentů systému .....	47
3.4.4 Požadavky na konfiguraci systému .....	49
<b>4 POJIŠTĚNÍ .....</b>	<b>50</b>

4.1	POŽADAVKY POJIŠŤOVEN.....	51
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>52</b>
<b>5</b>	<b>LEGISLATIVNÍ RÁMEC PRO VYBRANÉ BEZPEČNOSTNÍ SYSTÉMY .....</b>	<b>53</b>
5.1	LEGISLATIVNÍ RÁMEC NA PZS .....	53
5.2	NORMY PRO MZS.....	56
<b>6</b>	<b>BEZPEČNOSTNÍ ANALÝZA.....</b>	<b>57</b>
6.1	POPIS OBJEKTU A JEHO OKOLÍ .....	57
6.2	BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU .....	58
II.	Prověrka lokality – Struktura objektu.....	59
III.	Prověrka lokality – Ostatní vlivy.....	61
IV.	Stanovení pojistných tříd .....	62
V.	Stanovení stupně zabezpečení.....	62
VI.	Klasifikace prostředí.....	62
VII.	Stanovení typu ochrany .....	62
VIII.	Způsoby předání poplachové informace.....	62
IX.	Speciální požadavky .....	62
X.	Zvláštní opatření.....	62
XI.	Požadavky majitele objektu .....	63
6.3	SLABÁ MÍSTA OBJEKTU .....	63
6.4	HROZBY VYPLÍVAJÍCÍ Z BEZPEČNOSTNÍHO POSOUZENÍ .....	64
6.5	ANALÝZA KRIMINALITY .....	64
<b>7</b>	<b>VÝBĚR A POPIS KOMPONENTŮ PZS.....</b>	<b>66</b>
7.1	ÚSTŘEDNA DIGIPLEX EVO48 .....	66
7.1.1	Základní vlastnosti ústředny .....	66
7.1.2	Technické parametry ústředny .....	67
7.1.3	Příslušenství k ústředně .....	67
7.1.4	Zapojení ústředny .....	68
7.2	EXPANDÉR ARP-ZX8 .....	68
7.2.1	Vlastnosti modulu.....	68
7.2.2	Technické parametry modulu.....	69
7.2.3	Zapojení modulu.....	69
7.3	BEZDRÁTOVÝ MODUL MG-RTX3 .....	70
7.3.1	Vlastnosti modulu.....	70
7.3.2	Technické parametry modulu.....	71
7.3.3	Instalace .....	71
7.4	KOMUNIKAČNÍ MODUL PCS200.....	71
7.4.1	Vlastnosti modulu.....	72
7.4.2	Technické parametry modulu.....	72
7.4.3	Zapojení modulu.....	73
7.5	VENKOVNÍ SIRÉNA TEKNIM-720WR .....	74
7.5.1	Technické parametry sirény .....	74
7.6	VNITŘNÍ SIRÉNA SA-913 .....	74
7.6.1	Technické parametry sirény .....	75



7.7	LCD KLÁVESNICE K641 .....	75
7.7.1	Vlastnosti klávesnice .....	76
7.7.2	Technické parametry .....	76
7.8	LED KLÁVESNICE K648 .....	76
7.8.1	Vlastnosti klávesnice .....	77
7.8.2	Technické parametry .....	77
7.9	PARADOX PRO 476.....	78
7.9.1	Vlastnosti detektoru.....	78
7.9.2	Technické parametry detektoru.....	78
7.9.3	Detekční charakteristika detektoru .....	79
7.9.4	Instalace .....	80
7.10	DETEKTOR TRÍŠTĚNÍ SKLA GLASSTREK 457.....	80
7.10.1	Vlastnosti detektoru.....	80
7.10.2	Technické parametry detektoru.....	81
7.10.3	Detekční úhly detektoru.....	81
7.10.4	Instalace .....	81
7.11	DETEKTOR TRÍŠTĚNÍ SKLA FLEX GARD FG1625TAS.....	82
7.11.1	Vlastnosti detektoru.....	82
7.11.2	Technické parametry detektoru.....	83
7.11.3	Instalace .....	83
7.12	MAGNETICKÝ ZÁPUSTNÝ KONTAKT MAS 333 .....	84
7.12.1	Technické parametry .....	84
7.12.2	Pracovní diagram.....	85
7.12.3	Instalace .....	85
7.13	OPTICKO-KOUŘOVÝ POŽÁRNÍ DETEKTOR VAR-TEC FDR-26-S.....	86
7.13.1	Technické parametry .....	86
7.13.2	Instalace .....	87
7.14	DETEKTOR ÚNIKU PLYNU SD- ECG 983 N .....	87
7.14.1	Technické parametry .....	88
7.14.2	Instalace .....	88
7.15	DETEKTOR ZAPLAVENÍ A VLHKOSTI MENVIER 1450.....	89
7.15.1	Vlastnost detektoru.....	89
7.15.2	Technické parametry .....	89
7.15.3	Instalace .....	90
<b>8</b>	<b>VÝBĚR A POPIS KOMPONENTŮ MECHANICKÝCH ZÁBRANNÝCH PROSTŘEDKŮ.....</b>	<b>91</b>
8.1	BEZPEČNOSTNÍ DVEŘE – NEXT SD 101 .....	91
8.1.1	Vlastnosti dveří.....	91
8.1.2	Popis prvků dveří.....	91
8.1.3	Příslušenství k uvedeným dveřím.....	92
8.2	BEZPEČNOSTNÍ MŘÍŽE NEXT TYP B.....	93
<b>9</b>	<b>POPIS A KONFIGURACE PZS .....</b>	<b>94</b>
9.1	POPIS A KONFIGURACE SYSTÉMU.....	94
9.1.1	Popis a konfigurace podsystému 1 .....	95
9.1.2	Konfigurace podsystému 2.....	96

---

9.1.3	Konfigurace podsystemu 3.....	96
9.1.4	Další bezpečnostní a režimová opatření v objektu.....	97
9.2	DOKUMENTACE PZS – NÁVRH ROZMÍSTĚNÍ KOMPONENTŮ.....	97
<b>10</b>	<b>ROZPOČET ZABEZPEČENÍ.....</b>	<b>102</b>
	<b>ZÁVĚR.....</b>	<b>104</b>
	<b>CONSLUSION.....</b>	<b>105</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>106</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>110</b>
	<b>SEZNAM OBRÁZKŮ.....</b>	<b>111</b>
	<b>SEZNAM TABULEK.....</b>	<b>113</b>

## ÚVOD

Na úvod mé diplomové práce bych napsal několik slov, ve kterých bych zdůvodnil výběr tématu a také to, na co se má práce zaměřit.

Jakož to student v oboru zabezpečovacích technologií jsem rád, že své studium mohu završit prací, ve které budu navrhovat zabezpečení multiplexního domu, patřící mému otci, ve kterém se nacházejí dvě prodejny a obytná část. Pokusím se v co největší míře uplatnit své poznatky za své pěti – roční studium a to ze všech předmětů, které se zabývaly bezpečnostními systémy a jejich prvky. Na práci bude ovšem pravděpodobně znát absence praxe v tomto oboru, což doufám v následujících letech brzy napravím. Obor věnující se zabezpečovacím technologiím je velmi rozmanitý a vysoce se rozvíjející. S rozvojem vědy a techniky, poznatků z oblasti managementu a řízení a v neposlední řadě profesionalizací hlídacích služeb se rozšiřuje škála možností pro ochranu objektu. Majitel objektu má čím dál více možností, jak si svůj majetek může chránit. Umožňuje mu to nejenom rostoucí počet bezpečnostních agentur, které nabízejí komplexní ochranu objektu, ale i elektroinstalační firmy, které nejsou bezpečnostními agenturami v pravém slova smyslu, ale které kvůli zvyšujícímu se zájmu o ochranu majetku nabízejí vedle svých tradičních produktů také zabezpečovací systémy. Dále si zejména v poslední době můžeme všimnout pronikání nabídky zabezpečovacích systémů do různých hypermarketů a obchodních center, kde jsou prodávány jako běžné zboží. Takovéto systémy jsou mnohem levnější a jsou nabízeny tak, aby si je mohl uživatel nainstalovat sám, aniž by se on sám vyznal v zabezpečovacích technologiích. Tyto produkty ovšem nespĺňují všechny potřebné normy a certifikáty, které kvalitní bezpečnostní systémy musejí mít, ať už kvůli požadavkům pojišťoven či ochraně utajovaných informací. Kvalita těchto produktů či systémů je diskutabilní a zatím nemůže konkurovat kvalitním bezpečnostním systémům. Proto se tato práce nebude těmto systémům věnovat, ale bude zaměřena na systémy, které jsou kvalitní a splňují jak normy, tak požadavky pojišťoven. Teoretická část práce začne popisem ochrany objektu, následně se přejde k obecnému popisu vybraných bezpečnostních systémů a k tomu, jak by se v případě jejich návrhu mělo postupovat. Také budou uvedeny vybrané požadavky na tyto systémy, které vycházejí z patřičných norem včetně požadavků pojišťoven, protože pojištění je důležitou součástí ochrany majetku.

V praktické části bude zpracována legislativa, která se na vybrané bezpečnostní systémy vztahuje a dále bude následovat hlavní cíl práce, tedy návrhu systému, který bude vycházet

z bezpečnostní analýzy, příp. bezpečnostního posouzení, které stanovuje norma. Na základě provedení bezpečnostní analýzy, příp. bezpečnostního posouzení, bude zhotoven návrh zabezpečení objektu, ve kterém bude cílem to, aby obsahoval informace, které jsou uvedeny v související normě, která přesně popisuje údaje, které by měl návrh obsahovat. Součástí bude také dokumentace, kde bude vidět, jak je zabezpečení navrženo. Na závěr bude stanoven rozpis a cena materiálu.

## **I. TEORETICKÁ ČÁST**

## 1 OCHRANA OBJEKTU

Každý z nás se jistě rádi cítíme ve svém domě bezpečně a také když jsme mimo něj, chceme mít na vědomí, že náš dům s majetkem je chráněn a zabezpečen. Nejedná se jenom o zabezpečení proti vloupání, ale také zabezpečení proti požáru, úniku plynu, úniku vody a jiným nebezpečím, které závisí na dané lokalitě, daném objektu a technologiím a majetku, nacházejících se uvnitř objektu. Při návrhu konkrétní ochrany musíme znát předmět ochrany (co chránit) a cíl ochrany (proti čemu chránit). K tomu slouží bezpečnostní analýza nebo také bezpečnostní posouzení, které by měly dát na tyto otázky odpovědi. Samozřejmostí je dobře se vyznat v aktuální nabídce produktů k ochraně objektu a znát její základní rozdělení, které je následující:

- **Klasická ochrana** – základní forma ochrany objektu, se kterou je možné se prakticky setkat na každém objektu. Jedná se především o mechanické zábrany a zařízení, které znemožňují vstup do objektu, odcizení a poškození majetku uvnitř budovy a znesnadňují přístup na soukromý pozemek. [1]
- **Režimová ochrana** – představuje organizačně administrativní opatření, směřující k zajištění požadovaných podmínek pro smysluplnou funkci bezpečnostního systému a jeho sladění s provozem chráněného objektu. Zahrnují klíčový režim, režim vstupu a výstupu osob, vjezdu a výjezdu vozidel, režim pohybu osob a chráněných informací v objektu, režim manipulace s klíči, médii a ostatními identifikačními prostředky, které se používají pro systémy zabezpečení vstupů a výstupů. Režimová opatření bývají zpravidla popsána v provozním řádu objektu a obsahují i seznamy osob, které jsou oprávněny vstupovat do objektu či jeho částí nebo seznamy osob, které mají oprávnění nakládat s utajovanými informacemi. Z prostorového členění je rozdělujeme na vnější a vnitřní režimová opatření. [1]
- **Fyzická ochrana** – jedná se o ochranu prováděnou živou silou, zařazujeme zde hlídací službu, vrátné, zásahovou jednotku PCO, policii apod. Pokud je aplikována při ochraně objektu, závisí na její úrovni výsledná činnost ostatních druhů ochrany. Je ovšem ze všech typů ochrany nejdražší, protože u ní musíme počítat s vysokými náklady na režii (zejména na platy) i když pořizovací náklady jsou nízké. Pracovníci, působící na úrovni této ochrany musí splňovat určité kvalifikační předpoklady zaměřené na psychickou a fyzickou stránku, znalost vybraných právních předpisů a měli by pravidelně procházet školením. [1]

- **Technická ochrana** – do této ochrany spadají mechanické a elektronické systémy, které zabraňují, ztěžují, monitorují nebo detekují narušení bezpečnosti objektu. Patří sem mechanické zábranné systémy, poplachová zabezpečovací systémy, přístupové systémy, kamerové systémy, tísňové systémy a další systémy. [1]

Při výběru a návrhu zabezpečení platí tři následující pravidla:

- Každá ochrana může být překonána.
- Nejefektivnější je kombinace více typů ochran, jedna skupina nic neřeší.
- Technické prostředky nenahradí člověka – např. vyhodnocení falešného poplachu.

Výběr typů ochrany objektu se odvíjí také od jeho velikosti. U malého rodinného domku bude postačující kombinace technické ochrany – PZS a klasické ochrany. U velkého objektu jako je obchodní centrum by takováto kombinace byla nedostačující a to i kdyby PZS obsahoval mnohokrát více prvků PZS. Při takovémto zabezpečení je běžná kombinace systémů PZS, EPS, CCTV, MZS, ACS doplněných o hlídací služby a samozřejmostí jsou režimová opatření. Objekt, kterému je navrhováno zabezpečení, se řadí do středně velkých objektů, u kterých se ochrana provádí pomocí klasické a technické ochrany. Z technické ochrany to jsou především mechanické zábranné systémy a poplachové zabezpečovací systémy. A právě z důvodu, že návrh zabezpečení bude založen na technické ochraně a z ní vybraných bezpečnostních systémů, budu se práce v teoretické části dále těmito systémům věnovat.

## 1.1 Prostorové členění technické ochrany

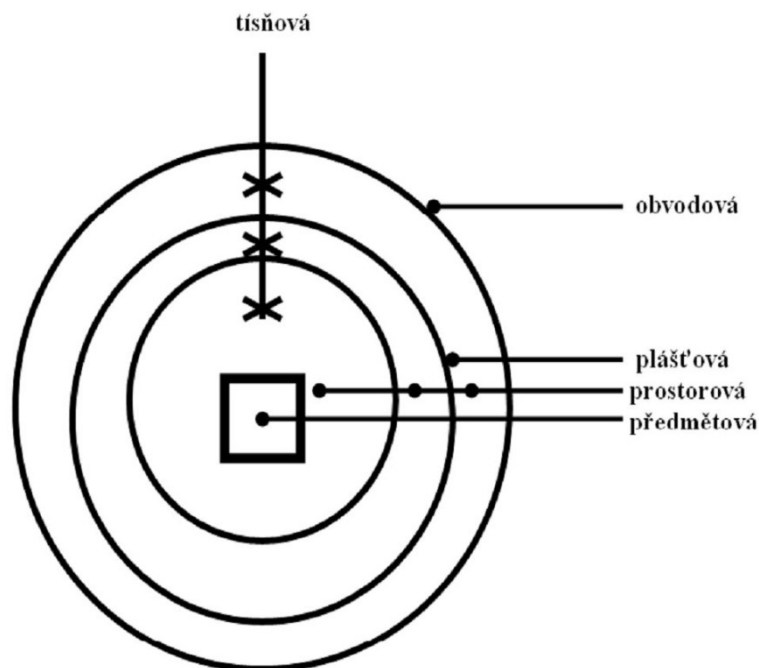
Technická ochrana se rozděluje do pěti základních okruhů ochranných zón:

- **Obvodová ochrana** – je označována také jako perimetrická či venkovní. Zajišťuje bezpečnost vyhrazenému území nebo detekuje narušení obvodu objektu. Obvodem objektu je myšlena jeho katastrální hranice, realizována nejčastěji přírodními nebo umělými bariérami (ploty, zdi, vodní toky apod.). Při použití prvků PZS je kladen důraz na odolnost těchto prvků proti falešným poplachům. [2]
- **Plášťová ochrana** – zabraňuje nebo signalizuje narušení pláště objektu. Může přitom jít o celou budovu nebo o vyčleněný komplex místností či prostor. Jedná se především o zabezpečení vstupu do všech stavebních otvorů v objektu, jako jsou dveře, okna, vikýře, šachty apod. Nejčastěji se jedná o kombinaci detektorů tříštění

skla a magnetických kontaktů, která může být doplněna o prvky MZS. U objektů s požadavkem na vyšší stupeň zabezpečení se na této úrovni ochrany používají i otřesové detektory, které mohou detekovat případné otřesy stěn či bezpečnostních dveří. Plášťová ochrana se obvykle realizuje zevnitř objektu a bývá také označována jako objektová ochrana. [2]

- **Prostorová ochrana** – jejím účelem je signalizovat změny v chráněném prostoru s tím, že by mělo jít o klíčová místa v objektu, jako jsou místa předpokládaného pohybu pachatele – chodby, schodiště apod. Na tomto okruhu ochranné zóny již pachatel překonal plášť objektu a vnikl do jeho vnitřních prostor, přičemž tato ochrana reaguje až na pohyb v tomto prostoru. Nejpoužívanějšími prvky této ochrany jsou jednoznačně pasivní infračervené detektory pohybu, ale také je obvyklá kombinace PIR detektorů s jiným typem detektoru, označovaných jako duální detektory. Tato ochrana bývá také označována jako pohybová ochrana. [2]
- **Předmětová ochrana** – zabraňuje nebo signalizuje napadení nebo neoprávněnou manipulaci s chráněnými předměty. Jedná se především o různá úschovná místa, jako jsou trezory apod. a detektory založené na principu zachycení změn při manipulaci s chráněným předmětem. Poplach je následně vyhlášen na základě bezprostřední přítomnosti pachatele u chráněného předmětu nebo manipulace s ním. Nejedná se pouze o předměty uvnitř objektu, ale také o předměty, jako jsou osobní automobily či zemědělské stroje. [2]
- **Tísňová ochrana** – účelem této ochrany je signalizovat ohrožení života napadením, zdravotní problémy či působení živlů uvnitř objektu (voda, plyn, požár aj.). Jedná se především o skryté, veřejné nebo osobní tísňové hlásiče. [2]

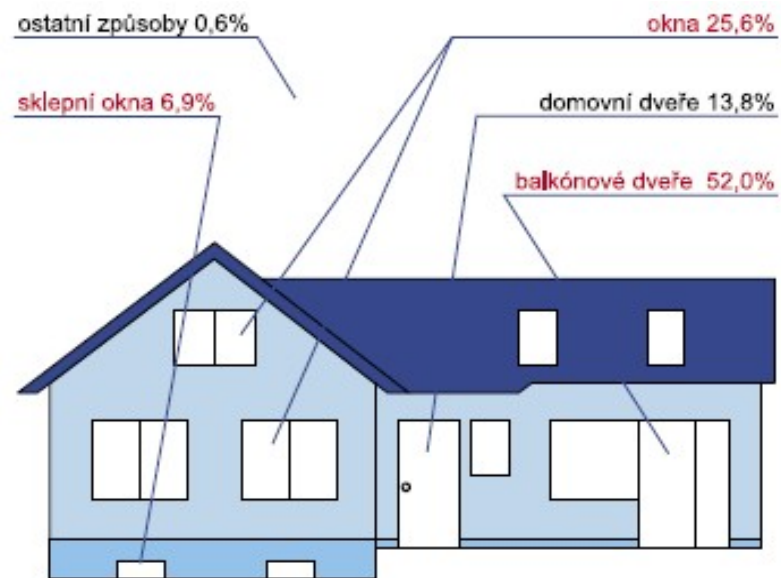




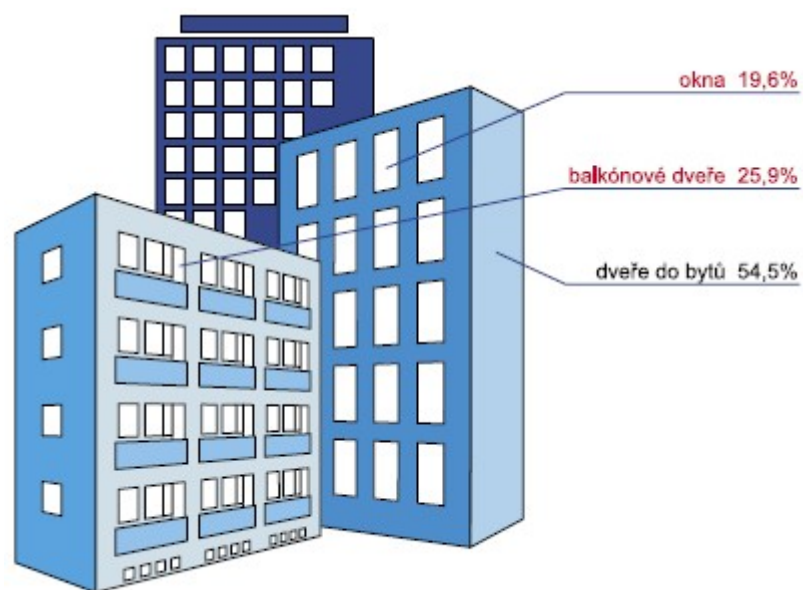
Obr. 1. Prostorové členění technické ochrany [2]

## 1.2 Způsoby vloupání do bytů a rodinných domů

Z policejních statistik vyplývá, že pachatelé krádeží vloupáním nejčastěji volí cestu do bytů v rodinných domech přes okna a balkónové dveře (takřka 80 % všech případů). Poněkud jiná je situace u bytů v bytových domech, kde volí zloději mnohdy přístupnější bytové dveře, ale i přesto jsou jejich cílem okna a balkónové dveře ve více jak 45 % případů. Statistika dále říká, že v drtivé většině vloupání oknem či balkónovými dveřmi (necelých 70 %) byl vypáčen rám nebo kování. Naopak přibližně 45 % pokusů o vloupání selhalo na vhodné technice zabezpečení (především mechanických zábranných systémů). Z těchto důvodů je patrné odolnost stavebních výplní proti vloupání posílit.



Obr. 2. Způsoby vloupání do rodinných domů [3]



Obr. 3. Způsoby vloupání do bytů v bytových domech [3]

## 2 MECHANICKÉ ZÁBRANNÉ SYSTÉMY

Mechanické zábranné systémy jsou považovány za základní prvek ochrany objektu. Mezi MZS řádíme veškeré mechanické prvky, které zamezují nebo ztěžují proniknutí nepovolaných osob do chráněného objektu přes obvodovou a plášťovou ochranu, a to zejména přes oplocení a dveřní nebo okenní otvory. Řádíme zde také veškeré uzamykatelné systémy, které slouží k ochraně předmětů před odcizením či jiným nebezpečím. Je potřebné mít vždy na vědomí, že každý mechanický zábranný systém je překonatelný v určitém čase, a proto je úkolem MZS zajistit, aby tento časový interval byl co největší. Doba, kterou pak musí pachatel vynaložit na její překonání, je v mnohých případech delší, než je pro pachatele únosné. Hodnota času potřebná pro překonání MZS záleží na následujících faktorech:

- na kvalitě MZS,
- na znalosti pachatele konstrukce daného MZS,
- na umístění MZS,
- na typu a kvalitě používaných nástrojů pro překonání MZS,
- na možnostech využití energetických zdrojů (zásuvka apod.). [4]

Tento časový interval, potřebný pro překonání bezpečnostního zařízení se nazývá průlomová odolnost a udává jak dlouho je konkrétní prostředek schopný odolávat kvalifikovanému napadení dostupnými metodami a nástroji. Vypočítá se podle následujícího vzorce:

$$\Delta t = t_2 - t_1 \text{ [min]} \quad (1)$$

$\Delta t$  – časový interval potřebný k překonání překážky, tedy odporový čas

$t_2$  – čas zahájení práce na překonání zábrany

$t_1$  – čas konečného překonání překážky

Tento vzorec platí pro výpočet minimální průlomové odolnosti pro otvorové výplně. V případě stanovení průlomové odolnosti pro úschové objekty je vzorec o něco odlišný, jelikož se na něj vztahují další veličiny. Průlomová odolnost je tedy základní charakteristikou MZS a je vyjádřena tzv. bezpečnostní úrovní objektu. [5]

## 2.1 Stupeň rizika ohrožených objektů

Vedle průlomové odolnosti je dalším kvantitativním ohodnocením prvků MZS také stupeň rizika ohrožených objektů, vyjádřený následujícím vztahem:

$$R = T_{\text{vloupání}} / t_i; t_i > 1 \quad (2)$$

**R** – stupeň rizika ohrožení objektu (koeficient rizikovosti)

**T<sub>vloupání</sub>** – doba minimální průlomové odolnosti úschovného objektu

**t<sub>i</sub>** – čas potřebný k zásahu policie ČR nebo SBS

Riziko ohrožení objektu bude tím menší, čím bude větší koeficient R. Aby byl prvek MZS účinný, musí být jeho hodnota větší než 1. Pokud bude hodnota menší než 1, ochrana podstatně ztrácí na efektivitě. Naopak čím bude hodnota větší než 1, tím více se bude riziko ohrožení snižovat a ochrana bude kvalitnější. [4]

## 2.2 Rozdělení mechanických zábranných systémů

Přestože MZS zahrnují širokou škálu mechanicko-bezpečnostních prvků, můžeme MZS rozdělit do tří základních skupin:

- Prostředky obvodové ochrany
  - zdi,
  - ploty,
  - vrcholové zábrany (ostnatý drát, žiletkový drát a další),
  - visací zámky a petlice,
  - průchozí prvky zdí a plotů (brány, závory turnikety apod.). [5]
- Prostředky plášťové ochrany
  - dveře (bezpečnostní dveře),
  - mříže,
  - rolety,
  - bezpečnostní skla a folie,
  - okna,
  - cylindrické vložky. [5]

- prostředky předmětové ochrany
  - komorové trezory
  - komerční úschovné objekty (ohnivzdorné skříně, skříňové trezory aj.). [5]

### 2.3 Požadavky na mechanické zábranné systémy

Požadavky a klasifikace na MZS vycházejí z toho, zda se jedná o prostředky plášťové příp. obvodové ochrany nebo prostředky předmětové ochrany. Pro splnění zadání diplomové práce jsou podstatnější požadavky na prostředky plášťové příp. obvodové ochrany a z tohoto důvodu se dále práce zaměřuje pouze na ně.

Norma, která stanovuje požadavky a klasifikace na prostředky plášťové ochrany, má označení ČSN P ENV 1627 a má název Okna, dveře, uzávěry – Odolnost proti násilnému vniknutí – Požadavky a klasifikace. Vztahuje se na následující způsoby otevírání: otáčení, sklápění, skládání, otevírání a sklápění, posunování (vodorovné a svislé) a navinování jakož i na pevné konstrukce. Na základě této normy je bezpečnostní prvek či prostředek zařazen do tzv. bezpečnostní třídy, která udává požadovanou úroveň odolnosti proti pokusům o násilné vniknutí. [6]

Tab. 1. Bezpečnostní třídy o odporový čas otvorových výplní [6]

Bezpečnostní třída	Kategorie náradí	Předpokládaný způsob napadení	Odporový čas [min]
1	Nepoužívá se	Příležitostný zloděj zkouší rozbít okno, dveře nebo okenice užitím fyzického násilí, např. kopáním, naražením ramene, vyvrtáváním.	Neměřen
2	A	Příležitostný zloděj dále zkouší rozbít okno, dveře nebo okenice užitím jednoduchých nástrojů, např. šroubováku, kleští, klínu.	3
3	B	Zloděj zkouší zajistit přístup použitím dalšího šroubováku či páčidla.	5
4	C	Zkušený zloděj dále používá pily, kladiva, sekery, sekáče a přenosné akumulátorové	10

		vrtačky.	
5	D	Zkušený zloděj dále používá elektrické nářadí, např. vrtačku, přímočarou pilu a úhlovou brusku o průměru max. 125 mm.	15
6	E	Zkušený zloděj dále používá výkonné elektrické nářadí např. vrtačku, přímočarou pilu a úhlovou brusku o průměru max. 230 mm.	20

Jak je vidět, obsahuje tabulka šest bezpečnostních tříd, přičemž první třída je pro objekty s nízkými riziky vloupání a třída šest pro objekty s velkými riziky vloupání. Dále tabulka uvádí předpokládaný způsob napadení pro každou bezpečnostní třídu. Poslední sloupec udává minimální odporový čas, resp. průlomovou odolnost, který musí prvek v dané třídě splňovat. Při výběru prvku v dané bezpečnostní třídě je třeba mít na vědomí, že první a druhá třída neposkytuje dostatečné zabezpečení, třetí a čtvrtá třída je pro civilní použití nejvhodnější, pátá a šestá třída má speciální určení, např. v oblasti bank či armády. Pojišťovny obvykle vyžadují minimálně bezpečnostní třídu 3.

### 2.3.1 Pyramida bezpečnosti

Dalším vodítkem, které klasifikuje mechanická zábranné prvky, je tzv. Pyramida bezpečnosti, je rozdělena čtyř stupňů bezpečnosti, reprezentující jednotlivé úrovně zabezpečení dle normy ČSN P ENV 1627. Definuje odolnost výrobků např. proti odvrtní, vyhmatání, vytržení, hrubému násilí atd.



Obr. 4. Pyramida bezpečnosti [7]

Jak je vidět z obrázku, má každý bezpečnostní stupeň své barevné označení, které umožňuje zákazníkovi optimální a přehledný výběr bezpečnostních prvků, protože každý takovýto výrobek má na obalu barevné i číselné označení stupně Pyramidy bezpečnosti. Je především vhodná pro zákazníky, kteří neznají nebo nemají přístup k výše uvedené normě. Základním předpokladem zařazení výrobku do systému Pyramidy bezpečnosti je jeho přezkoušení zkušební laboratoří a u certifikačního orgánu pak následná certifikace odolnosti výrobku proti násilnému vniknutí (ČSN P ENV 1627).

## 2.4 Návrh MZS

Návrh MZS by měl vycházet z bezpečnostní analýzy nebo bezpečnostního posouzení (které je dále popsáno v části návrhu PZS) či z požadavků pojišťoven. Doporučený je pak následující postup:

1. Stanovit dojezdový čas zásahové jednotky PCO či policie
2. Podle důležitosti chráněného zájmu stanovit koeficient rizikivosti
3. Z těchto údajů stanovit minimální průlomový čas pro MZS, resp. jejich průlomovou odolnost
4. Následně navrhnout konkrétní MZS [4]

### 3 POPLACHOVÉ ZABEZPEČOVACÍ SYSTÉMY

Poplachový zabezpečovací systém a především jeho návrh, bude zabírat největší část diplomové práce a to jak v části teoretické tak praktické. Než se ale přejde k popisu tohoto systému, je nejdříve dále uvedeno objasnění změny v normě 50131-1 ed.2, která popisuje systémové požadavky na PZTS, proti její předchozí normě, a to především změnu názvu EZS na PZS.

#### 3.1 Změna normy 50131-1 ed.2 proti předchozím normám

Poplachové zabezpečovací systémy byly a jsou dosud známé pod názvem elektronické zabezpečovací systémy. V roce 2009 nabyla účinnosti norma ČSN EN 50131-1 ed.2, která nahrazuje normu ČSN EN 50131-1 z roku 1999. Tato norma na rozdíl od předchozího vydání rozlišuje poplachové systémy pro detekci přepadení a poplachové systémy pro detekci vniknutí. Z tohoto důvodu jsou některé body této normy formulovány odděleně pro tyto dva druhy zabezpečení. V originále této normy se kromě jediné zkratky, IAS (Intruder Alarm Systém – poplachový systém pro detekci vniknutí), použité v předchozím vydání normy, objevuje zkratka I&HAS (Intruder and Hold-up Alarm Systém – poplachový systém pro detekci vniknutí a přepadení). Na několika místech normy jsou použity zkratky HAS (Hold-up Alarm Systém – poplachový systém pro detekci přepadení) tam, kde systém postrádá funkci detekce vniknutí, a IAS tam, kde systém postrádá funkci detekce přepadení. Proto jsou nyní v českém překladu normy místo dosud používané zkratky EZS používány zkratky z originálu – I&HAS „poplachové zabezpečovací a tísňové systémy“, IAS pro „poplachové zabezpečovací systémy“ a pro HAS „poplachové tísňové systémy“. V českých textech lze uvedené zkratky z originálu nahradit následujícím způsobem: I&HAS=PZTS, IAS=PZS, HAS=PTS. Jelikož se budu především zabývat návrhem poplachového systému pro detekci vniknutí, tedy klasického EZS, budu dále ve své práci používat zkratku PZS.

Mimo výše uvedené skutečnosti, je norma proti předchozímu vydání více přehlednější díky prezentaci velkého množství funkcí formou tabulek a zavádí novou funkci – detekci podstatného snížení dosahu detektorů pohybu. Přesněji definuje podmínky znemožňující uvedení do stavu střežení a definuje za jakých podmínek je povoleno tyto podmínky překonat. Dále je dle normy podstatně snížena doba ověřování dostupnosti komunikace v okamžiku nastavování střežení a zvýšila se povinná kapacita paměti událostí na



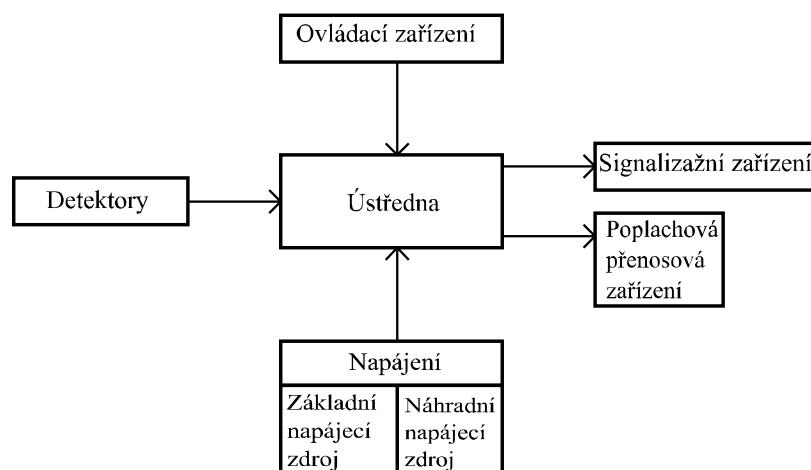
dvojnásobek a byly přidány některé povinně zaznamenávané události. Naprosto nově jsou definovány požadavky na přenos poplachu poplachovým přenosovým systémem. [8]

### 3.2 Popis a účel poplachového zabezpečovacího systému

PZS jsou komplexem technických prvků sloužících k detekování či rozpoznání přítomnosti nežádoucích osob s tím účelem, aby dokázaly tuto skutečnost určitým způsobem (akusticky, opticky) signalizovat a informovat majitele objektu nebo určenou osobu o této skutečnosti. Je tedy zřejmé, že proti mechanickým zábranným systémům nezabraňují vstupu nežádoucích osob do objektu, ale pouze na něj upozorňují. To je tedy hlavní důvod, proč tyto systémy mezi sebou doplňovat a kombinovat. Ale nyní zpět k poplachovému systému.

Srdcem celého systému je ústředna, které monitoruje a vyhodnocuje stavy detektorů v objektu a v případě narušení objektu je na ní, aby vyhlásila poplach a poslala informaci o tomto poplachu dále. PZS musí obsahovat následující prvky:

- ústřednu,
- detektory (vstupní prvky),
- signalizační zařízení / poplachové přenosové systémy (výstupní prvky),
- ovládací zařízení,
- napájecí zdroj,
- kabeláž. [2]



Obr. 5. Schéma PZS

### 3.2.1 Ústředny PZS

Jak již bylo naznačeno, je ústředna mozkiem celého systému PZS. Základní funkce ústředny PZS jsou následující:

- příjem a vyhodnocení výstupních elektrických signálů od detektorů,
- napájení detektorů a dalších komponentů PZS elektrickou energií,
- umožnění diagnostiky systému PZS,
- umožnění pomocí ovládacího zařízení do stavu střežení a do stavu klidu,
- ovládání signalizačních, přenosových, zapisovacích a jiných zařízení, která indikují narušení.

Ústředny PZS se v zásadě dělí do čtyř skupin, a to podle způsobu připojení smyček. [6]

#### 3.2.1.1 Analogové ústředny

Každá poplachová smyčka je připojena na samostatný vyhodnocovaný obvod, kde jsou informace předávány pomocí změny napětí nebo proudu. Do obvodu tedy přichází analogový signál. Smyčky jsou zpravidla zakončeny tzv. zakončovacím odporem tak, aby smyčka vykazovala předepsanou hodnotu odporu pro příslušný typ ústředny. Pokud dojde k aktivaci detektoru ve smyčce, změní se tím odpor smyčky a dojde k vyhlášení poplachu. Nejčastěji jsou smyčky PZS zapojeny sériovým řazením detektorů. Nevýhodou tohoto systému je ovšem poměrně rozsáhlá kabeláž, protože ke každému detektoru musí být přiveden kabel příslušné smyčky. [5]

#### 3.2.1.2 Sběrníkové ústředny (ústředny s přímou adresací čidel)

Ústředna, pracující na principu komunikace po datové sběrnici ústředna – detektor. Detektory předávají informace ve formě dat, kdy ústředna periodicky generuje adresy jednotlivých detektorů a přijímá příslušné odezvy. Všechny detektory musí být vybaveny komunikačním modulem, který umožňuje komunikaci s ústřednou. Výhodou tohoto systému je minimální kabelová síť, kde jsou jednotlivé detektory připojeny v libovolném pořadí na zpravidla čtyřvodičovém vedení (dva vodiče slouží pro napájení a dva jako datová sběrnice. Další výhodou je, že v případě aktivace detektoru ústředna oznámí, které konkrétní čidlo bylo aktivováno. Nevýhodou je omezení na celkovou délku vedení a také nutnost se vyvarovat uzavřeným okruhům přes nezanedbatelnou plochu, do kterých by se mohlo indukovat elektromagnetické rušení. [5]

### 3.2.1.3 *Koncentrátorové ústředny*

Tyto ústředny pracují na principu datové komunikace ústřednou – koncentrátor (sběrníkový modul smyček či expandér). Detektory jsou připojeny na koncentrátory pomocí smyček jako u analogových ústředen a komunikace mezi koncentrátory a ústřednou probíhá po analogové nebo datové sběrnici. Lze také na vstupy koncentrátorů přímo připojit jednotlivé digitální detektory, stejně jako u sběrníkových ústředen. [5]

### 3.2.1.4 *Ústředny s bezdrátovým přenosem*

Jedná se o ústředny pracující nejčastěji v pásmu telemetrie 433 MHz. Ústředna přijímá informace od detektorů bezdrátovým přenosem, kde přenos signálu je nejčastěji osmibitový, kódovaný a adresa detektoru je čtyřbitová. Tyto systémy se používají nejčastěji všude tam, kde by byla náročná či nákladná instalace kabeláže. Venku mají tyto systémy dosah až 200 m, ale v objektu je tento dosah značně snížen. Výhody jsou především ve snadné instalaci bez nutnosti větších stavebních zásahů a také snadné rozšíření systému o další prvky se snadnou změnou konfigurace systému. Ústředny pracují buď s jednosměrnou, nebo obojsměrnou komunikací. [5]

## 3.2.2 **Detektory PZS**

Dalšími základními prvky v systému PZS jsou detektory, sloužící k detekci narušení objektu. Detektory jsou zařízení, která reagují na fyzikální změny tak, že převádí vstupní fyzikální veličiny na jinou výstupní fyzikální veličinu. Při narušení objektu nastane změna vstupního signálu (jejího parametru), která způsobí změnu parametru výstupní fyzikální veličiny, která je následně zpracovávána a vyhodnocena. Detektory používané v PZS pracují často na různých fyzikálních principech. [5]

### 3.2.2.1 *Rozdělení detektorů PZS*

Základní rozdělení detektorů v systému PZS je podle druhu ochranné zóny, kterou má detektor detekovat. Rozdělení vychází z již uvedeného prostorového členění technické ochrany:

- **Prvky obvodové ochrany:**
  - mikrofonicke kabely,
  - infračervené závory a bariéry,

- mikrovlnné bariéry,
  - štěrbinové kabely,
  - zemní tlakové hadice,
  - perimetrická pasivní infračervená čidla. [6]
- **Prvky plášťové ochrany:**
- magnetické kontakty,
  - čidla na ochranu prosklených ploch,
  - mechanické kontakty,
  - vibrační čidla,
  - poplachové fólie, tapety, polepy a poplachová skla,
  - drátová čidla,
  - rozpěrné tyče. [6]
- **Prvky prostorové ochrany:**
- pasivní infračervená čidla,
  - aktivní infračervená čidla,
  - ultrazvuková čidla,
  - mikrovlnná čidla,
  - kombinovaná duální čidla. [6]
- **Prvky předmětové ochrany:**
- otřesová čidla,
  - čidla na ochranu zavěšených předmětů,
  - kapacitní čidla. [6]

### 3.2.3 Detektory prostředí

Zatím jsem uváděl detektory, které mají sloužit k ochraně objektu před neoprávněnou osobou nebo přesněji k její detekování. Ovšem zabezpečení objektu dnes již nezahrnuje jen ochranu proti hrozbám, jako jsou vloupání, odcizení majetku a jim podobné. Ve stále větší

míře zahrnuje zabezpečení objektu také tzv. hlásiče nebo-li detektory prostředí, které jsou určeny pro detekování hrozeb především uvnitř objektu. Nejznámější a nejrozšířenější jsou hlásiče požáru, které se dokonce při stavbě nového domu stávají povinností. Vedle těchto požárních hlásičů existuje mnoho druhů detektorů prostředí, které jsou určeny pro detekování či snímání různých druhů látek nebo veličin. Zde jsou vedeny nejběžnější detektory prostředí:

- hlásiče požáru:
  - hlásiče teplotní,
  - ionizační hlásiče kouře,
  - optické hlásiče kouře,
  - multisenzorové hlásiče s využitím plynové detekce,
  - optické hlásiče plamene,
  - lineární optické hlásiče,
  - lineární tepelné detektory – teplotní kabely,
  - aspirační hlásiče, [5]
- detektory úniku plynu,
- detektory teploty,
- detektory vlhkosti,
- detektory zaplavení,
- detektory stavu elektroinstalace aj.

#### 3.2.4 Signalizační zařízení

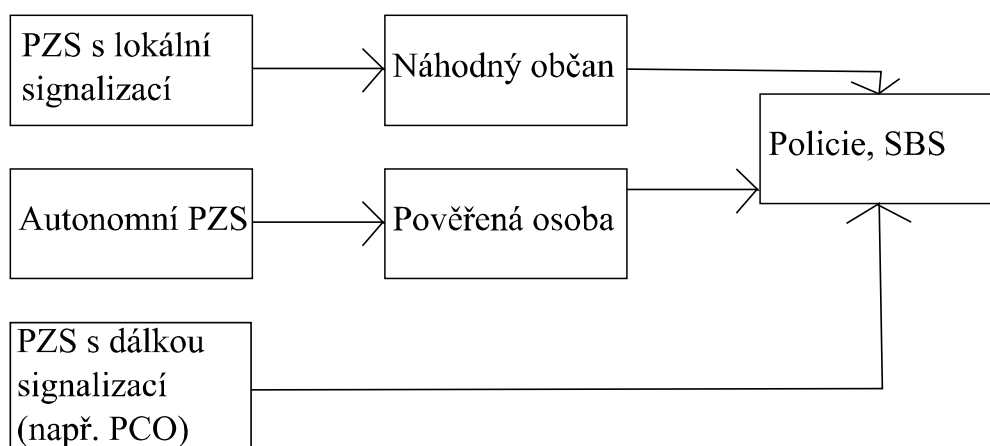
Jedná se o výstupní prvky PZS, které mají v případě narušení objektu opticky nebo akusticky toto narušení signalizovat. Nejčastěji používaným je akustická signalizace (siréna), jejíž součástí může být optická signalizace (světelný maják). Při použití sirén se jedná spíše o psychologický efekt, který by měl odradit pachatele než spoléhat na to, že při aktivaci sirény upozorní na poplach policii náhodný občan. Z tohoto důvodu by se měla tato zařízení instalovat tak, aby byla dobře viditelná a zároveň obtížně dostupná. [5]

### 3.2.5 Poplachová přenosová systémy

V případě vyhlášení poplachu, musí ústředna tuto informaci předat (v případě, že jsou tyto systémy součástí PZS) a to buď pověřené osobě či majiteli objektu nebo přímo na pult centralizované ochrany. Toto předání informace se uskuteční pomocí poplachových přenosových systémů, které zahrnují síť a zařízení pro přenos informací. Pro předání těchto informací se v dnešní době využívají následující přenosové cesty:

- telefonní linky,
- GSM brány,
- radiové sítě,
- internetová spojení,
- vyhrazené přenosové cesty.

Pro zajištění větší bezpečnosti se používají dvě přenosové cesty, které jsou na sobě nezávislé.



Obr. 6. Možný způsoby předání poplachová informace

Na obrázku jsou uvedeny tři možné způsoby předání poplachové informace. U PZS s lokální signalizací se jedná o sirénu či maják a předpokládáme, že náhodný občan zavolá policii. U autonomního PZS je poplachová informace předána stálé službě objektu, která provádí vyhodnocení informace i zákrok. Je řešena taktéž akustickou či optickou signalizací. U PZS s dálkovou signalizací je informace předána např. majiteli objektu nebo na PCO pomocí GSM brány a ten pak po zvážení situace může zavolat policii.

### 3.2.6 Ovládací zařízení

Slouží k ovládání celého systému PZS a především pak k uvádění systému do stavu střežení a do stavu klidu. Volíme je podle stupně zabezpečení a podle požadavků zákazníka s tím, aby pro uživatele byla tato zařízení co nejkomfortnější. Jejich základní funkce jsou následující:

- odstavení a resetování systému,
- konfigurace instalačních parametrů systému,
- odpínání a připínání smyček,
- zadávání uživatelských kódů. [5]

Nejčastěji se umísťují co nejbližně vstupním dveřím, aby uživatel mohl v daném čase co nejrychleji objekt zastřežit či odstřežit. Mezi nejpoužívanější ovládací zařízení řadíme:

- kódové klávesnice,
- blokovací zámky,
- čtečky identifikačních karet,
- spínací zámky.

### 3.2.7 Napájecí zdroje

Napájecí zdroje slouží pro napájení celého systému PZS elektrickou energií a to i v případě výpadku napájecího napětí ze sítě. Z tohoto hlediska rozdělujeme napájecí zdroje na základní napájecí zdroj a náhradní napájecí zdroj. V případě rozsáhlého systému PZS používáme přídatné síťové napájecí zdroje s vlastním náhradním zdrojem napětí.

Základní napájecí zdroj musí být schopen dodávat takový proud, který bude součtem proudových odběrů všech prvků v systému včetně ústředny. Musí být dimenzován tak, aby po skončení nejdelšího výpadku sítě dodával potřebný proud i pro proud potřebný k dobíjení připojeného akumulátoru během doby stanovené v související normě. Náhradní napájecí zdroj musí být dimenzován tak, aby byl schopen překonat nejdelší výpadek základního zdroje dle požadavků normy. [5]

Vztah, za kterého odvodíme potřebnou kapacitu náhradního zdroje je následující:

$$Q = [ ( I + 0,1 * I ) * t ] * 1,2 \quad (3)$$

$Q$  – potřebná kapacita akumulátoru

$I$  – odběr všech komponentů PZS

$0,1 \cdot I$  – rezerva

$t$  – požadovaná doba zálohování (dle normy)

$1,2$  – koeficient stárnutí [9]

Je třeba mít na vědomí, že uvedený vzorec není obecně platný.

Norma rozlišuje tři typy napájecích zdrojů:

- Typ A – Základní napájecí zdroj (síťový zdroj) a náhradní napájecí zdroj dobíjený (dobíjený akumulátor).
- Typ B – Základní napájecí zdroj a náhradní napájecí zdroj nedobíjený (akumulátor nedobíjený).
- Typ C – Základní zdroj napájení s omezenou kapacitou (baterie). [2]

### 3.2.8 Kabeláž

V systému PZS se používají následující 4 druhy vedení:

- Napájení AC – jištěný přívod z rozvaděče o napětí 230V a průřezu  $1,5Cu$ .
- Napájení 12 V – je určeno pro napájení čidel a ostatních komponentů PZS. Jedná se o napájení z výstupu AUX ústředny nebo pomocného zdroje.
- Zóny – Jedná se o vedení, na kterém je nízké napětí zpravidla kolem 5V. Je potřeba se vyvarovat souběhu se silovým vedením a umístěním s telefonem nebo sítí v jednom kabelu.
- BUS – mezi ústřednou a klávesnicí je přenos dat typu sběrnice. V moderních systémech je BUS komunikace možná i mezi ostatními komponenty EZS (čidla, moduly). Sběrnice nesmí mít souběh se silovým vedením a nesmí být ve společném kabelu s jiným vedením.



### 3.3 Vybrané systémové požadavky na PZS dle normy ČSN EN 50131-1 ed.2

#### 3.3.1 Stupně zabezpečení

Pro provedení PZS mu musí být přiřazen stupeň zabezpečení, který je rozdělen do čtyř stupňů, přičemž stupeň 1 je nejnižší a stupeň 4 je nejvyšší. Jsou vhodné zejména jako vodítko pro projektanty či osoby zodpovědné za ochranu objektu.

Tab. 2. Stupně zabezpečení [8]

<b>Stupeň 1</b>	Nízké riziko	Předpokládá se, že vetřelec nebo lupič mají malou znalost PZS a mají k dispozici omezený sortiment snadno dostupných nástrojů.
<b>Stupeň 2</b>	Nízké až střední riziko	Předpokládá se, že vetřelec nebo lupič mají omezené znalosti PZS a používání běžného náradí a přenosných přístrojů
<b>Stupeň 3</b>	Střední až vysoké riziko	Předpokládá se, že vetřelec nebo lupič jsou obeznámeni s PZS a mají rozsáhlý sortiment nástrojů a přenosných elektronických zařízení.
<b>Stupeň 4</b>	Vysoké riziko	Používá se, má – li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů PZS.

#### 3.3.2 Třídy prostředí

Každý prvek v PZS je určený pro jistý druh prostředí, které se v této normě rozděluje do čtyř tříd v závislosti na teplotě prostředí a jeho vlhkosti.

Tab. 3. Třídy prostředí [8]

<b>Třída prostředí I – vnitřní</b>	Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách při stálé teplotě (předpokládají se změny teplot
------------------------------------	---

	v rozmezí +5 °C až +40 °C, při střední relativní vlhkosti přibližně 75 % bez kondenzace).
<b>Třída prostředí II – vnitřní – všeobecné</b>	Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách, kde není stálá teplota (předpokládají se změny teplot v rozmezí -10 °C až +40 °C, při střední relativní vlhkosti přibližně 75 % bez kondenzace).
<b>Třída prostředí III – venkovní – chráněné nebo extrémní vnitřní podmínky</b>	Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty PZS nejsou plně vystaveny povětrnostním vlivům (předpokládají se změny teplot v rozmezí -25 °C až +50 °C, při střední relativní vlhkosti přibližně 75 % bez kondenzace).
<b>Třída prostředí IV – venkovní – všeobecné</b>	Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty PZS jsou plně vystaveny povětrnostním vlivům

### 3.3.3 Přístupové úrovně

Pro kategorizaci přístupu uživatelů ke komponentům systému specifikuje norma čtyři přístupové úrovně:

- Úroveň 1 – Přístup pro kohokoli – funkce, u nichž je vyžadován přístup na úrovni 1, který nesmí mít žádná omezení přístupu.
- Úroveň 2 – Přístup pro uživatele (např. osobu obsluhující systém) – funkce, které ovlivňují provozní stav, aniž by došlo ke změně konfigurace systému. Přístup k funkcím na této úrovni musí být vymezen prostřednictvím klíče nebo kódové klávesnice nebo zámku nebo dalšího ekvivalentního prostředku.
- Úroveň 3 – Přístup pro uživatele (např. servisní techniky) – všechny funkce ovlivňující konfiguraci PZS mimo zásahů do konstrukce zařízení.
- Úroveň 4 – Přístup pro uživatele (např. výrobce zařízení) – přístup k součástkám, které umožňují změnu konstrukce zařízení. Používá se především při výměně operačního softwaru. [8]

### 3.3.4 Ochrana proti sabotáži

Komponenty PZS musí mít prostředky, které zamezí přístup k jejich vnitřním součástkám pro minimalizaci rizika sabotáže. Požadavky na ochranu proti sabotáži se liší podle stupně zabezpečení a podle toho, zda je komponent PZS umístěn uvnitř nebo vně střeženého prostoru. Komponenty umístěné vně střežených prostor, musí mít vhodné prostředky pro ochranu proti sabotáži (např. přídatná ovládací zařízení, výstražná zařízení). Všechny svorky a prvky elektronického nastavování musí být umístěny uvnitř krytů komponentů PZS. Tyto kryty musí dostatečně robustní, aby nemohlo dojít k nezjištěnému přístupu k vnitřním prvkům. Následující tabulka specifikuje komponenty PZS, které musí být vybaveny prostředky pro detekci sabotáže. [8]

Tab. 4. Komponenty na které se vztahuje detekce sabotáže [8]

Komponenty	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Ústředna, poplachový přenosový systém, výstražné zařízení, napájecí zdroj, doplňkové ovládací zařízení	P	P	P	P
Detektory vniknutí	V	P	P	P
Rozvodné krabice	V	V	P	P
V = volitelné, P = povinné				

V další tabulce jsou uvedeny požadavky na detekci možných způsobů sabotáží, rozdělených opět podle stupně zabezpečení.

Tab. 5. Požadavky na detekci možných způsobů sabotáží [8]

Způsoby	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Otevření normálním způsobem	P	P	P	P
Odejmutí z montážní plochy	V	P	P	P
Vniknutí do akustického výstražného zařízení	V	V	V	V
Vniknutí do ústředny, poplachového přenosového systému a doplňkového	V	V	V	P

ovládacího zařízení				
Změna orientace detektoru	V	V	P	P
V = volitelné, P = povinné				

### 3.3.5 Požadavky na napájení

Napájecí zdroje musí splňovat požadavky obsažené v normě ČSN EN 50131-6, která, jak již bylo uvedeno, mimo jiné rozděluje napájecí zdroje na tři typy – typ A, typ B a typ C.

Norma požaduje, aby napájecí zdroje byly schopné zajišťovat energii pro PZS za všech podmínek a mohou být umístěny v jednom nebo více komponentech PZS, nebo v samostatném krytu.

U napájecího zdroje typu C (baterie), musí být tento zdroj schopen napájet PZS po dobu nejméně jednoho roku a to za jakýchkoliv provozních podmínek a také musí generovat poplachový signál nebo zprávu dříve, než napětí klesne pod úroveň potřebnou pro normální provoz PZS. V případě napájecích zdrojů typu A a B, musí být náhradní napájecí zdroj schopen napájet systém PZS po dobu stanovenou v následující tabulce. [8]

Tab. 6. Minimální doba napájení náhradním napájecím zdrojem [8]

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

V PZS, který má napájecí zdroj typu A, musí být náhradní napájecí zdroj nabit na 80% maximální kapacity v časech stanovených v následující tabulce.

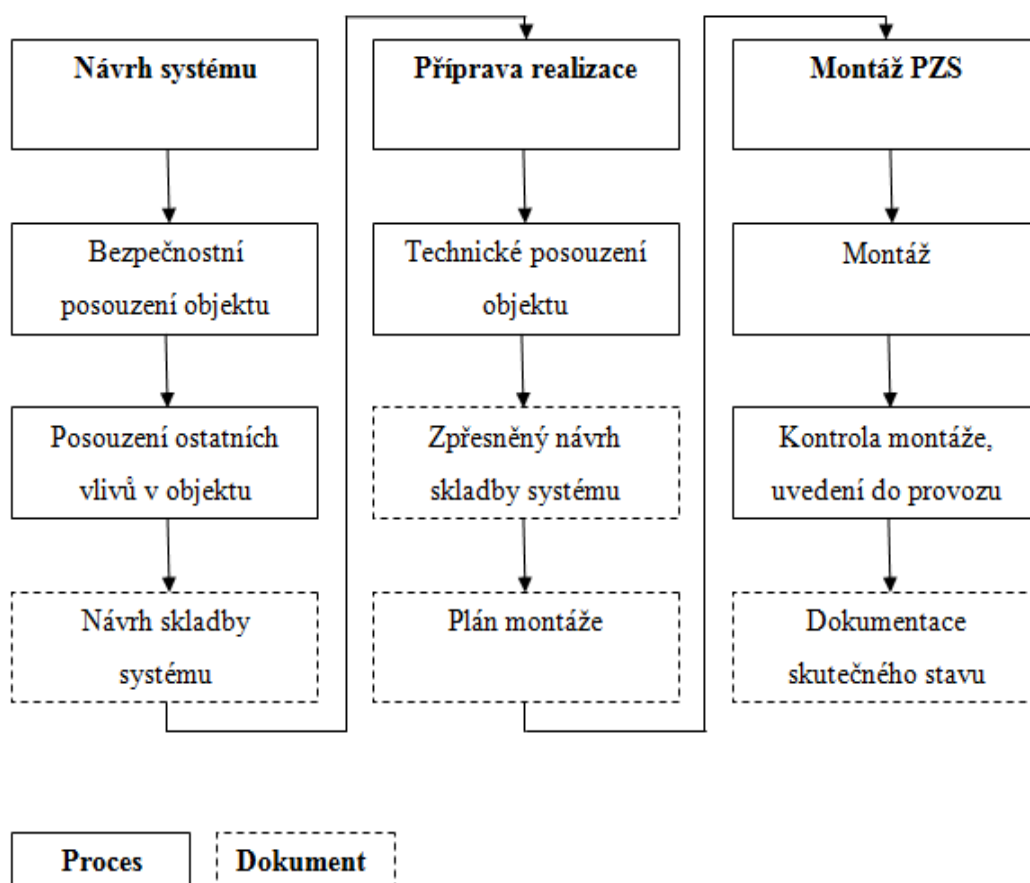
Tab. 7. Doba nabíjení náhradního napájecího zdroje [8]

Typ náhradního zdroje	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Maximální doba po nabití	72	72	24	24

### 3.3.6 Zřizování PZS

Zřizování PZS vychází z norem ČSN CLC/TC 50131-7 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace a TNI 33 4591-1 Komentář k CLC/TC 50131-7 - Část 1: Návrh EZS.

Ještě než přejdu k návrhu PZS, popíši zde následující vývojový diagram činností při zřizování PZS, který je uveden v normě ČSN CLC/TC 50131-7.



Obr. 7. Vývojový diagram činností při zřizování PZS [10]

Z diagramu je vidět, že norma uvádí tři etapy zřizování PZS:

- Návrh systému,
- Příprava realizace,
- Montáž PZS

Zřizování PZS je v některých literaturách doplněno ještě o další etapu – trvalý provoz.

Pro účely splnění zadání diplomové práce je nejdůležitější první etapa a to návrh systému. Z tohoto důvodu budou dále v teoretické části rozebírány jednotlivé kroky návrhu systému, které pak budou využity v praktické části.

### 3.4 Návrh PZS

Návrh systému je, jak již bylo nastíněno, prvním krokem při zřizování PZS. Cílem je stanovit rozsah systému PZS včetně výběru jeho komponentů příslušného stupně zabezpečení a příslušné třídy prostředí. Výstupem je pak dokument, který by měl obsahovat následující informace:

1. Údaje o zákazníkovi – jméno, adresa, obchodní jméno a všechny další informace nutné k identifikaci zákazníka.
2. Údaje o střežených objektech – název a adresa střežených objektů, jejich popis a účel využití objektu.
3. Stupeň zabezpečení – stupeň navrženého PZS, příp. jeho podsystémů.
4. Třída okolního prostředí – třída prostředí každého komponentu systému.
5. Seznam materiálu (přehled komponentů) – seznam typů rozmístění veškerého zařízení a dále stanovení předpokládaného pokrytí detektorů pohybu.
6. Konfigurace systému – podrobné informace o konfiguraci systému, včetně postupu uvádění systému do stavu střežení/klidu.
7. Hlášení poplachu – informace o poplachových a výstražných zařízeních a informace o způsobu předání poplachu (pokud je informace o poplachu předávána na PCO, tak i jeho název).
8. Legislativa – informace o shodě jednotlivých komponentů PZS s požadavky místní nebo národní legislativy.
9. Normy – informace o shodě jednotlivých komponentů PZS s národními nebo evropskými normami.
10. Další předpisy – informace o shodě jednotlivých komponentů PZS s jakýmkoli dalšími předpisy, např. směrnicemi pojišťoven.
11. Certifikace – podrobnosti prohlášení o certifikaci komponentů PZS.

12. Zásah – plánovaná odezva na aktivaci poplachu nebo poruchy (kdo, jakým způsobem a za jak dlouho bude zásah provádět).
13. Údržba – doporučení pro pravidelnou údržbu PZS a jeho komponentů včetně údajů o četnosti servisních prohlídek.
14. Opravy - podrobné údaje o servisní firmě nebo středisku. [10]

Aby se mohl takovýto dokument zpracovat, je nejdříve potřeba znát informace o chráněném objektu včetně vlivů, které na něj působí uvnitř i mimo něj a mnoho dalších faktorů, které mohou působit na objekt z hlediska bezpečnosti (především hrozby). Získání těchto informací se provádí pomocí tzv. bezpečnostního posouzení, kterého popisují obě výše zmiňované normy a určují aspekty, které by v rámci bezpečnostního posouzení měly být brány v úvahu. Je třeba dodat, že bezpečnostní posouzení, je určeno především pro I&HAS. Druhou možností pro získání informací o chráněném objektu z hlediska bezpečnosti je bezpečnostní analýza, která je rozsáhlejší než bezpečnostní posouzení, zahrnuje více aspektů a je mnohem využitelnější v oblasti bezpečnosti vůbec. Zahrnuje totiž i metody analýzy rizik, které se používají především pro rozsáhlejší systémy.

Následuje otázka, kterou z těchto metod při získání informací o objektu vybrat. Je to i z důvodu toho, že při návrhu zabezpečení malého či středně velkého objektu je bezpečnostní posouzení bráno jako synonymum bezpečnostní analýzy. S tímto názorem lze částečně souhlasit, protože při provádění bezpečnostní analýzy malého či středně velkého objektu není nutné, aby byla bezpečnostní analýza objektu rozsáhlá či obsahovala analýzu rizik, ale postačuje ji provést formou bezpečnostního posouzení.

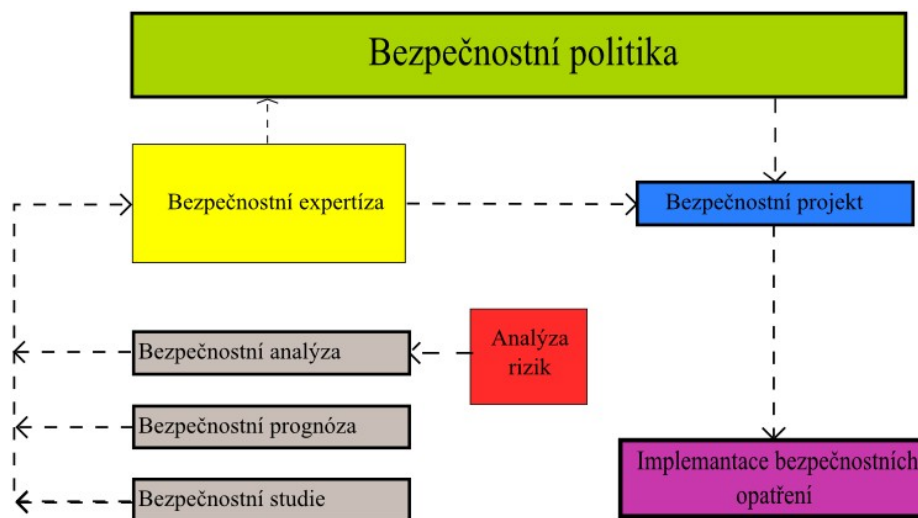
### 3.4.1 Bezpečnostní analýza

Před návrhem jakéhokoliv systému je potřeba si nejprve celý stav zanalyzovat. Jelikož se práce zabývá návrhem zabezpečení objektu, je pro ni důležitá analýza z hlediska bezpečnosti, tedy bezpečnostní analýza. Obecně se dá říci, že bezpečnostní analýza je první etapou přípravy návrhu systému fyzické, technické a režimové ochrany objektu, majetku, osob i technologií uvnitř objektu. Pokud má být takováto ochrana účinná, nelze ji realizovat bez kvalifikovaně zpracované bezpečnostní analýzy jako objektivního východiska dalších bezpečnostně projektových prací. Bezpečnostní analýza má poskytovat širší pohled na analyzovaný objekt a jejím cílem a výstupem by mělo být identifikování maxima zranitelností obsažených ve zkoumaném objektu včetně jeho nedostatků,

definování a odhadnutí možných rizik a hrozeb, které by mohly mít negativní dopady na analyzovaný objekt. Nesmí se přitom zapomenout na určení efektivity a funkčnosti stávajících bezpečnostních opatření či systémů, aby bylo možné navrhnout nové tak, aby mohla být všechna rizika snížena na akceptovatelnou úroveň. Bezpečnostní analýza je tedy proces, při kterém se provádí dekompozice zkoumaného objektu na základní prvky, vyhledávají se a zkoumají se vnitřní zranitelnosti objektu, vnější hrozby a implementované ochranné mechanismy. [11]

### 3.4.1.1 Bezpečnostní analýza jako součást bezpečnostní politiky

V současné době si stále více organizací uvědomuje důležitost péče o bezpečnost. Systematickým řešením problému bezpečnosti v organizaci je dokument zvaný bezpečnostní politika. Tento dokument v obecné rovině popisuje základní požadavky organizace na zabezpečení a jeho cílem je ochrana veškerého hmotného i nehmotného majetku firmy, ochrana jejího dobrého jména a předmětu činnosti organizace. Obsah bezpečnostní politiky musí pokrývat veškeré aspekty zabezpečení ochrany organizace, počínaje např. ochranou budov přes definování jednotlivých skupin zaměstnanců, zálohování dat až po např. plány obnovy činnosti. Bezpečnostní politiku schvaluje vedení organizace a její schválená podoba je závazná pro všechny zaměstnance organizace. Aby mohla být bezpečnostní politika naplněna, musejí se správně stanovit bezpečnostní rizika vůči aktivitám dané organizace a přijmout odpovídající přiměřené bezpečnostních opatření. A právě zde je nutné provést bezpečnostní analýzu, která tyto rizika identifikuje a pomocí některé z metod analýzy rizik stanoví jejich závažnost.



Obr. 8. Bezpečnostní analýza jako součást bezpečnostní politiky



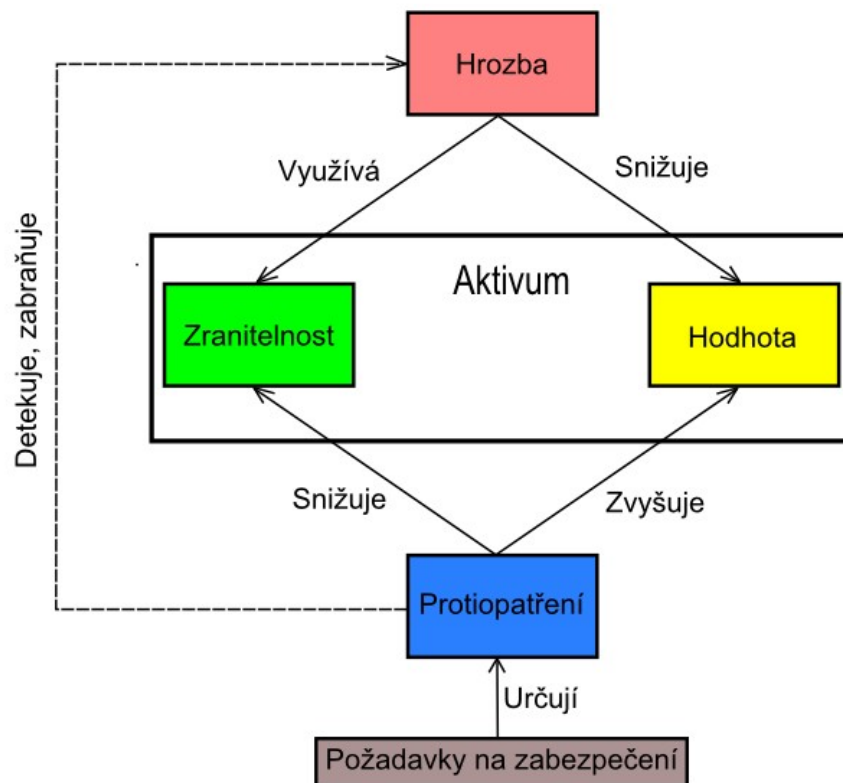
Jak je vidět z obrázku, je součástí bezpečnostní analýzy také analýza rizik, která definuje pravděpodobnost vzniku hrozeb a jejich dopadu na aktiva. Vedle bezpečnostní analýzy je pro organizaci důležitá i bezpečnostní prognóza, které by měla popisovat a předpovídat další vývoj v oblasti bezpečnosti organizace. Měla by se opírat o kvalifikované odhady, vztahovat se k určitému časovému období a vyjadřovat alternativy možných budoucích stavů. Na obrázku je dalším vstupem do bezpečnostní politiky tzv. bezpečnostní studie, která není nezbytnou součástí, nicméně je často na místě. Z hlediska finančního jde o poměrně levnou záležitost, jež může celý projekt zkrátit a tím ve finále i zlevnit. Účelem takovéto studie je získat základní orientaci v organizaci a činnostech firmy i základní údaje o bezpečnostní situaci. Na podkladě těchto informací je možné stanovit přesněji zejména rozsah budoucích prací, rozvržení a náplň jednotlivých etap a tím i rámcovou finanční náročnost. Tyto tři dokumenty se následně shrnou do tzv. bezpečnostní expertízy. Smyslem této expertízy je shromáždění potřebných odborných podkladů pro definování celkové bezpečnostní politiky organizace a pro vypracování tzv. bezpečnostního projektu. Bezpečnostní projekt konkretizuje a popisuje způsob realizace bezpečnostních opatření v jednotlivých druzích bezpečností a na jeho základě se implementují bezpečnostní opatření.

#### **3.4.1.2 Analýza rizik**

Jak již bylo uvedeno, je součástí každé kvalifikované bezpečnostní analýzy také analýza rizik. Analýza rizik je obvykle chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a jejich dopadu na aktiva, tedy stanovení rizik a jejich závažnosti. V analýze rizik se používají následující pojmy:

- aktivum – vše co má pro subjekt nějakou hodnotu a mělo by být odpovídajícím způsobem chráněno,
- hrozba – je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu,
- zranitelnost – vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou,
- riziko – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti,
- protiopatření – postup, technický prostředek nebo cokoliv, co bylo navrženo pro zmírnění působení hrozby, snížení zranitelnosti nebo dopadu hrozby. [11]

Mezi uvedenými pojmy jsou souvislosti a vazby, uvedené na následujícím obrázku:



Obr. 9 Vazby v analýze rizik

Hrozba využije zranitelnosti, překoná protiopatření a působí na aktivum, kde způsobí škodu. Aktivum svou hodnotou motivuje člověka k aktivaci hrozby. Vůči působení hrozby se aktivum vyznačuje určitou zranitelností. Aktivum je zároveň chráněno protiopatřeními před hrozbami. Protiopatření chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva. Protiopatření zároveň odrazují od aktivování hrozeb. Hrozba působí jednak přímo na aktivum, nebo na protiopatření, s cílem získat přístup k aktivu. Aby mohla hrozba působit, musí být aktivována. Pro svou aktivaci vyžaduje zdroje (vytvoření podmínek pro její působení). Pravděpodobnost, že hrozba přejde v událost, nazýváme rizikem. Tuto pravděpodobnost pak stanovujeme na základě některé z metod analýzy rizik.

### 3.4.2 Bezpečnostní posouzení

Podobně jako bezpečnostní analýza je bezpečnostní posouzení první etapou přípravy návrhu systému PZS. Cílem je stanovení potřebného stupně zabezpečení, případně pojistné třídy dané pojišťovny, ve smyslu jejich směrnic. Aspekty, které je nutno brát při bezpečnostním posouzení v potaz, jsou uvedeny v normě ČSN CLC/TC 50131-7 a jedná se

především o aspekty, které mají základ v zabezpečovaných hodnotách a aspekty týkajících se stavebních dispozic objektu.

### **Bezpečnostní posouzení objektu – zabezpečované hodnoty**

Míra rizika vloupání do střežených objektů závisí na charakteru střeženého majetku a berou se v úvahu následující faktory:

1. Druh majetku
  - Snadnost zpeněžení
  - Atraktivita pro pachatele
  - Nebezpečí vloupání
2. Hodnota majetku
  - Maximální pravděpodobná hodnota jednotlivé ztráty
  - Následné výdaje související se ztrátou
  - Osobní vztah k věcem
3. Množství nebo velikost
  - Snadnost odejmutí a převozu
  - Snadnost dalšího nakládání/zpeněžení
  - Snadnost přístupu do střežených prostor
4. Historie krádeží
  - Způsoby vloupání při předcházejících krádežích a vloupání
5. Nebezpečí
  - Pro okolní prostředí
  - Zneužití střeženého majetku
  - Pro osoby
6. Poškození
  - Vandalismus na střeženém objektu
  - Riziko žhářství na střeženém majetku
  - Psychologické problémy osob po loupeži [10]

### **Bezpečnostní posouzení objektu – budova**

Při posuzování rizik jsou určujícím faktorem také stavební dispozice objektu. Aspekty, které se mají brát v úvahu jsou následující:

1. Konstrukce

- a. Stěny
  - b. Podlahy
  - c. Sklepy
  - d. Střechy
  - e. Stropy
2. Otvory
    - a. Dveře
    - b. Světlíky
    - c. Okna
    - d. Ventilační prostupy
    - e. Ostatní části usnadňující nepovolený vstup
  3. Režim provozu objektu
    - a. Přítomnost pracovníků ostrahy
    - b. Veřejný/neveřejný prostor
    - c. Osídlenou objektu
    - d. Doprava
  4. Držitelé klíčů
    - a. Dosažitelnost držitelů klíčů schopných reagovat na poplach PZS
    - b. Evidence
    - c. Uložení
  5. Lokalita
    - a. Riziko kriminality v dané oblasti
    - b. Sousední objekty, které by mohly usnadnit vloupání
    - c. Rychlost a kvalita reakce na poplachový signál PZS
    - d. Blízkost nebo jiný vztah k sousedním objektům
  6. Stávající zabezpečení
    - a. Kvalita a rozsah stávajících mechanických zabezpečovacích zařízení
    - b. Kvalita a rozsah stávajícího PZS
  7. Historie krádeží, loupeží a výhružek
    - a. Počet předcházejících incidentů a způsob jejich realizace
  8. Místní legislativa nebo předpisy
    - a. Bezpečnostní předpisy, které by mohly ovlivnit návrh systému PZS
    - b. Požární předpisy

- c. Požadavky vzhledem ke konstrukci objektu
- 9. Prostředí střeženého objektu
  - a. Městská zástavba
  - b. Venkov [10]

### **Bezpečnostní posouzení objektu – vlivy působící na PZS a mající původ ve střežených objektech**

Jedná se o faktory, které ovlivňují výběr, umístění a nastavení komponentů PZS, především detektorů. Obecně je lze považovat za ovlivnitelné uživatelem. Příklady faktorů, které by mohly negativně ovlivnit provoz PZS jsou následující:

1. Vodovodní potrubí
  - a. Vliv pohybu vody v potrubích z plastů (při nasazení mikrovlnných detektorů)
2. Vytápění vzduchotechnické a klimatizační systémy
  - a. Vliv turbulence vzduchu (např. při nasazení ultrazvukových detektorů)
3. Vývěsní štíty nebo obdobné zavěšené předměty
  - a. vliv zavěšených předmětů, které se mohou pohybovat v zorném poli detektorů (např. záclony, rostliny)
4. Výtahy
  - a. Vliv vibrací způsobený výtahy jinými strojními zařízeními (např. při nasazení otřesových detektorů)
5. Zdroje světla
  - a. Vliv osvětlovacích zařízení (výbojky, zářivky), které mohou rušit mikrovlnné detektory
  - b. Vliv bodových reflektorů, které pokud jsou nasměrovány na čočky pasivního infračerveného detektoru, mohou způsobit planý poplach
  - c. Vliv světlometů vozidel
6. Elektromagnetické rušení
  - a. Veškeré elektrické záření může být zdrojem elektromagnetického rušení a ovlivnit provoz PZS (zejména při instalaci kabelových rozvodů)
  - b. Vlivy elektrostatických výbojů při zacházení s elektronickými součástkami (elektrické svařovací soupravy, elektrické generátory nebo motory, domácí spotřebiče s elektromotory)

7. Vnější zvuky
  - a. Při použití ultrazvukových detektorů brát v úvahu vlivy zařízení, které jsou schopny generovat zvuky v přibližně stejném frekvenčním pásmu (např. kompresory, telefonní zvonky, vzduchová potrubí)
8. Domácí zvířata
  - a. Při použití detektorů pohybu brát v úvahu možný výskyt zvířat
9. Průvan
  - a. Vliv průvanu je nejcitlivější na ultrazvukové pasivní infračervené detektory
  - b. Možnost pohybu volně zavěšených předmětů (zavěsy, rostliny atd.)
10. Uspořádání skladovaných předmětů
  - a. Brát v úvahu rozmístění skladovaných předmětů, které by mohly při manipulaci zastínit zorné pole detektoru
  - b. Možnost samovolného uvolnění skladovaných předmětů
11. Stavební konstrukce střežených objektů
  - a. Věnovat zvláštní pozornost konstrukci střech, stěn, podlah a sklepů.
  - b. U lehkých stavebních materiálů možnost vibrace
  - c. Stav a usazení dveří a oken
12. Zvláštní pozornost
  - a. Typ a konstrukce skla (tvrzené vrstvené atd.) – podle toho zvolit vhodný typ detektoru
  - b. Možnost vyjmutí skla z rámu
  - c. Brát v úvahu teplotní rozdíly na povrchu skla (může dojít ke kondenzaci vody)
13. Riziko planých poplachů u tísňových systémů
  - a. Věnovat pozornost při umístění, aby nedocházelo k aktivaci planých poplachů např. dětmi [10]

### **Bezpečnostní posouzení objektu – vlivy působící na PZS a mající původ vně střežených objektů**

Obecně faktory, které uživatel nemůže ovlivnit, a které mohou ovlivnit provoz PZS. Příklady faktorů, které mohou negativně ovlivnit provoz PZS jsou následující:

1. Dlouhodobě působící faktory

- a. Faktory, u nichž se nepředpokládá změna (řádově roky) – železnice, silnice, letecká doprava, parkoviště
2. Krátkodobě působící faktory
  - a. Vlivy výstavby v blízkosti střeženého objektu
3. Vlivy počasí
  - a. Brát v úvahu převažující a potenciální vlivy počasí
  - b. Působení blesků
4. Vysokofrekvenční rušení
  - a. Zařízení, které mohou způsobovat vysokofrekvenční rušení (vysílače veřejné rozhlasové sítě nebo televize, základnové stanice GSM, radary)
  - b. vliv na bezdrátové komponenty PZS
5. Sousední objekty
  - a. Vlivy vibrací nebo generace elektromagnetického rušení od zařízení (zejména průmyslové objekty)
6. Vlivy klimatických podmínek
  - a. Použití zařízení vhodná pro dané potenciální klimatické podmínky, např. teplotní rozsah nebo vlhkost
7. Ostatní vlivy
  - a. Aktivity v přístupných vnějších částech objektu (např. hrající se děti)
  - b. Aktivity v přilehlých částech budovy [10]

### 3.4.3 Volba a umístění komponentů systému

Po provedení bezpečnostní analýzy nebo bezpečnostního posouzení se přejde k fázi výběru komponentů PZS a jejich umístění. Komponenty mají být zvoleny tak, aby odpovídaly stupni zabezpečení a dané třídě prostředí. Při jejich umístění se musí věnovat pozornost minimalizaci vzniku falešných poplachů. V případě umístění detektorů musíme dodržovat doporučení výrobce tak, aby zajišťovaly požadovaný rozsah pokrytí. Projektant by měl znát také fyzikální podstatu detektorů, aby se vyvaroval nevhodnému umístění detektorů (např. PIR detektor naproti oknu). Vhodnou pomůckou pro projektanta je níže uvedená tabulka, která uvádí minimální rozsah střežení:

Tab. 8. Minimální rozsah střežení [10]

Vzít v úvahu	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Obvodové dveře	O	O	O+P	O+P
Okna		O	O+P	O+P
Ostatní otvory		O	O+P	O+P
Stěny				P
Stropy nebo střechy				P
Podlahy				P
Místnosti	T	T	T	T
Předmět (vysoké riziko)			S	S
<b>O</b> = otevření		<b>S</b> = objekt, vyžadující zvláštní pozornost		
<b>P</b> = průnik		<b>T</b> = past		

Další z komponentů PZS – komunikátor má být umístěn uvnitř střeženého prostoru podobně jako ústředna, která musí být z komponentů PZS nejvíce chráněna. Volba ústředny, by měla vycházet z jejich následujících parametrů:

- počet zón,
- počet podsystémů,
- počet datových výstupů,
- typ ústředny (analogová apod.),
- počet klávesnic,
- počet uživatelských kódů,
- paměť událostí,
- sběrníkové moduly (typy),
- počet programovatelných výstupů,
- zdroj pro napájení komponentů AUX (jaký proud je k dispozici),



- výstup pro sirénu (jaký proud je k dispozici). [9]

Dalším velmi podstatným komponentem je propojení PZS. Zde záleží na tom, zda se jedná o propojení kabelem nebo bezdrátovou komunikaci. V případě pevného propojení by měly být kabely vedeny uvnitř střeženého prostoru, pokud to ovšem podmínky nedovolují a jsou vedeny mimo střežený prostor, musejí být chráněny vhodným způsobem. Předpisy pro vnitřní sdělovací vedení určuje norma ČSN 34 2300. Důležité je, aby rozměr a typ kabelu přiváděl napětí ke komponentu systému měřené při maximální hodnotě odebíraného proudu a spodní hranici výstupního napětí, které by nebylo nižší než je spodní maz napájecího napětí komponentů. V případě bezdrátové komunikace se má věnovat pozornost vlivu úmyslného nebo neúmyslného radiového vysílání, které používá stejný kmitočet a stejný způsob modulace jako bezdrátové prvky v PZS, protože by tyto vlivy mohly znemožnit správnou komunikaci.

Výstražná či signalizační zařízení mají být zvoleny tak, aby jejich zvuk byl odlišný od zvuku výstražných zařízení jiného PZS. Také je třeba brát v úvahu národní předpisy, které mohou upravovat dobu trvání akustické signalizace (spadá do konfigurace systému). [10]

#### **3.4.4 Požadavky na konfiguraci systému**

Návrh systému zahrnuje i podrobné informace o hlavních funkcích systému, nastavení systému (především postupů pro uvádění do jednotlivých stavů střežení/klid) a údajů pro programování okruhů jako je noc, den, sabotáž atd. V případě konfigurace uvádění PZS do stavu střeží/klidu popisuje tento postup výše uvedená norma. [10]

## 4 POJIŠTĚNÍ

Při návrhu zabezpečení je častým požadavkem zákazníka, aby zabezpečení splňovalo požadavky pojišťovny, u které má pojištěn majetek, případně objekt. Je to samozřejmě na místě, protože součástí ochrany objektu či majetku má být také pojištění. Každá bezpečnostní agentura nebo projektant by měli mít základní přehled v požadavcích pojišťoven v závislosti na pojistné hodnotě. Když si prohlédneme statistiky o počtu a způsobech vloupání za poslední léta, bylo by hloupé až krátkozraké, nepřipomenout si činnost pojišťoven. Pojišťovny nabízejí dnes celou škálu pojištění. Pro ochranu objektu či majetku je určeno pojištění majetku, které poskytuje finanční náhradu v případě škody v důsledku živelní události, krádeže nebo loupeže. Jeho základním cílem je ochrana majetku proti následkům nepředvídatelných událostí. Toto pojištění se dále dělí dvou kategorií:

- **Pojištění domácnosti** – vztahuje se na věcné škody na věcech, které jsou součástí bytu, pokud jsou věci uvedeny v pojistných podmínkách pojišťovny. Pojištění domácnosti se zpravidla vztahuje na dvě skupiny pojistných rizik:
  - riziko krádeže věcí v pojištěné domácnosti (příp. v dalších nebytových prostorách) a riziko vzniklé na základě vloupání,
  - riziko živelné zkázy, tj. zkázy pojištěných věcí napař. v důsledku požáru, výbuchu plynu, zemětřesení, záplav, povodní, pádu stromu či letadla aj.
- **Pojištění nemovitosti** – je určeno k zabezpečení budov, staveb a bytů proti živelným pohromám a krádežím. Pojištění se sjednává zejména pro tři typy nemovitostí:
  - rodinné domy vč. vedlejších objektů typu kolen, samostatně stojících garáží, plotů, studní aj.
  - byty (zdi, podlahy, stropy)
  - rekreační objekty, tj. chaty a chalupy

Tato pojištění je nutné od sebe odlišovat, ačkoliv často dochází k jejich záměně. Pojištění domácnosti se totiž vztahuje pouze na věci náležející k domácnosti, jako je např. nábytek, elektronika, cennosti, audiovizuální technika, aj. Naproti tomu pojištění nemovitostí se vztahuje pouze na pojištěnou stavbu, nikoli tedy na věci, které tato stavba uvnitř obsahuje.

## 4.1 Požadavky pojišťoven

Každá pojišťovna, která nabízí pojištění majetku, má své pojistné podmínky v závislosti na pojistné hodnotě, které určují požadavky na zabezpečení. Obecně lze říci, že čím vyšší je pojistná hodnota pojišťovaného objektu či majetku, tím větší budou požadavky na zabezpečení. Konkrétní požadavky se však u jednotlivých pojišťoven liší, stejně tak vliv stupně zabezpečení na cenu pojistného. Musí se také připomenout, že pojišťovny jsou sdruženy v České asociaci pojišťoven, která mimo jiné vydala několik aplikačních směrnic, které určovaly požadavky na zabezpečení, a které většinou vycházely z technických norem. Směrnice byly vždy pouze doporučující a pojišťovny se jimi mohly řídit, ale nemusely. ČAP před několika lety přestala směrnice aktualizovat a pojišťovny se nyní řídí vlastními předpisy. Často ale tyto předpisy u některých pojišťoven kopírují původní směrnice ČAP. Situace v ČAP je dnes tedy taková, že její sekce neživotního pojištění se na posledním zasedání dohodla, že situaci v této oblasti zmapuje, nepředpokládá se ale, že by k tomu došlo dříve, než koncem roku 2011. Jelikož tedy nejsou pojistné podmínky u pojišťoven stejné, je na obrázku uveden příklad pojišťovny Allianz na zabezpečení proti vloupání v závislosti na pojistné hodnotě.

Limit plnění	200 000,- Kč	700 000,- Kč	2 000 000,- Kč	5 000 000,- Kč
Zabezpečení	A	B	C	D
alternativa 1	bezpečnostní zámek tř.2* (tj. s bezpečnostní vložkou a s bezpečnostním štítem)	masivní dveře (odolné proti dynam. zatížení dle tř.2*), dva bezpečnostní zámky tř.3*, okna do 3 m nad terénem odolnosti tř.2* (mříže, žaluzie, rolety)	bezpečnostní dveře tř.2*, bezpečnostní zámek tř.4*, okna do 3 m nad terénem odolnosti tř.2*, EZS st.2** s lokální signalizací	bezpečnostní dveře tř.2*, bezpečnostní zámek tř.4*, okna do 3 m nad terénem odolnosti tř.2*, EZS st.2** s lokální signalizací, fyzická ostraha
alternativa 2	bezpečnostní zámek tř.1*, EZS st.1** s lokální signalizací	bezpečnostní zámek tř.2*, EZS st.2** s lokální signalizací	bezpečnostní zámek tř.3*, EZS st.3** se signalizací na PCO	bezpečnostní zámek tř.3*, EZS st.4** se signalizací na PCO
alternativa 3	bezpečnostní zámek tř.1*, fyzická ostraha	bezpečnostní zámek tř.2*, fyzická ostraha	bezpečnostní zámek tř.3*, ozbrojená ostraha	bezpečnostní zámek tř.3*, dvoučlenná ozbrojená ostraha
* ČSN P ENV 1627 - odpovídá systému značení "Pyramida bezpečnosti":			tř.2 = dostatečná ochrana (zelená) tř.3 = vysoká ochrana (modrá) tř.4 = velmi vysoká ochrana (červená)	
** Směrnice České asociace pojišťoven ČAP 50 131-7				

Obr. 10. Příklad pojištění proti vloupání v závislosti na pojistné hodnotě [12]

## **II. PRAKTICKÁ ČÁST**

## 5 LEGISLATIVNÍ RÁMEC PRO VYBRANÉ BEZPEČNOSTNÍ SYSTÉMY

Zabezpečení objektu bude zahrnovat poplachové zabezpečovací systémy a mechanické zábranné systémy. Následující text obsahuje vybranou legislativu na tyto bezpečnostní systémy doplněnou o potřebné elektrotechnické normy. Tento legislativní rámec je začat více zešíroka, protože určuje požadavky nejen na prvky bezpečnostních systémů, ale na výrobky celkově. Jedná se o následující zákony:

1. Zákon č. 22/1997Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů.
2. Zákon č. 59/1998 Sb. o odpovědnosti za škodu způsobenou vadou výrobku.
3. Zákon č. 64/1986 Sb. o České obchodní inspekci.
4. Zákon č. 102/2001 Sb. o obecné bezpečnosti výrobků.

Dále jsou uvedeny nařízení vlády, k provedení zákona č. 22/1997Sb o technických požadavcích na výrobky, kterými se stanovují technické požadavky na konkrétní zařízení. V případě PZS se jedná o elektrická zařízení.

1. Nařízení vlády č. 17/2003Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí.
2. Nařízení vlády č. 616/2006Sb., technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility.
3. Nařízení vlády č. 426/2000 Sb., kterým se stanoví technické požadavky na rádiová a na telekomunikační koncová zařízení.

### 5.1 Legislativní rámec na PZS

1. Normy

Tab. 9. Normy pro PZS

Označení normy	Zjednodušený název
ČSN EN 50131-1 ed. 2	Systémové požadavky
ČSN EN 50131-2-2	Detektory narušení - Pasivní infračervené detektory

ČSN EN 50131-2-3	Požadavky na mikrovlnné detektory
ČSN EN 50131-2-4	Požadavky na kombinované pasivní infračervené a mikrovlnné detektory
ČSN EN 50131-2-5	Požadavky na kombinované pasivní infračervené a ultrazvukové detektory
ČSN EN 50131-2-6	Detektory otevření (magnetické kontakty)
ČSN CLC/TS 50131-2-7-1	Detektory narušení - Detektory rozbíjení skla (akustické)
ČSN CLC/TS 50131-2-7-2	Detektory narušení - Detektory rozbíjení skla (pasivní)
ČSN EN 50131-3	Ústředny
ČSN EN 50131-4	Výstražná zařízení
ČSN EN 50131-5-3	Požadavky na zařízení využívající bezdrátové propojení
ČSN EN 50131-6 ed. 2	Napájecí zdroje
ČSN CLC/TS 50131-7	Pokyny pro aplikace

## 2. Technické normalizační informace

Tab. 10. TNI pro PZS

Označení TNI	Název dokumentu
TNI 33 4591-1	Komentář k ČSN CLC/TS 50131-7 - Část 1: Návrh EZS
TNI 33 4591-2	Komentář k ČSN CLC/TS 50131-7 - Část 2: Montáž EZS
TNI 33 4591-3	Komentář k ČSN CLC/TS 50131-7 - Část 3: Prohlídky a funkční zkoušky EZS, revize elektrické instalace EZS

## 3. Související elektrotechnické normy

Tab. 11. Elektrotechnické normy

Označení normy	Název dokumentu
ČSN 33 2000-1	Elektrické instalace budov -Část 1: Rozsah platnosti, účel a základní hlediska
ČSN 33 2000-3	Elektrotechnické předpisy. Elektrická zařízení. Část 3: Stanovení základních charakteristik
ČSN 33 2000-4-41 ed. 2	Elektrické instalace nízkého napětí -Část 4-41: Ochranná opatření pro zajištění bezpečnosti -Ochrana před úrazem elektrickým proudem
ČSN 33 2000-4-43	Elektrické instalace budov -Část 4: Bezpečnost -Kapitola 43: Ochrana proti nadproudům
ČSN 33 2000-5-51 ed. 3	Elektrické instalace nízkého napětí -Část 5-51: Výběr a stavba elektrických zařízení -Všeobecné předpisy
ČSN 33 2000-5-52	Elektrotechnické předpisy -Elektrická zařízení -Část 5: Výběr a stavba elektrických zařízení -Kapitola 52: Výběr soustav a stavba vedení
ČSN 33 2000-6	Elektrické instalace nízkého napětí -Část 6: Revize
ČSN 34 2300	Předpisy pro vnitřní rozvody sdělovacích vedení
ČSN 33 4000	Elektrotechnické předpisy. Požadavky na odolnost sdělovacích zařízení proti přepětí a nadproudu
ČSN 33 4010	Elektrotechnické předpisy. Ochrana sdělovacích vedení a zařízení proti přepětí a nadproudu atmosférického původu
ČSN 33 0165	Elektrotechnické předpisy. Značení vodičů barvami nebo číslicemi. Prováděcí ustanovení
ČSN 33 1500	Elektrotechnické předpisy. Revize elektrických zařízení
ČSN 33 2130 ed. 2	Elektrické instalace nízkého napětí -Vnitřní elektrické rozvody (navrhování, provádění a rekonstrukce)

ČSN EN60529	Stupně ochrany krytem (krytí -IP kód)
-------------	---------------------------------------

## 5.2 Normy pro MZS

Tab. 12. Normy pro MZS

Označení normy	Název dokumentu
ČSN P ENV 1627	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí - Požadavky a klasifikace
ČSN P ENV 1628	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí - Zkušební metoda pro stanovení odolnosti při statickém zatížení
ČSN P ENV 1629	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí - Zkušební metoda pro stanovení odolnosti při dynamickém zatížení
ČSN P ENV 1630	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí - Zkušební metoda pro stanovení odolnosti proti manuálním pokusům o násilné vniknutí
ČSN 74 7731	Dveře odolnější proti vloupání
ČSN EN 1303	Stavební kování - Cylindrické vložky pro zámky - Požadavky a zkušební metody
ČSN EN 1906	Stavební kování - Dveřní štíty, kliky a knoflíky - Požadavky a zkušební metody
ČSN EN 12320	Stavební kování - Visací zámky a příslušenství visacích zámků - Požadavky a zkušební metody



## 6 BEZPEČNOSTNÍ ANALÝZA

### 6.1 Popis objektu a jeho okolí

Objekt se nachází v obci Brumov-Bylnice na adrese Hodňov 1011. Jde o třípodlažní multifunkční dům, tvořený dvěma prodejny a bytovou jednotkou. Byt není v současné době vybaven a využívám. Podle majitele budou tyto prostory do budoucna využívány buďto jako byt (nejpravděpodobnější možnost), anebo jako kanceláře či jiné prostory k pronájmu. Prodejny se nacházejí v přízemí, ve kterém je rovněž vstup do bytové jednotky. První prodejna (dále prodejna č. 1) se orientuje na prodej barev-laků a jejich potřeb. V druhé prodejně (dále prodejna č. 2) je obchod s drogerií. Objekt je přístupný z vedlejší silnice a pro zákazníky těchto prodejen je určeno malé parkoviště přístupné rovněž z vedlejší silnice, a které je součástí pozemku, na kterém se objekt nachází. Vedle objektu se nachází prodejna s loveckými potřebami, sázková kancelář a pošta. Za objektem je menší rodinný dům se zahradou oddělenou plotem. Naproti objektu přes hlavní silnici se nachází pohostinství. Velkou výhodou objektu je to, že takřka před vchodem do prodejny č. 2 se nachází veřejné osvětlení.

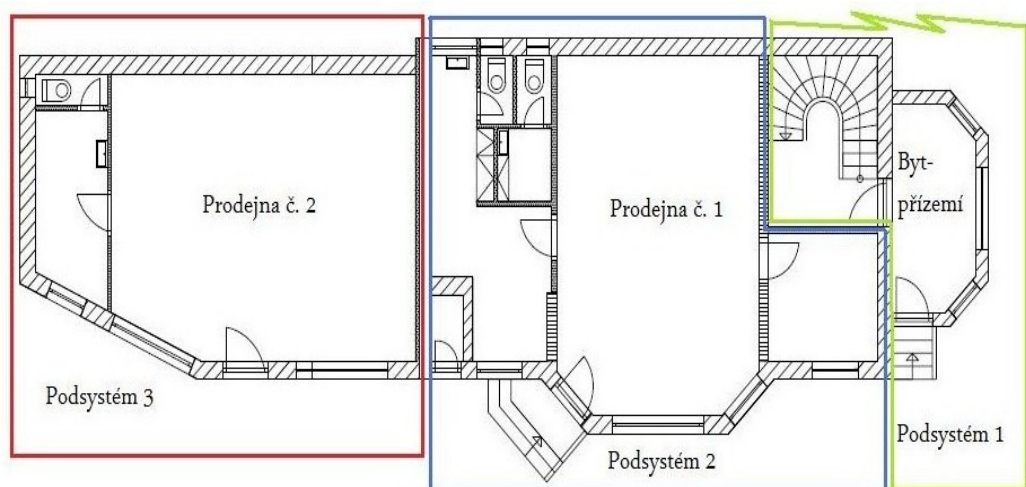
Při návrhu zabezpečení je potřeba brát v úvahu charakteristiku objektu – tedy to, že objekt je charakteristický tím, že slouží především jako objekt k pronájmu. Z toho vyplývá, že návrh zabezpečení by měl být univerzálnější a ne konkrétně navržen na současné prodejny a jejich zboží, protože tyto prodejny tam nemusí být dlouhodobě a po nich tam může vzniknout jiná prodejna s naprosto odlišným zbožím.



Obr. 11. Pohled na přední stranu objektu



Obr. 12. Pohled na západní stranu objektu



Obr. 13. Rozdělení přízemí objektu

## 6.2 Bezpečnostní posouzení objektu

### I. Prověrka lokality – Druh a rozsah majetku v objektu

#### Druh majetku

- Hmotný majetek
- Neatraktivnost majetku pro potenciálního pachatele

#### Hodnota majetku

- Prodejna č. 1 – majetek do 500 000 Kč
- Prodejna č. 2 – majetek do 400 000 Kč
- Byt – majetek do 100 000 Kč, v budoucnu cca do 500 000 Kč

#### **Vlastnictví majetku**

- Prodejna č. 1 – podnikatelský subjekt (dále podnájemník č. 1)
- Prodejna č. 2 – podnikatelský subjekt (dále podnájemník č. 2)
- Byt – soukromá osoba (dále majitel)

#### **Objem a velikost majetku**

- Snadnost krádeže: ano
- Snadnost přepravy: ano
- Snadnost zpeněžení zcizeného majetku: ne

#### **Historie krádeží**

- Výskyt krádeží: ne

#### **Utajované skutečnosti**

- Výskyt utajovaných skutečností: ne

#### **Poškození**

- Riziko vandalismu: ano
- Riziko zhářství: ne

## **II. Prověrka lokality – Struktura objektu**

#### **Základní údaje o objektu**

- Poloha objektu: městská zástavba
- Popis objektu: vícepodlažní; počet podlaží: 3 + sklep
- Účel objektu:
  - Byt
  - Prodejna č. 1 – zaměření barvy-laky
  - Prodejna č. 2 – zaměření drogerie

#### **Konstrukce objektu**

- Stavební konstrukce stěn, podlah a stropů:

- Pevná (venkovní zdivo, tloušťka stěn nad 300 mm)
- Lehká (vnitřní zdivo, tloušťka stěn nad 150 mm)

### Otvorové výplně

- Obvodové dveře a jejich konstrukce
  - Prodejna č. 1 – jednokřídlé prosklené
  - Prodejna č. 2 – jednokřídlé prosklené
  - Byt – jednokřídlé dřevěné
- Balkonové dveře
  - Byt – jednokřídlé prosklené, jedny v prvním patře
- Okna a jejich konstrukce
  - Prodejna č. 1 – otevíratelná čtyři okna, jedno neotevíratelné
  - Prodejna č. 2 – otevíratelná dvě okna
  - Byt – otevíratelná, 3 okna v přízemí, 7 oken v prvním patře a jedno okno v druhém patře
- Ostatní průlezné otvory a jejich výplně: ano – výlohy
  - Prodejna č. 1 – jedna výloha
  - Prodejna č. 2 – dvě výlohy

### Osazenstvo

- Počet osob normálně přítomných v objektu: dvě osoby (prodejci v prodejnách) + jejich zákazníci
- Fyzická ostraha: ne
- Přístup veřejnosti do objektu:
  - V prodejnách ano (v otevíracích hodinách)
  - V bytě ne

### Držení klíčů

- Dosažitelnost držitelů klíčů reagovat na činnost PZS: vyhovující

### Lokalita

- Riziko kriminality v lokalitě objektu: malé
- Možnost usnadnění vloupání ze sousedních objektů: ne
- Sousední obydlené objekty: ano

- Možnost zpozorování neoprávněného vniknutí do střeženého objektu za sousedních objektů: ano

### **Stávající zabezpečení**

- Mechanická zábranné prostředky
  - Prodejna č. 1 – vstupní dveře opatřeny dvěma zámky – klasickým a bezpečnostním, výloha je potažena bezpečnostní folií
  - Prodejna č. 2 – vstupní dveře opatřeny dvěma zámky – klasickým a bezpečnostním, výlohy jsou provedeny s bezpečnostním sklem
  - Byt – vstupní dveře opatřeny klasickým zámkem (bez bezpečnostního kování)
- Jiné poplachové systémy: ne
- Požadavky na úpravy mechanických částí: ano
  - Výměna vstupních dveří do bytu

### **Místní legislativa a předpisy**

- Předpisy ovlivňující projekt PZS : ne

### **III. Prověrka lokality – Ostatní vlivy**

#### **Podmínky uvnitř objektu**

- Vodovodní potrubí z plastů – pouze odpadní potrubí vedené v bytě z druhého patra
- Tepelné, klimatizační a ventilační systémy: v bytě se nachází plynový kotel, radiátory jsou ve všech částech objektu
- Zavěšené tabule a jiné předměty: ne
- Výtahy: ne
- Světla: v prodejnách jsou instalovány zářivky
- Elektromagnetické rušení: ne
- Domácí zvířata a škůdci: ne
- Průvan: ne
- Skladování nebo zpracování hořlavých či výbušných předmětů: ano, v obou prodejnách se prodávají předměty či látky, které jsou hořlavé.
- Přítomnost prašné nebo korozní atmosféry: ne

#### **Podmínky vně objektu**

- Pozemní a podzemní dopravní komunikace, parkoviště, letecká doprava: ano – pozemní doprava, objekt je blízko u hlavní cesty
- Vlivy počasí: ne
- Vysokofrekvenční rušení: ne
- Činnost v sousedních objektech (provoz těžkých strojů apod.): ne
- Ostatní vlivy: ne

#### **IV. Stanovení pojistných tříd**

Neprovedeno (z důvodů uvedených v teoretická části práce)

#### **V. Stanovení stupně zabezpečení**

Vzhledem k účelu a majetku objektu je pro PZS objektu stanoven stupeň zabezpečení 2 – nízké až střední riziko.

#### **VI. Klasifikace prostředí**

Vzhledem k provoznímu režimu objektu je určena třída prostředí II – prostředí vnitřní všeobecné.

#### **VII. Stanovení typu ochrany**

Ve všech částech objektu bude aplikována plášťová a prostorová ochrana.

#### **VIII. Způsoby předání poplachové informace**

Předání poplachové informace bude místní i dálkové (předání informace na mobilní telefon).

#### **IX. Speciální požadavky**

Je vhodné instalovat následující detektory prostředí:

- Požární hlásiče
- Detektor prostředí
- Detektor úniku plynu

#### **X. Zvláštní opatření**

Opatření vzhledem k minulým krádežím, poloze objektu apod.: ne

## XI. Požadavky majitele objektu

Požadavkem majitele je, aby hlášení o poplachu a jiné informace ze systému mu přicházely na mobilní telefon. Dalším požadavkem majitele je, aby se dal PZS rozšířit v případě, že bude objekt v budoucnu rozšířen o další patro, které by se nacházelo nad prodejnou č. 2.

### 6.3 Slabá místa objektu

Objekt je rozdělen do tří částí. V bytové části je rizikovým místem pro vloupání vstupní místnost, která má tři okna a vstupní dveře jsou ve velmi špatném stavu. O něco méně rizikovým jsou balkonové dveře, které jsou sice v prvním patře východní části budovy, ale jsou celé prosklené, i když by potenciální pachatel musel použít žebřík. Do bytu se lze také dostat za střechy prodejny č. 2, protože na této straně má byt dvě okna. Prodejna č. 1 má nejrizikovější místo v zadní části objektu, kde se nacházejí tři okna a kde by takřka nebylo potenciálního zloděje vidět. Do prodejny č. 1 lze také vniknout vstupními dveřmi či přes výlohy, ovšem pachatel by musel počítat s přímým výhledem na něj z hlavní cesty a veřejným osvětlením, které je kousek od vchodu. Prodejna č. 2 již tak dobře viditelná z hlavní cesty není a rizikovými místy je jak okno na západní straně objektu, tak okno na přední straně objektu. Výlohy a vstupní dveře nejsou tak viditelné z hlavní cesty jako v případě prodejny č. 1, ale výhodou je, že přímo před vchodem je veřejného osvětlení.



Obr. 14. Vstupní dveře do bytové části objektu



Obr. 15. Vstupní dveře do prodejny č. 1

#### 6.4 Hrozby vyplívající z bezpečnostního posouzení

- Neoprávněné vniknutí do objektu a s tím spojené odcizení či poškození majetku
- Vandalismus (týká se především výloh)
- Požár (především v obou prodejnách)
- Únik plynu (v místnosti s plynovým kotlem)
- Únik vody (v koupelně)

#### 6.5 Analýza kriminality

Bezpečnost a veřejný pořádek v obci zajišťuje městské policie a obvodní oddělení policie ČR Valašské Klobouky. Pro bezpečnostní analýzu jsou relevantní následující údaje:

Tab. 13. Trestná činnost v obci Brumov-Bylnice

Rok	Počet trestných činů	Počet majetkové trestné činnosti
2009	59	42
2010	53	40



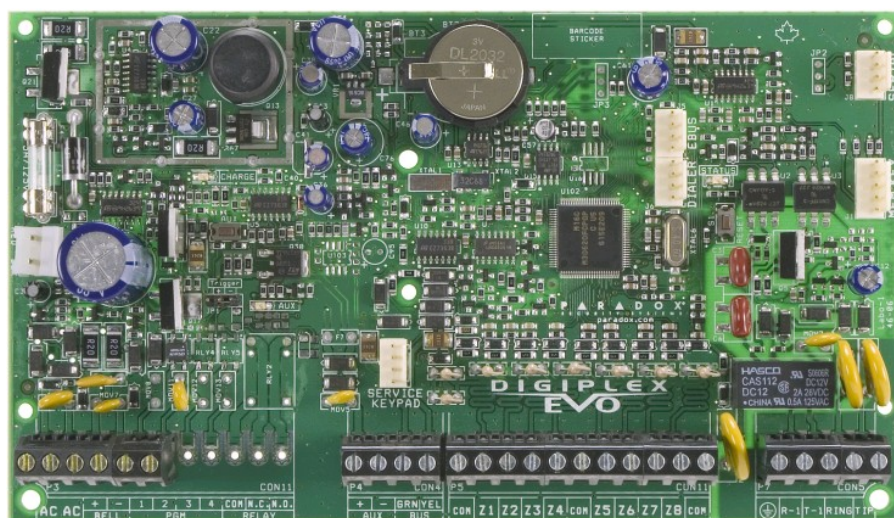
*Tab. 14. Počet vloupání v obci Brumov-Bylnice dle typu objektu*

<b>Rok</b>	<b>2009</b>	<b>2010</b>
Vloupání do bytů	0	4
Vloupání do objektů firem	4	3
Vloupání do chat	1	0
Vloupání do vozidel	5	1
Ostatní majetková trestná činnost	32	32

## 7 VÝBĚR A POPIS KOMPONENTŮ PZS

### 7.1 Ústředna Digiplex Evo48

Pro PZS jsem vybral ústřednu kanadské firmy Paradox Security Systems, která je určena pro střední a velké objekty. Ústřednu je možné rozšířit do maximálního počtu čtyřiceti osmi zón a také o bezdrátovou nastavbu. Celý systém je možné rozdělit do čtyř podsystémů. Jedná se o koncentrátorovou ústřednu, lze tedy na ní připojit detektory buď přímo pomocí sběrnice anebo přes expandéry.



Obr. 16. Ústředna Digiplex Evo48 [13]

#### 7.1.1 Základní vlastnosti ústředny

- 4 podsystémy
- 8 zón na ústředně (16 zdvojených zón, ATZ) rozšiřitelných na 48 zón přes čtyřvodičovou sběrnici
- 13 typů naprogramovatelných zón
- podpora max. 127 rozšiřujících sběrnicevých modulů
- připojení modulu až do vzdálenosti 914 m od ústředny
- 96 uživatelských kódů
- paměť na 1024 událostí
- 2 pevné PGM na ústředně (+3 volitelně)
- vestavěné přístupové funkce
- připojení modulů systémem Plug & Play
- programování bezdrátových ovladačů přes master nebo instalační kód

- vestavěná baterie pro zálohu času
- 1,7A spínaný napájecí zdroj
- 1 dohlížený bell výstup, AUX výstup a telefonní linka
- tlačítko pro softwarový reset
- tlačítko pro aktivaci/deaktivaci AUX výstupu
- programování ústředny přes LCD klávesnici nebo software Winload
- přehrání firmware přes 307USB převodník
- možnost bezdrátové nastavby přes RTX3 [13]

### 7.1.2 Technické parametry ústředny

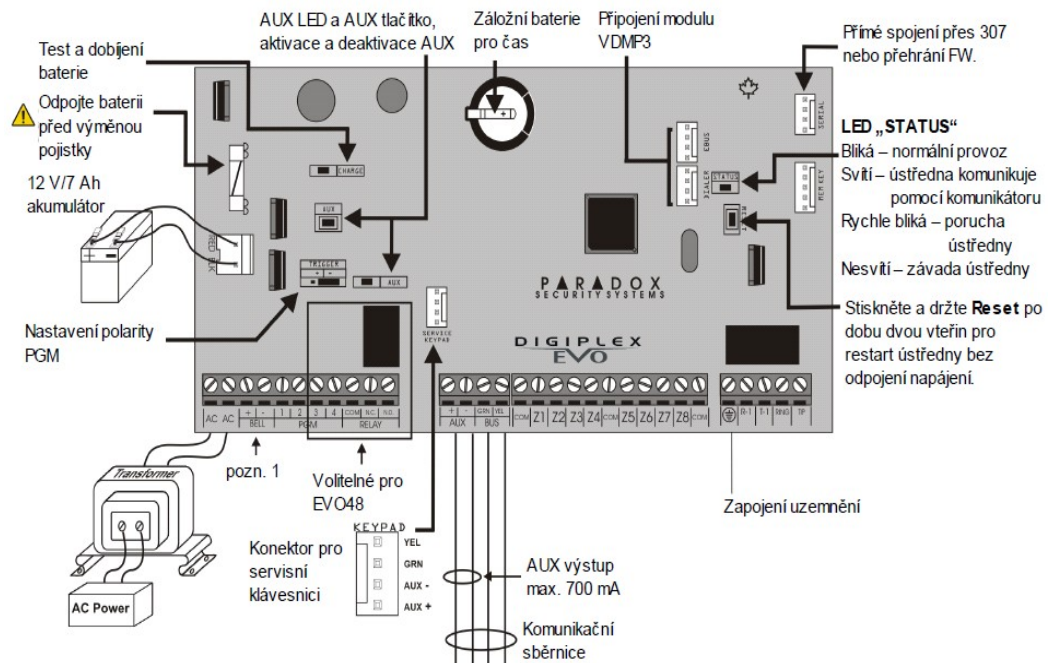
Tab. 15. Technické parametry ústředny [13]

Napájení ústředny	16 V AC, 50 - 60 Hz, 40 VA
Zálohovací akumulátor	12 V DC, min 4 Ah
Napájecí výstup	12 V DC, 600 mA trvale, 700 mA max.
Proudový odběr ústředny	110 mA
Výstup na sirénu	1 A, elektronická pojistka 3 A
Optická signalizace	LED dioda CHARGE, STATUS, AUX
Dobíjecí proud záložního akumulátoru	350/700 mA
PGM výstupy na ústředně	2 x opto-relé 50 mA polarita +/-
Doporučený záložní akumulátor	12 V, 7 Ah/18 Ah

### 7.1.3 Příslušenství k ústředně

- Box pro ústřednu – ESPRIT BOX D
- Záložní akumulátor BASIC 12V/18Ah (z výpočtu)
- 6 – žilový kabel Ka6x - 2x0.6+4x0.4
- Sběrníkový kabel UTP CAT3 2P Cu, 2x2x0.5

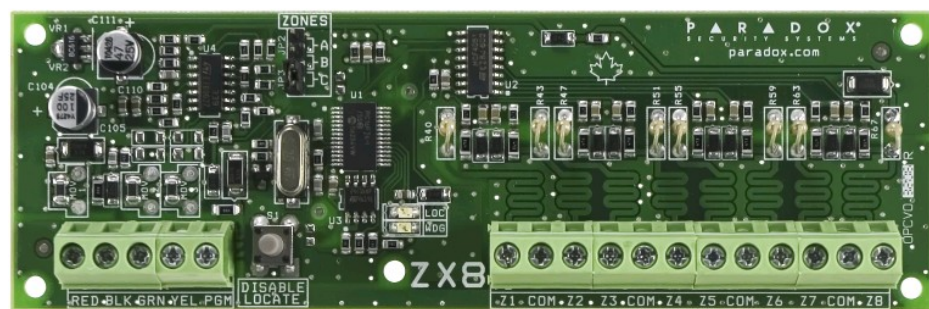
### 7.1.4 Zapojení ústředny



Obr. 17. Příklad zapojení ústředny [14]

## 7.2 Expandér ARP-ZX8

Pomocí tohoto sběrnicového modulu se může ústředna Digiplex Evo48 rozšířit o 8 drátových zón pro detektory a o jeden PGM.



Obr. 18. Základní deska expandéru ARP-ZX8 [15]

### 7.2.1 Vlastnosti modulu

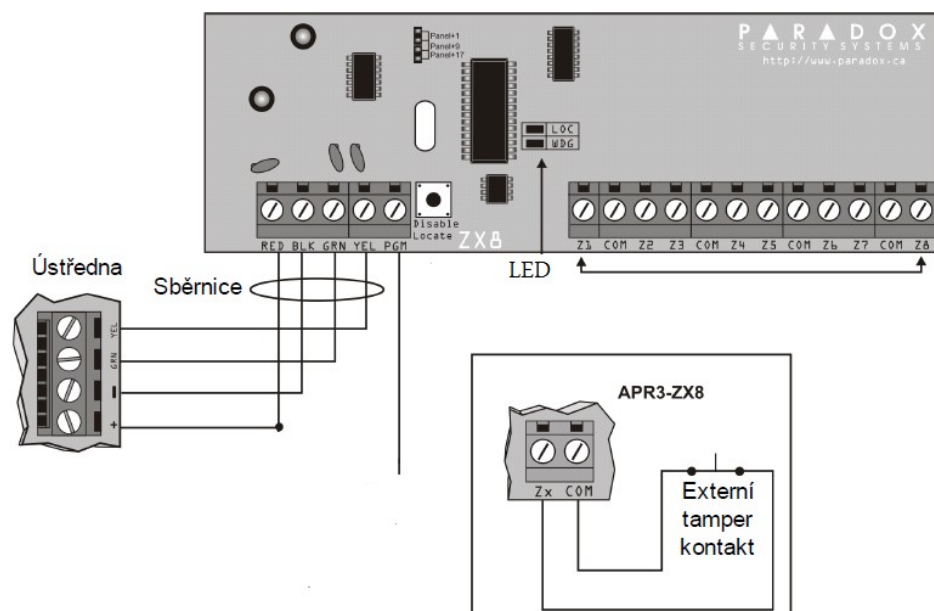
- Maximální počet 16 zón s využitím ATZ
- Plně programovatelné zóny
- Jeden programovatelný výstup PGM
- Pro modul určen BOX E
- Programování pomocí programu Winload nebo LCD klávesnice [15]

### 7.2.2 Technické parametry modulu

Tab. 16. Technické parametry modulu [15]

Napájení	9 - 16V DC
Proudový odběr	min 28 mA, max. 31 mA
Pracovní teplota	-10 až + 50 °C
Vlhkost	max. 95%
Typ zón	NC, s detekcí tamperu na smyčce
Rozměry	140x46mm
Vyhodnocení	digitální
Max. zatížení PGM výstupu	50 mA
Metody zpracování	Automatické pulsy, dvě úrovně, teplotní kompenzace
Optická indikace	Červená, Zelená dioda

### 7.2.3 Zapojení modulu



Obr. 19. Příklad zapojení modulu [16]

### 7.3 Bezdrátový modul MG-RTX3

Modul MG-RTX3 představuje bezdrátovou nástavbu od výrobce Magellan, která je kompatibilní i s ústředny výrobce Paradox. Využívá obousměrnou komunikaci s možností připojit prvky výrobce Magellan. Pracuje na frekvenci 868MHz a 433MHz. Tento modul dokáže rozšířit systém o 32 bezdrátových zón.



Obr. 20. Bezdrátový modul MG-RTX3 [17]

#### 7.3.1 Vlastnosti modulu

- Upgrade firmware
- Dohled baterie, tamperu a kontrolního intervalu vysílače
- Detekce rušení signálu, měření síly signálu
- Zobrazení síly signálu vysílače
- Vzdálené ovládání
- Aktualizace programového vybavení přes 306USB nebo Winload
- 3 PGM výstupy +1 volitelný
- Inteligentní komunikace s ústřednou po BUS sběrnici
- 1 modul MG-RTX3 = 32 bezdrátových zón a 32 klíčenek
- Počet modulů MG-RTX3 omezen pouze povoleným počtem modulů na BUS sběrnici [17]

### 7.3.2 Technické parametry modulu

Tab. 17. Technické parametry modulu [17]

Napájení	11-16V DC
Proudový odběr	Max. 50mA
Pracovní teplota	0 až + 50 °C
Vlhkost	max. 85%
Citlivost	12dBm
Přenos	technologie plovoucího kódu
Anténa	dipól
Rozměry	15 cm x 16 cm x 3 cm

### 7.3.3 Instalace

Při instalaci je nutno vybrat takové místo, kde nehrozí pohlcování a rušení radiových vln a v blízkosti se nenachází místo se silnými zdroji elektromagnetického rušení. Je proto nepřijatelné umístit přijímač na železný podklad nebo do plechové krabice. Jakékoliv silnější zdroje elektromagnetického pole nebo kovové předměty mezi modulem a vysílačem, snižují dosah. Modul se umísťuje tak, že vertikální anténa směřuje kolmo vzhůru a horizontální anténa je k vertikální kolmá.

## 7.4 Komunikační modul PCS200

Modul PCS200 umožňuje ústřednám Paradox bezdrátovou komunikaci a přenos systémových událostí prostřednictvím GPRS nebo GSM sítě. Modul PCS200 lze nakonfigurovat tak, aby posílal události koncovému uživateli prostřednictvím SMS a vzdáleně komunikoval se softwarem NEware a Winload přes GPRS. Pomocí GSM tak může být uživatel informován o poplachu v konkrétní zóně, zapnutí/vypnutí příp. o poruše systému. Modul se připojuje k ústředně pomocí datové sběrnice do maximální vzdálenosti dvou metrů. Anténu na modulu lze instalovat do vzdálenosti 18 metrů od modulu s využitím anténního prodloužení v závislosti na síle signálu.



Obr. 21. Komunikační modul PCS200

#### 7.4.1 Vlastnosti modulu

- Přenos událostí na PCO přes GPRS nebo přes GSM
- Posílání SMS zpráv na 16 telefonních čísel
- Typy SMS zpráv: poplach, zapnutí/vypnutí, porucha
- 1 SIM karta pro libovolný operátor
- Max. vzdálenost od ústředny po sériovém kabelu - 2m
- Max. vzdálenost od ústředny přes CVT485 - 300m
- České jazykové prostředí pro SMS zprávy
- Hliníkový box
- Konečný uživatel může zastřežit či odstřežit systému zasláním textové SMS zprávy na PCS200 - GSM režim
- Doplnující volitelné zařízení: Paradox Hlasový modul VDMP3, Anténa rozšíření, 12 Vdc externí napájecí zdroj [18]

#### 7.4.2 Technické parametry modulu

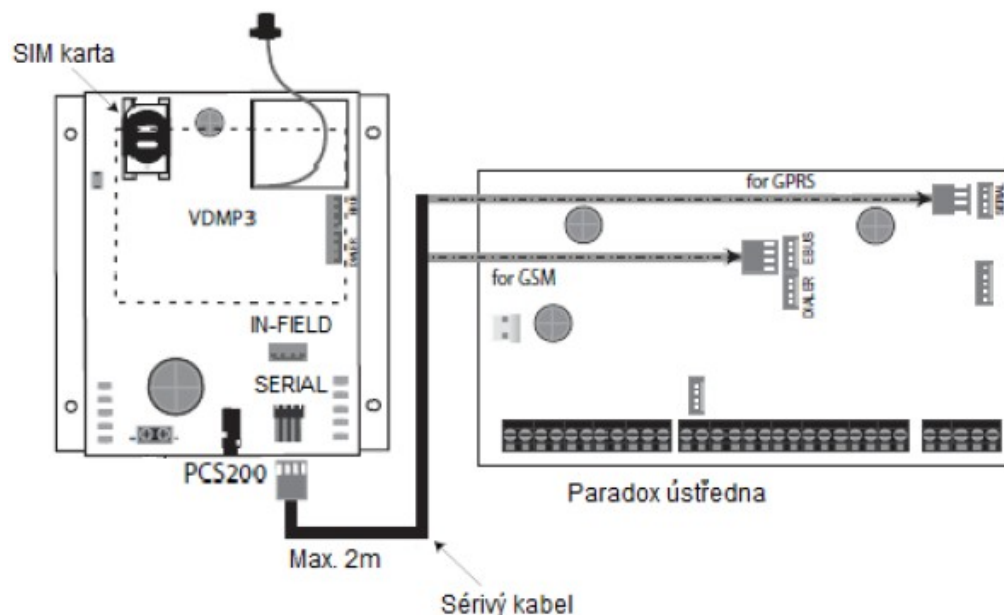
Tab. 18. Technické parametry modulu [18]

Napájení	9 - 16V DC
Proudový odběr	min 60mA, max. 600 mA při GPRS / GSM přenosu
Pracovní teplota	0 až + 50 °C
Šířka pásma	70 / 80 / 140 / 170 MHz, Automatická detekce



	pásma
Anténa	Zisk antény <3dBi, impedance 50 ohmů Příkon> špičkový výkon 2W
Výstupní výkon	Class 4 (2W) @ 850 / 900 MHz Class 2 (1W) @ 1800 / 1900 MHz
Rozměry	12,2 cm X 10,2 cm X 4,8 cm
Kódování	128-bit (MD5 a RC4) nebo 256-bit (AES)
SMS protokol	8-bit (IRA: ITU-T.50) nebo 16-bit (UCS2 ISO/IEC10646)
Metody zpracování	Automatické pulsy, dvě úrovně, teplotní kompenzace
Optická indikace	LED diody, GSM a GPRS komunikace, síla signálu, status Error

### 7.4.3 Zapojení modulu



Obr. 22. Zapojení modulu [19]

## 7.5 Venkovní siréna TEKNIM-720WR

Tato siréna je vybavena jak akustickou tak optickou signalizací. Siréna používá piezoměnič pro akustickou signalizaci a stroboskop pro optickou signalizaci. K zálohování je součástí dodávky Ni-MH akumulátor. Siréna má také vnitřní plechový kryt elektroniky, který zvyšuje odolnost pro případ mechanického poškození. Sirény je určena až pro čtvrtý stupeň zabezpečení a pro třídu prostředí IV.



Obr. 23. Siréna Teknim-720WR [20]

### 7.5.1 Technické parametry sirény

Tab. 19. Technické parametry sirény [20]

Napájení	9 – 16 V DC
Proudový odběr	450 mA
Akustický výkon	118 dB/m
Optická signalizace aktivace sirény	červený blikáč stroboskop 1Hz
Akustická signalizace	piezo siréna
Detekce napájení	2 červené LED diody
Tamper	detekce sejmutí ze zdi, otevření sirény
Venkovní krytí	IP 44
Rozměry	š 212 x v 300 x h 60 mm

## 7.6 Vnitřní siréna SA-913

Tato siréna také používá pro signalizaci piezoměnič, ale je na rozdíl od předešlé nezálohovaná a nemá optickou signalizaci.



Obr. 24. Siréna SA-913 [21]

### 7.6.1 Technické parametry sirény

Tab. 20. Technické parametry [21]

Napájení	11 – 14 V DC
Proudový odběr	120 mA
Akustický výkon	110 dB/m
Akustická signalizace	piezo siréna
Rozměry	š 74 x v 113 x h 46 mm

## 7.7 LCD klávesnice K641

Klávesnice Digiplex K641 umožňuje ovládací a programovací funkce, pomocí kterých lze programovat celý systém PZS. Základní charakteristikou je dvouřádkový modrý displej se 32 znaky, které zobrazují zprávy, zajišťují instrukce a oznamují stavy PZS. Na displeji lze nastavit osvětlení, kontrast, rychlost pohybu (přepínání jednotlivých zpráv) a také lze displej a zprávy přizpůsobit požadavkům zákazníka.



Obr. 25. LCD klávesnice K641 [22]

### 7.7.1 Vlastnosti klávesnice

- Zobrazování v češtině
- 14 jedno dotykových tlačítek
- 3 vestavěné panické poplachy
- Jedna zóna a jedno PGM
- Adresace klávesnice v systému- jedinečné číslo SN
- Firmware je uložen v EEPROM paměti
- Programování klávesnice: na klávesnici nebo pomocí programu WinLoad
- Tlačítka pro listování v menu
- Jedno klávesové zrychlené příkazy
- Uživatelské programování zvonkohry "CHIME" pro každou zónu
- Prohlížení historie událostí
- Možnost přiřazení jedné, nebo více skupinám [22]

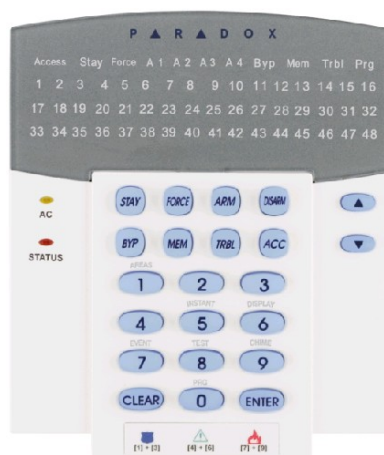
### 7.7.2 Technické parametry

Tab. 21. Technické parametry [22]

Napájení	9 - 16V DC
Proudový odběr	min 80mA, max. 120 mA
Pracovní teplota	0 až + 40 °C
Typ zóny na klávesnici	NC, bez hlídání tamperu
Programovatelný výstup PGM	max. zatížení 50 mA
Typy inkace	LED indikace stavu AC, READY
Rozměry	145x122x34 mm

## 7.8 LED klávesnice K648

Tato klávesnice se liší od předchozí hlavně tím, že pomocí ní nelze programovat PZS. Klávesnice zobrazuje 48 zón na přehledném panelu nad klávesami. Klávesnice se k ústředně připojuje jako předešlá, tedy na sběrnici. Je určena a certifikována pro 3. stupeň zabezpečení.



Obr. 26. LED klávesnice K648 [23]

### 7.8.1 Vlastnosti klávesnice

- 48 LED pro zobrazení zón ( každá LED může být přiřazena libovolné zóně )
- Adresace klávesnice v systému: jedinečné číslo SN
- Firmware je uložen v procesoru klávesnice
- jedna zóna a jedno PGM
- Uživatelské programování zvonkohry "CHIME" pro každou zónu
- 14 jedno dotykových tlačítek
- 3 vestavěné panické poplachy [23]

### 7.8.2 Technické parametry

Tab. 22. Technické parametry [23]

Napájení	9 - 16V DC
Proudový odběr	min 50mA, max. 110 mA
Pracovní teplota	0 až + 40 °C
Typ zóny na klávesnici	NC, bez hlídání tamperu
Programovatelný výstup PGM	max. zatížení 50 mA
Typy indikace	LED indikace stavu AC, READY a každého z podsystémů = ARM 1-4
Rozměry	145x122x34 mm

## 7.9 Paradox Pro 476

Jedná se standardní analogový pasivní infračervený detektor, který je určený pro montáž do rohu i na zeď. Je charakteristický vysokou odolností proti VF rušení a inteligentním vyhodnocováním signálu, kdy převádí každý pohybový signál na pulzní vstup, který určuje, zda detekovaná pohybová energie odpovídá poplachovému stavu. Zachycená energie se změří a uchová v paměti pro další zpracování, kdy procesor rozhoduje o typu přijaté energie a popř. zamítá nepohybové signály. Detektor je určen a certifikován pro 2. stupeň zabezpečení a splňuje požadavky pro 2. třídu prostředí.



Obr. 27. Paradox Pro 476 [24]

### 7.9.1 Vlastnosti detektoru

- Technologie automatického počítání pulsů
- Automatická teplotní kompenzace
- Kovový kryt pro odrušení VF polí
- Dvojnásobný prvek
- Čočka bez mrtvé zóny pod čidlem
- Ochranný kontakt
- Vysoká odolnost proti VF rušení
- Základní deska osazena pouze z přední kryté strany
- Vestavěné relé
- Dosah 11 x 11 m, úhel 110° [24]

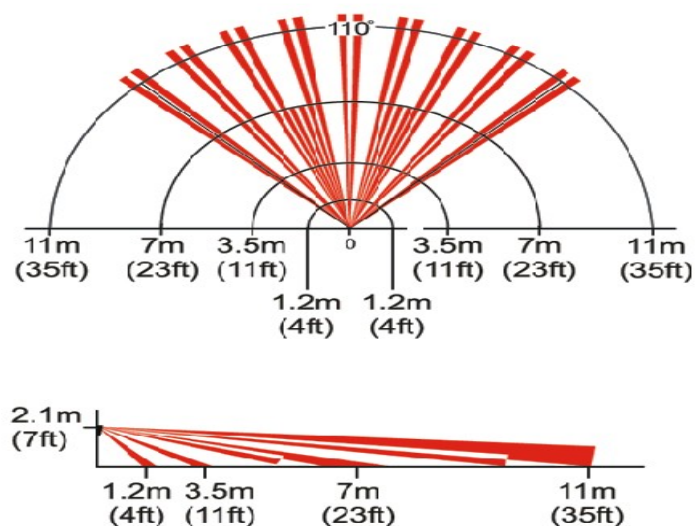
### 7.9.2 Technické parametry detektoru

Tab. 23. Technické parametry [24]

Napájení	9 - 16V DC
----------	------------

Proudový odběr	min 15mA, max. 27mA
Pracovní teplota	-10 až + 50 °C
Krytí	IP50
Vlhkost	max. 95%
Poplachové relé	28V DC, 150 mA
Tamper	28V DC, 150 mA
Vyhodnocení	analogové
Náběh	po připojení napětí 10 sec.
Senzor	Duální PIR
Detekční rychlost	0.2m - 7m/sec
Metody zpracování	Automatické pulsy, dvě úrovně, teplotní kompenzace
Optická indikace	Zelená dioda
Montážní výška	2,1 m až 2,7 m

### 7.9.3 Detekční charakteristika detektoru



Obr. 28. Detekční charakteristika [24]

#### 7.9.4 Instalace

Výška instalace detektoru je doporučena na 2,1m +/-10 procent. Při této výšce bude detektor poskytovat úplné pokrytí od 1,2m do 9,0m. Při instalaci je doporučeno vyhnout se v zorném poli následujícím objektům:

- Lesklé a průhledné stěny
- Ventilátory a horkovzdušná topení
- Předměty rychle měnící teplotu
- Chladničky
- Netěsnící okna, proud vzduchu
- Infračervené zdroje světla atd.

#### 7.10 Detektor tříštění skla GLASSTREK 457

Jedná se o akustický detektor tříštění skla, který se hodí pro detekci rozbití klasických skleněných tabulí, temperovaného nebo laminovaného skla. Při detekci využívá dvou frekvencí, typických pro rozbití výše uvedených skel a to nízkofrekvenční vlnu nárazu a vysokou frekvenci tříštění skla. Pokud pomocí mikroprocesorem řízeného programu, který analyzuje signál z vysoce citlivého nízko šumového mikrofону, nedojde k současnému vzniku uvedených frekvencí, nedojde na detektoru k vyhlášení poplachu. Detektor je určen a certifikován pro 3. stupeň zabezpečení a splňuje požadavky pro 2. třídu prostředí, tedy vnitřní-všeobecné.



Obr. 29. GLASSTREK 457 [25]

##### 7.10.1 Vlastnosti detektoru

- Analýza slyšitelného pásma a infrazvuku
- Nastavitelná citlivost pro vzdálenost od 4,5 do 9 m
- Dosah 9 metrů



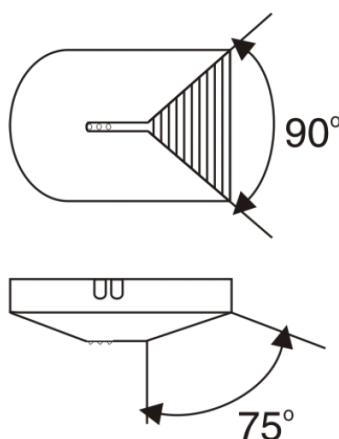
- Imunita proti VF rušení
- Ochranný kontakt [25]

### 7.10.2 Technické parametry detektoru

Tab. 24. Technické parametry [25]

Napájení	9- 16V DC
Proudový odběr	min 20mA, max. 37mA
Pracovní teplota	-10 až + 50 °C
Krytí	IP50
Vlhkost	max. 95%
Poplachové relé	28 V DC, 150 mA
Tamper	28 V DC, 150 mA
Senzor	citlivý mikrofon s nízkým šumem
Rozměry	90x67x25 mm

### 7.10.3 Detekční úhly detektoru



Obr. 30. Detekční úhly [25]

### 7.10.4 Instalace

Detektor má být instalován na pevné ploše bez otřesů a chvění a měl by být umístěn naproti chráněným plochám, přitom se musí brát v úvahu detekční úhel detektoru. Strana

detektoru nesmí být nijak zastíněná, aby měla přímý výhled na chráněnou plochu. Detektor se nedoporučuje používat pokud:

- Je chráněná skleněná plocha potažena bezpečnostní fólií
- Se nacházejí v blízkosti hlučné předměty jako zvonky ventilátory, kompresory a ostatní hlasité zařízení
- Jsou u oken jakkoliv izolované závěsy

### 7.11 Detektor tříštění skla Flex Gard FG1625TAS

Jedná se akustický duální detektor tříštění skla, který se používá pro detekci tříštění tabulového, tvrzeného, lepeného, drátovaného skla, skla s nalepenou bezpečnostní fólií a utěsněného vakuového skla. Ke zpracování signálů používá technologie Flex Core a Flex Guard. Flex Core představuje zpracování signálu v zákaznickém ASIC obvodu, který vyhodnocuje přijaté signály paralelně podle více parametrů. Tímto způsobem je dosaženo rychlejšího zpracování signálů než konvenčního postupného zpracování. Technologie Flex GuardR je citlivá na ultra nízké kmitočty, které jsou generovány při úderu do skleněné plochy. Kombinací těchto technologií má zajistit co nejvyšší odolnost proti falešným poplachům. Detektor je určen a certifikován pro 2. stupeň zabezpečení a splňuje požadavky pro 2. třídu prostředí.



Obr. 31. Flex Gard FG1625TAS [26]

#### 7.11.1 Vlastnosti detektoru

- Nastavitelná citlivost do čtyř úrovní
- Vícenásobné zpracování a analýza signálu
- Neomezená volba montážního místa
- Dosah 7,6m, úhel 360°
- Minimální rozměr chráněné skleněné plochy je 28 cm<sup>2</sup> [26]

### 7.11.2 Technické parametry detektoru

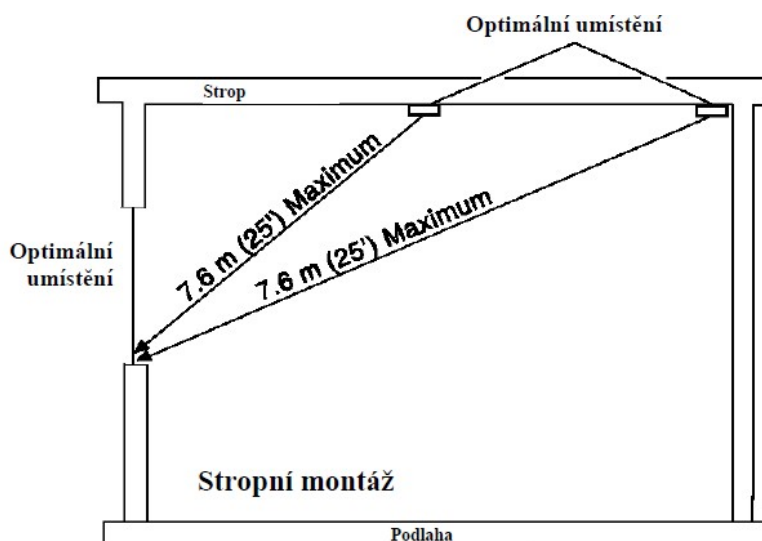
Tab. 25. Technické údaje [26]

Napájení	6 - 18V DC
Proudový odběr	min 12 mA, max. 22 mA
Pracovní teplota	-10 až + 50 °C
Krytí	IP50
Vlhkost	max. 95%
Poplachové relé	24V DC, 125 mA
Tamper	24V DC, 25 mA
Vyhodnocení	analogové
Senzor	akustický mikrofón
Metody zpracování	technologie Flex Core a Flex Guard

### 7.11.3 Instalace

Detektor je nejvhodnější umístit na zeď, která je proti chráněné skleněné ploše. Maximální vzdálenost od chráněné plochy nesmí přesáhnout 7,6 m a výška umístění detektoru by neměla být nižší než dva metry. Mezi detektorem a chráněnou plochou nesmějí být žádné překážky, aby byla zajištěna přímá viditelnost. Pokud jsou mezi detektorem a plochou závěsy, je nutné ověřit dosah detektoru testerem, ale doporučuje se instalovat detektor mezi závěs a chráněnou plochu. Detektor by se nedoporučuje umístit na:

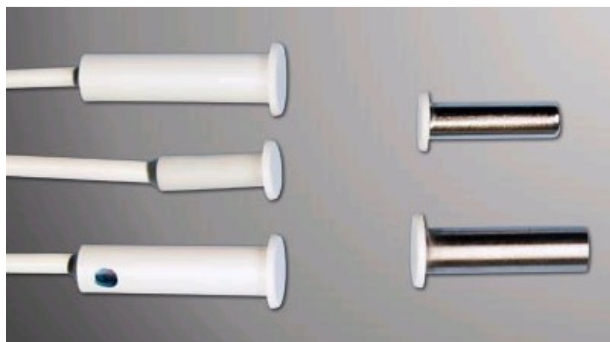
- stejnou zeď jako chráněná skleněná plocha
- na volně stojící sloupy / podpěry
- v hlučných místnostech, kde jsou například kompresory, elektrická zařízení atd., která jsou v činnosti, pokud je zabezpečovací systém ve střežení



Obr. 32. Optimální instalace detektoru [26]

## 7.12 Magnetický zápusťný kontakt MAS 333

Tento magnetický kontakt je určen pro použití v zabezpečovacích poplachových systémech jako čidlo otevření (dveří, oken apod.). K vyhlášení poplachu dojde při změně vzájemné polohy vlastního magnetického kontaktu a ovládacího magnetu. Tento typ je určen pro zápusťnou montáž. Poplach v ochranné smyčce je vyvolán při přerušení přívodního kabelu. Kontakt je určen a certifikován pro 2. stupeň zabezpečení.



Obr. 33 MAS 333 [27]

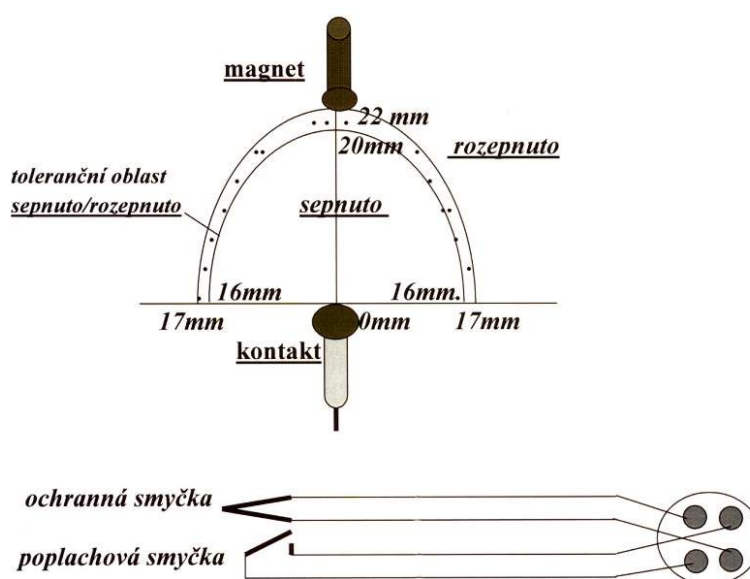
### 7.12.1 Technické parametry

Tab. 26. Technické parametry [27]

Odpor - stav sepnuto/rozepnuto	max. 2 ohm / min. 10 na devátou ohm
Pracovní teplota	-10 až + 50 °C
Krytí	IP 65

Vlhkost	max. 95%
Poplachové relé	max. 50V/ max. 250 mA
Tamper	max. 50V/ max. 250 mA
Rozměry	průměr 6 x 20mm, magnet průměr 6 x 22mm

### 7.12.2 Pracovní diagram



Obr. 34. Pracovní diagram detektoru [27]

### 7.12.3 Instalace

Magnetický kontakt a magnet musí být montován zápusným způsobem do otvoru průměru 6mm a je vhodné zajistit obě části vhodným tmelem či lepidlem podle materiálu, do kterého jsou zapuštěny. Pracovní vzdálenost mezi kontaktem a magnetem je v sepnutém stavu v rozmezí 0 až 22mm, záleží na vzájemné poloze a směru pohybu magnetu při otevření (axiálně, či radiálně). Kontakt ani magnet nesmí být zabudovány do feromagnetických materiálů. Přesto mohou být ovlivněny vlastnosti je-li v blízkosti feromagnetický materiál, zejména vzdálenosti sepnutí a rozepnutí - nutno vyzkoušet správnou funkci např. multimetrem.

### 7.13 Opticko-kouřový požární detektor VAR-TEC FDR-26-S

Detektor VAR-TEC FDR-26-S je určen jako doplňková signalizace k systémům PZS. Detekce kouře je založena na principu vniknutí kouře do vyhodnocovací komůrky, která je prosvětlována IR diodou a tento svit je zpětně vyhodnocován. Vlivem kouře se změny odrazové parametry v komůrce a detektor vyhodnotí poplach. Na přítomnost kouře teploty reaguje detektor svitem LED a překlopením relé. Kouř je detekován pouze v případě, že „zasáhne“ přímo detektor. K ukončení poplachu dojde až po „vyčištění“ detekčního prostoru v čidle od kouře. Detektor splňuje požadavky normy ČSN EN 54-7.



Obr. 35. VAR-TEC FDR-26-S [28]

#### 7.13.1 Technické parametry

Tab. 27. Technické parametry [28]

Napájení	10,5 -14V DC
Proudový odběr	klid 0,032 mA, poplach 55 mA
Pracovní teplota	-10 až + 50 °C
Krytí	IP42
Vlhkost	max. 95%
Výstup	NO/NC (továrně NO),relé max. 1A, 30V SS
Optická indikace	červená LED dioda
Detekční plocha	max. 40 m <sup>2</sup>
Montážní výška	max. 7 m

### 7.13.2 Instalace

Při instalaci detektoru je nutné dodržet několik zásad. Pokud je hlídaná místnost delší než 10m, použijte dva detektory. Nejvhodnější umístění je ve středu stropu, pokud to ale podmínky neumožňují tak minimálně 50 cm od rohu místnosti. Tyto podmínky jsou nutné pro správný zásah detektoru kouřem. Tento detektor instalujeme v takových podmínkách, kde se předpokládá v počátečním stadiu požáru vznik světlého kouře. Nelze ho použít v prostorech, kde při technologickém provozu vznikají zplodiny hoření nebo aerosoly světlé barvy. Pro typickou místnost s rovným stropem a instalační výškou 3m je hlídaná plocha na jeden opticko-kouřový hlásič max. 40m<sup>2</sup>. Při takto definovaném prostoru je maximální vzdálenost mezi hlásiči 8m. I přes to, že detekční plocha s rostoucí instalační výškou roste, doporučuje se i při větší instalační výšce počítat s max. 40m<sup>2</sup> na jeden detektor.

### 7.14 Detektor úniku plynu SD- ECG 983 N

Tento detektor detekuje únik zemního plynu a je vhodný do místností s plynovými kotli, kuchyní apod. Detektor ECG 983 N vyhodnocuje množství výbušného plynu v prostřední pomoci měření v ionizační komůrce a při výskytu uvedeného množství LEL vyhlásí poplach. Detektory jsou dodávány se samo-resetovací patičí, která zjednodušuje instalaci v systémech EZS. Po odeznění poplachového stavu na senzoru, přejde detektor automaticky do klidového stavu. Na přítomnost plynu reaguje detektor houkáním sirény, blikáním červené a zelené LED a překlopením relé. Plyn je detekován pouze v případě, že „zasáhne“ přímo detektor. Zkouška funkčnosti detektoru se může provádět přiložením magnetu (sepne relé, aktivace sirény) a fouknutím plynu ze zapalovače (sepne relé, aktivace sirény).



Obr. 36. SD- ECG 983 N [29]

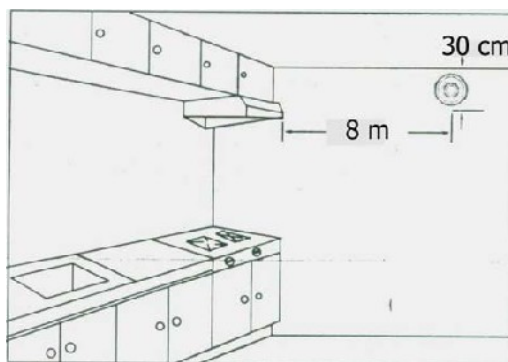
### 7.14.1 Technické parametry

Tab. 28. Technické parametry [29]

Napájení	10,5 - 16V DC
Proudový odběr	Max. 40 mA
Pracovní teplota	-10 až + 50 °C
Signalizace	Zelená LED – správná funkce detektoru Pulzně houká siréna + bliká střídavě zelená a červená LED – poplach
Vlhkost	max. 95%
Výstup	NO/NC relé max. 1A, 30mV DC
Vnitřní siréna	70dB

### 7.14.2 Instalace

Místo instalace odpovídá fyzikálním parametrům detekovaného plynu. Dále je potřeba si uvědomit, že na rozdíl od požárního detektoru není hlídán plošně celý prostor, ale je hlídán konkrétní zařízení (kotel, sporák, zásobník, přívod, atd.). V případě zemního plynu, umístíme detektor nad zařízení nejlépe ke stropu. Instalace maximálně 30 cm pod strop a maximálně 8m od hrany hlídaného zařízení.



Obr. 37. Instalace detektoru [28]



## 7.15 Detektor zaplavení a vlhkosti Menvier 1450

Detektor 1450 slouží k detekci zaplavení a vlhkosti a je určen pro vodivé neagresivní tekutiny. Detektor obsahuje interní detekční snímač a je vybaven výstupním přepínacím NO/NC kontaktem. Detektor má v každém rohu jeden detekční bod v podobě pozlacené tyčinky. K detekci zaplavení dojde tehdy, pokud kapalina spojí alespoň dva detekční body na kratší straně obdélníkového krytu detektoru. Citlivost se nastavuje trimrem na plošném spoji – ve směru hodinových ručiček větší citlivost (postačuje spojení dvou detekčních bodů), proti směru hodinových ručiček menší citlivost (musí dojít ke spojení detekčních bodů na obou stranách detektoru).



Obr. 38. Menvier 1450 [30]

### 7.15.1 Vlastnost detektoru

- Detekce zaplavení a vlhkosti
- Až 10 externích sond 1450S
- Vzdálenost externích sond až 60 m
- NO/NC reléový výstup
- Nastavitelná citlivost
- Připojení přes svorkovnici
- Kompaktní rozměry
- Detekční body [30]

### 7.15.2 Technické parametry

Tab. 29. Technické parametry [30]

Napájení	12- 24V DC
Proudový odběr	max. 30 mA

Pracovní teplota	-10 až + 50 °C
Krytí	IP40
Vlhkost	max. 95%
Výstup	NO/NC relé max. 1A, 30mV DC
Rozměry	96x64x31mm

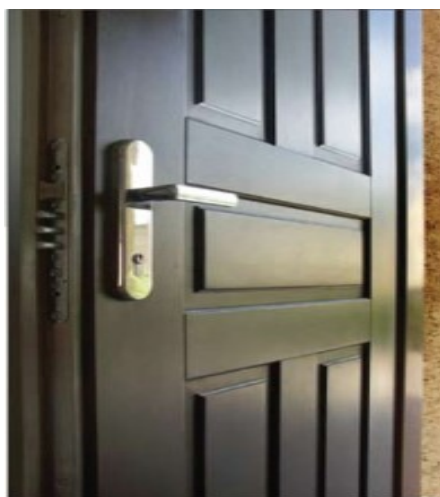
### 7.15.3 Instalace

Detektor se instaluje ve vodorovné poloze do místa, kde se požaduje detekovat přítomnost kapaliny nebo kondenzující vlhkosti. Jelikož detektor podporuje připojení externích sond, je také možné vlastní detektor umístit mimo zaplavovaný prostor a do tohoto prostoru instalovat přídavnou sondu. K detektoru může být připojeno paralelně až 10 externích sond typu 1450S s délkou stíněného kabelu max. 60 m. V případě použití telefonního kabelu může být maximální délka pouze 20 m. Sondy se připojují přes svorky označené písmenem S.

## 8 VÝBĚR A POPIS KOMPONENTŮ MECHANICKÝCH ZÁBRANNÝCH PROSTŘEDKŮ

### 8.1 Bezpečnostní dveře – Next SD 101

Tyto bezpečnostní dveře splňují požadavky třetí bezpečnostní třídy a jsou tvořeny tuhou ocelovou kostrou s rámem a žebrováním a jejich povrch je z vysokotlakého laminátu, dýhy či masivního dřeva. Tyto dveře jsou prodávány ve výrobní míře 197 x 90 cm, dají se ovšem na zakázku vyrobit i v požadované míře zákazníka. Dveře je možné dodat v různých variantách a odstínech barvy.



Obr. 39. Bezpečnostní dveře [31]

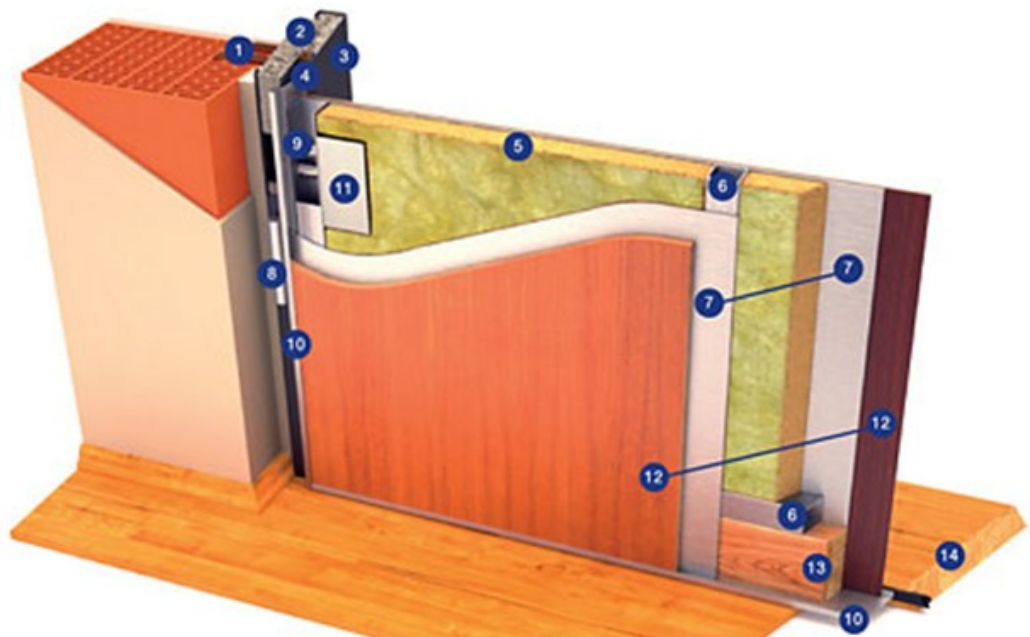
#### 8.1.1 Vlastnosti dveří

- 17 jisticích bodů
- Dvojité celoplošné pancéřování 1mm plechem
- Pancéřování zámku zesíleno speciálním plechem
- Bezpečnostní třída 3
- Tepelná izolace  $U = 1,3$
- Zvuková izolace 33-39 dB
- Odolnost proti zatížení větrem třída 1
- Otvírání dovnitř [31]

#### 8.1.2 Popis prvků dveří

1. ocelové kotvy
2. betonová výplň zárubně

3. bezpečnostní zárubeň
4. obložka zárubně s těsněním
5. zvuková a tepelná izolace
6. ocelový skelet
7. oboustranné pancéřování
8. bezpečnostní panty s ložiskem
9. dvojité zamykací body
10. nerezové hrany
11. automatické zamykací body
12. povrch dveří
13. dřevěný hranol umožňující
14. zkrácení dveří
15. práh s integrovaným těsněním [31]



Obr. 40. Popis prvků dveří [31]

### 8.1.3 Příslušenství k uvedeným dveřím

- Bezpečnostní zárubeň SF1 (100 mm)
- Bezpečnostní kování NEXT T1 (madlo + klika nebo klika + klika)
- Cylická bezpečnostní vložka EDZ GPI

Všechny prvky jsou v třetí bezpečnostní třídě.

## 8.2 Bezpečnostní mříže Next Typ B

Pro objekt budou postačující tyto pevné mříže, které jsou vyráběny dle požadavků zákazníka, co se týče designu a velikosti. Pro objekt jsou potřebné 3 bezpečnostní mříže o odlišných velikostech. Povrchová úprava těchto mříží se provádí buď pozinkováním, nebo práškovými barvami. Jsou vyráběny pro druhou a třetí bezpečnostní třídu. Velikost ok, konstrukce a výběr materiálu splňuje požadavky pojišťoven.



*Obr. 41. Bezpečnostní mříže Next Typ B [31]*

Rozměry mříží pro objekt (výška x šířka):

- 50 x 40 cm
- 100 x 60 cm
- 70 x 40 cm

## 9 POPIS A KONFIGURACE PZS

### 9.1 Popis a konfigurace systému

Celý PZS bude mít 30 zón a bude rozdělen do tří podsystemů:

- Podsystem 1 – byt
- Podsystem 2 – prodejna č. 1
- Podsystem 3 – prodejna č. 2

Ústředna bude umístěna v podsystemu 1 a bude napájena pomocí kabelu CYKY-J 3×1,5 (3Cx1,5). Kabel bude tažen z ústředny rovnou do rozvaděče na samostatný jistič. Tento jistič tak bude moci sloužit jako vypínač pro odpojení ústředny od elektrického napětí. Do ústředny budou připojeny 4 klávesnice pomocí sběrnice stejně jako 3 expandéry sloužící k rozšíření drátových zón. Detektory budou připojeny 6-žilovým kabelem jak do ústředny, tak do expandérů, kde každý expandér rozšiřuje systém o osm drátových zón. V systému se nacházejí tři expandéry.

Záložní akumulátor bude umístěn ve stejném boxu jako ústředna a v případě výpadku elektrické energie bude systému dodávat energii minimálně 12 hodin. Systém má dvě signalizační zařízení – venkovní a vnitřní sirénu. Venkovní siréna je umístěna v posledním patře tak, aby byla dobře vidět a měla odstrašující efekt. V případě narušení objektu nežádoucí osobou či v případě vzniku požáru bude tato siréna sloužit pro signalizaci (opticky i akusticky) uvedených stavů. Vnitřní siréna je umístěna uvnitř podsystemu 1 a její účel je především pro případy, vnitřního požáru, úniku vody či úniku plynu, ale také vloupání. Hlášení poplachu nebude jen lokální, ale bude také dálkové pomocí komunikačního modulu PCS200, který bude mimo jiné moci posílat majiteli a ostatním uživatelům objektu SMS zprávy o poplachu apod.

Co se týče konfigurace, bude pro ni použita LCD klávesnice K641, která mimo jiné slouží pro programování. Přístup do jednotlivých podsystemů bude dán přístupovou úrovní, kde majitel objektu bude mít přístupovou úroveň 3 (dle normy) a bude moci sám konfigurovat celý systém PZS pomocí LCD klávesnice. Podnájemníci budou mít přístupovou úroveň 2 a budou využívat LED klávesnici především pro nastavování stavu střežení a stavu klidu. Z tohoto důvodu je LCD klávesnice umístěna v části objektu 1. Následující text je rozdělen do tří částí, kde se každá část věnuje popisu a konfiguraci dílčího podsystemu.

### 9.1.1 Popis a konfigurace podsystému 1

Podsystém 1 zahrnuje 15 zón, které jsou připojeny jak k ústředně, tak k expandérům. Tento podsystém bude využívat režimu STAY, ve kterém bude vypnuta prostorová ochrana, aby se uživatelé mohli volně pohybovat po objektu a zároveň, aby byl objekt částečně střežen. Tuto část systému bude možno ovládat ze dvou klávesnic, přitom z jedné z nich se bude moci programovat celý systém PZS. Uvádění do stavu střežení a stavu klidu se bude provádět LED klávesnicí, která je umístěna v přízemí. Pro uvedení do stavu střežení se použije klávesa ARM, kdy následně uživateli bude indikováno odchodové zpoždění zelenou LED diodou na klávesnici a po ukončení klávesnice dlouze pískne. Odchodové zpoždění bude nastaveno na 15 s, přitom k ukončení odchodového zpoždění dojde v případě narušení a uklidnění zpožděné zóny 1. Uvedení do stavu střežení bude tedy započato uvnitř střeženého prostoru a ukončeno mimo něj.

Pro uvedení systému do stavu klidu bude zóna 1 naprogramovaná se zpožděním 20 s, aby uživatel během této doby stihl zadat na klávesnici svůj uživatelský kód a dokončil zadávání klávesou DISARM.

Skladba návrhu tohoto podsystému zahrnuje nejvíce detektorů PZS. Všechny tyto detektory jsou uvedeny v následující tabulce, která obsahuje zařazení jednotlivých detektorů do jednotlivých zón včetně popisu těchto zón.

Tab. 30. Konfigurace zón v podsystému 1

Název zóny	Typ zóny	Režim STAY	Název detektoru
Zóna 1	zpožděná, 30 s	VYPNUTO	MAS 333
Zóna 2	okamžitá	VYPNUTO	MAS 333
Zóna 3	okamžitá	VYPNUTO	Flex Gard FG1625
Zóna 4	následně zpožděná, 30 s	ZAPNUTO	Paradox Pro 476
Zóna 5	okamžitá	VYPNUTO	MAS 333
Zóna 6	okamžitá	VYPNUTO	GLASSTREK 457
Zóna 7	okamžitá	ZAPNUTO	Paradox Pro 476
Zóna 8	okamžitá	ZAPNUTO	Paradox Pro 476
Zóna 9	okamžitá	VYPNUTO	MAS 333
Zóna 10	okamžitá	ZAPNUTO	Paradox Pro 476
Zóna 11	okamžitá	VYPNUTO	MAS 333
Zóna 12	24 hodinová plyn	VYPNUTO	SD- ECG 983 N
Zóna 13	24 hodinová voda	VYPNUTO	Menvier 1450
Zóna 14	24 hodinová požár	VYPNUTO	VAR-TEC FDR-26-S
Zóna 15	okamžitá	ZAPNUTO	Paradox Pro 476

### 9.1.2 Konfigurace podsystému 2

Podsystém 2 zahrnuje 8 zón, které jsou připojeny k expandéru ZX8. Podsystém se bude moci ovládat přes LED klávesnici čtyřmístným uživatelským kódem. Uvádění do stavu střežení a stavu klidu se bude provádět rovněž LED klávesnicí. Postup je obdobný jako u podsystému 1.

Pro uvedení do stavu střežení se použije klávesa ARM, kdy následně uživateli bude indikováno odchodové zpoždění zelenou LED diodou na klávesnici a po ukončení klávesnice dlouze pískne. Odchodové zpoždění bude nastaveno na 15 s, přitom k ukončení odchodového zpoždění dojde v případě narušení a uklidnění zpožděné zóny 1. Uvedení do stavu střežení bude tedy započato uvnitř střeženého prostoru a ukončeno mimo něj. Informace o narušení tohoto podsystému budou zaslány SMS zprávou majiteli objektu a uživateli této prodejny – tedy prodejny č. 1.

Tento podsystém zahrnuje detektory uvedené v následující tabulce včetně zařazení jednotlivých detektorů do jednotlivých zón a popisu těchto zón.

Tab. 31. Konfigurace zón v podsystému 2

Název zóny	Typ zóny	Název detektoru
Zóna 15	zpožděná, 30 s	MAS 333
Zóna 16	okamžitá	Flex Gard FG1625TAS
Zóna 17	následně zpožděná, 30 s	Paradox Pro 476
Zóna 18	okamžitá	MAS 333
Zóna 19	okamžitá	Paradox Pro 476
Zóna 20	okamžitá	MAS 333
Zóna 21	okamžitá	Paradox Pro 476
Zóna 22	24 hodinová požár	VAR-TEC FDR-26-S

### 9.1.3 Konfigurace podsystému 3

Podsystém 3 zahrnuje 7 zón, které jsou připojeny k expandéru ZX8. Podsystém se bude moci ovládat přes LED klávesnici čtyřmístným uživatelským kódem. Uvádění do stavu střežení a stavu klidu se bude provádět rovněž LED klávesnicí. Postup je obdobný jako u předešlých podsystémů. Informace o narušení tohoto podsystému budou jako předchozím případem zaslány SMS zprávou majiteli objektu a uživateli této prodejny – tedy prodejny č. 2. Následující tabulka stejně jako předchozí, uvádí detektory v podsystému 3 včetně zařazení jednotlivých detektorů do jednotlivých zón a popisu těchto zón.



Tab. 32. Konfigurace zón v podsystému 3

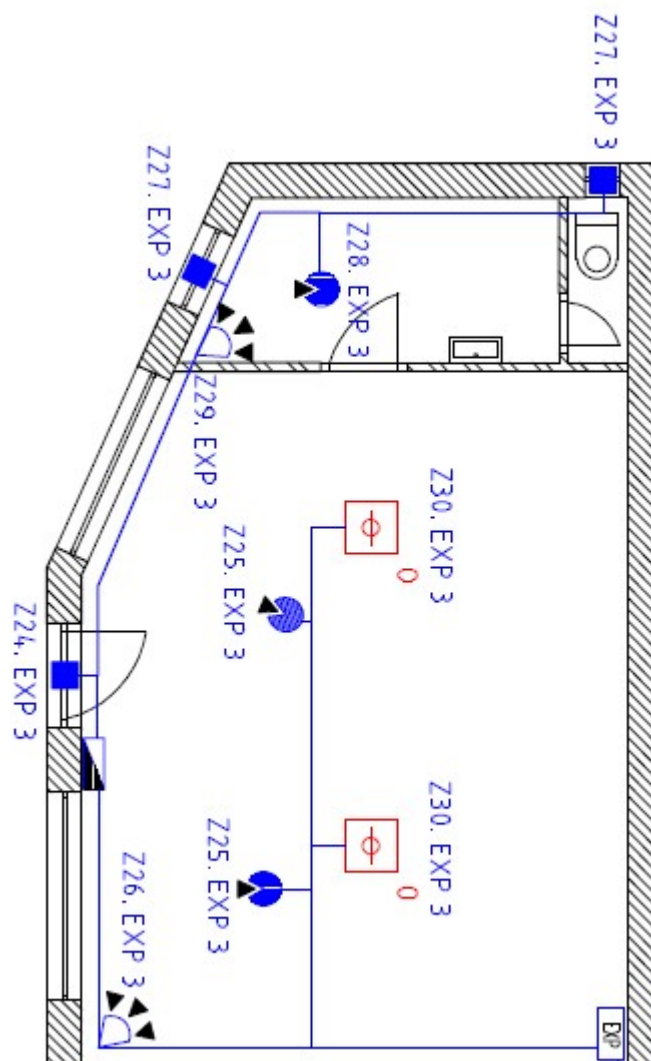
Název zóny	Typ zóny	Název detektoru
Zóna 23	okamžitá	MAS 333
Zóna 24	zpožděná, 30 s	MAS 333
Zóna 25	okamžitá	Flex Gard FG1625
Zóna 26	následně zpožděná, 30 s	Paradox Pro 476
Zóna 27	okamžitá	MAS 333
Zóna 28	okamžitá	GLASSTREK 457
Zóna 29	okamžitá	Paradox Pro 476
Zóna 30	okamžitá	VAR-TEC FDR-26-S

#### 9.1.4 Další bezpečnostní a režimová opatření v objektu

- Vždy před spaním provést kontrolu zajištění oken a dveří
- Kontrolovat návštěvníky před otevřením dveří kukátkem, domácím telefonem apod.
- Není-li přehled o užívání všech domovních klíčů, raději vyměnit zámek
- Učit děti kdy a jak co nejrychleji přivolat pomoc policie nebo sousedů
- Neříkat dětem důležité detaily o vaší finanční situaci, aktivitách apod.
- Vnímavost ke sporům nebo výhrůzkám, informovat o tom ostatní členy rodiny, případně i policii
- informovat někoho spolehlivého z našeho okolí při opuštění domu na několik dnů, zabezpečit pravidelný výběr pošty, novin, apod.
- Povolit vstup opravářů nebo jiných osob až po prověření jejich totožnosti nebo pověření od zaměstnavatele [33]

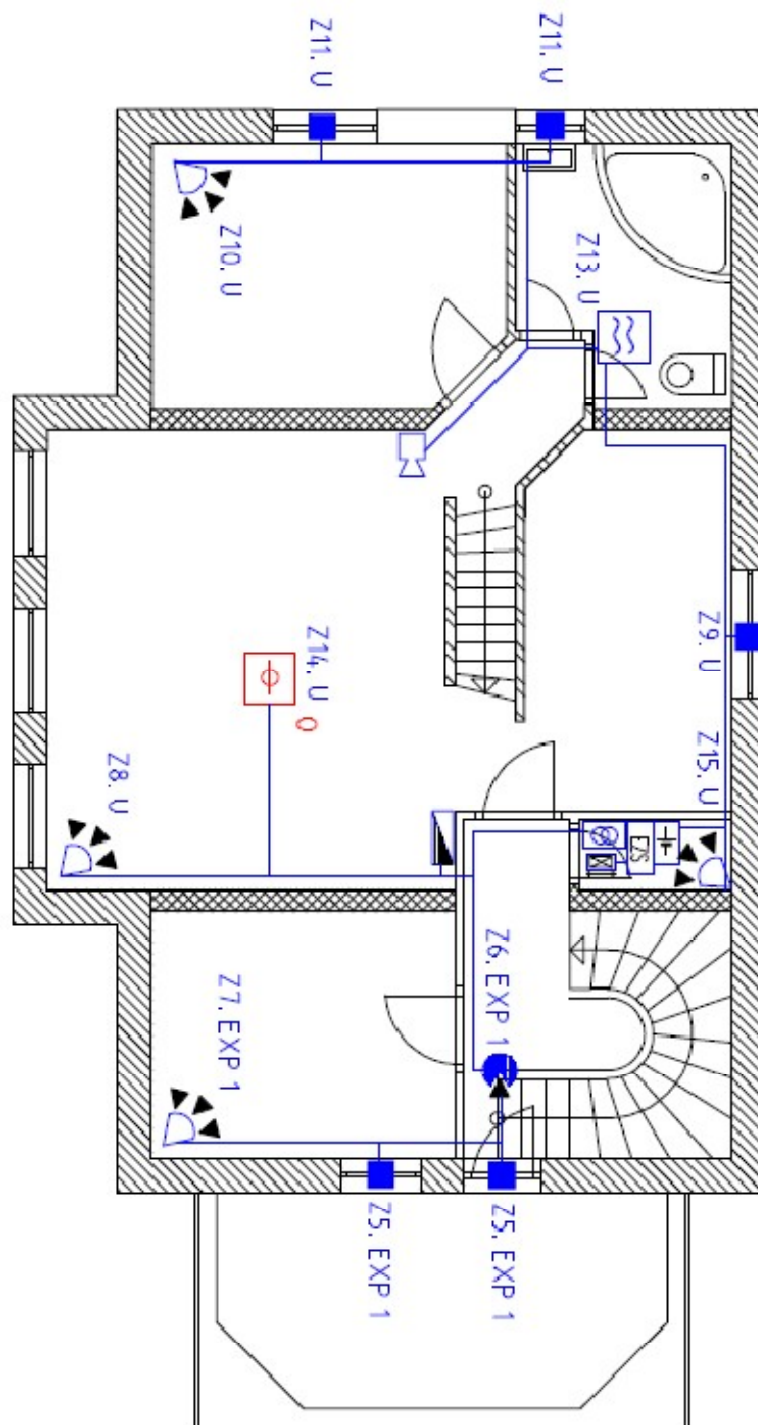
## 9.2 Dokumentace PZS – návrh rozmístění komponentů

Dokumentace je zhotovena v měřítku 1:100 a obsahuje rozmístění prvků PZS v celém objektu doplněných o kabelové trasy pro sdělovací vedení a je rozdělena do čtyř obrázků (výkresů) dle rozdělení podsystémů. U každého prvku je popis s číslem zóny (např. Z30), ve které je zapojen a také to zda je detektor připojen přímo do ústředny (např. Z15. U) nebo do expandéru (např. Z27. EXP3) a jeho číslo v ústředně.

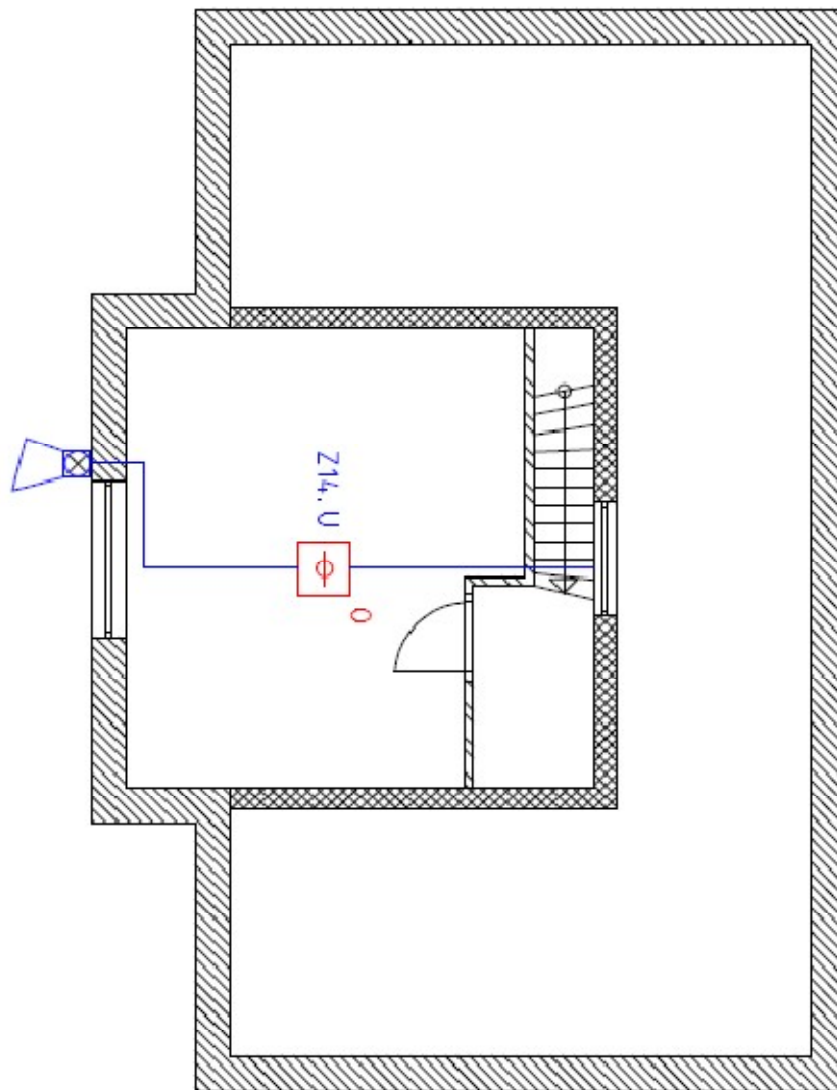


Obr. 42. Podsystem 3 – přízemí





Obr. 44. Podsystem 1 – 1. Patro



Obr. 45. Podsystem 2 – druhé patro

## 10 ROZPOČET ZABEZPEČENÍ

### 1. Pro PZS

Tab. 33. Celková cena za komponenty PZS

Typ komponentu	Název	Počet kusů	Cena za kus (v Kč)	Cena celkem (v Kč)
Ústředna	Digiplex Evo48	1	3220	3220
Expandér	ARP-ZX8	3	1443	4329
Komunikační modul	PCS200	1	5890	5890
Venkovní siréna	TEKNIM-720WR	1	1211	1211
Vnitřní siréna	SA-913	1	275	275
LCD klávesnice	K641	1	3379	3379
LED klávesnice K648	K648	2	2794	5588
Detektor	Paradox Pro 476	10	289	2890
Detektor tříštění skla	GLASSTREK 457	2	653	1306
Detektor tříštění skla	Flex Gard FG1625TAS	4	850	3400
Magnetický zápusťný kontakt	MAS 333	18	194	3492
Opticko-kouřový požární detektor	VAR-TEC FDR-26-S	6	852	5112
Detektor úniku plynu	SD- ECG 983 N	1	830	830
Detektor zaplavení a vlhkosti	Menvier 1450	1	950	950
Box na ústřednu	ESPRIT BOX D	1	761	761
Box pro expandéry	BOX E	2	520	1040
Záložní akumulátor	Akumulátor BASIC 12V/18Ah	1	847	847
6 - žilový kabel	Ka6x - 2x0.6+4x0.4	250	15	3750
Sběrníkový kabel	UTP CAT3 2P Cu, 2x2x0.5	120	7	840
Celkem				49110

Výsledná cena PZS bez instalačních a projekčních prací je do 50 000 Kč. V případě rozšíření systému o bezdrátový modul MG-RTX3 by se cena zvýšila o 2200Kč.

## 2. Pro MZS

Tab. 34. Celková cena za komponenty MZS

Typ komponentu	Název	Počet kusů	Cena (v Kč)
Bezpečnostní dveře	Next SD 101	1	13700
Bezpečnostní zárubeň	SF1	1	2 970
Bezpečnostní kování	NEXT T1	1	1120
Cylindrická bezpečnostní vložka	EDZ GPI	1	608
Bezpečnostní mříže Next Typ A	50 x 40 cm	1	1800
	100 x 60 cm	1	1800
	70 x 40 cm	2	3600
Celkem			25598

## ZÁVĚR

Předmětem této diplomové práce bylo navrhnout zabezpečení daného objektu. Aby vůbec mohlo k tomuto návrhu dojít, muselo se provést bezpečnostní posouzení, částečně i bezpečnostní analýza, které daly odpovědi na to, jaká rizika objektu či majetku uvnitř objektu hrozí, jaká jsou slabá místa objektu a také jaká jsou stávající bezpečnostní opatření. Záleželo také na hodnotě majetku a jeho atraktivnosti pro pachatele. Na základě těchto aspektů bylo navrženo další mnohem rozsáhlejší zabezpečení, které zahrnuje poplachové zabezpečovací systémy a mechanické zábranné prostředky. Tyto komponenty jsou popsány tak, aby bylo zřejmé, na jakém principu fungují, jaké mají technické parametry, detekční charakteristiky a případně jak se mají instalovat. V případě poplachových zabezpečovacích systémů odpovídají komponenty druhému stupni zabezpečení a výše. Součástí návrhu je také konfigurace systému, které je rozdělena dle rozdělení subsystémů, do kterých byl objekt rozdělen hned ze začátku praktické části. Návrh je doplněn také režimovými opatřeními, popisují zásady, které by měli uživatelé objektu dodržovat. Jako grafická dokumentace jsou zvoleny výkresy zpracované v programu Autocad, ve kterých je rozmístění jednotlivých komponentů zabezpečení, včetně kabelových tras. Závěrem práce je uveden přehled cen jednotlivých komponentů zabezpečení, aby měl čtenář představu, kolik takové zabezpečení stojí bez provedení instalačních a projekčních prací.

Návrh zabezpečení odpovídá uvedeným normám v kapitole Stanovení legislativních požadavků, a obsahuje i některé komponenty, které sice norma nevyžaduje, ale pro účel ochrany objektu jsou tyto komponenty na místě. Na práci bude jistě znát absence praxe v oboru, ale na druhou stranu by měl návrh odpovídat souvisejícím normám a poznatkům ze studia.



## CONSLUSION

The subject of this thesis was design the security of the building. To enable a suggestion proposal, had to perform security assessments, security analysis, partly to give answers on the risks of an object or property within the house risk, what are the weak points of object and what are the existing security measures. Depended on the value of the property and its attractiveness to offenders. Based on these aspects has been proposed much more extensive security that includes security alarm systems and mechanical barriers. These components are described as to show the principle on which they operate, what their technical parameters, detector characteristics and possibly how to install. In case of a security alarm system components corresponding to the second security level and above. The proposal is a system configuration, which is divided by sub-division in which the object was broken early in the practical part. The proposal is also complemented by lifestyle changes, describe the principle that users should observe the object. As a graphic file is selected drawings prepared in AutoCAD, which is the deployment of security components, including cable routes. Finally, work is a summary of the individual components of security to the reader an idea of the cost of such security without making the installation and design work.

Designing Security for equivalent standards is listed in Chapter provides legislative requirements, and includes some components that are standard, while not required, but for the purpose and object of protection of these components in place. The work will certainly know the lack of experience in the field, but on the other hand, the proposal should conform to related standards and knowledge of the study.

**SEZNAM POUŽITÉ LITERATURY**

- [1] ČANDÍK, Marek. *Objektová bezpečnost II*. Vyd. 1. Zlín : UTB ve Zlíně, 2004. 100 s. ISBN 80-7318-217-3.
- [2] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín : UTB ve Zlíně, 2007. 134 s. ISBN 978-80-7318-554-1.
- [3] Brex spol.s r.o. [online]. c2010 [cit. 2011-05-20]. OKNA? ...zaměřeno na bezpečnost!. Dostupné z WWW: <[http://www.brex.cz/profilplast/docs/bezpecnost\\_oken.pdf](http://www.brex.cz/profilplast/docs/bezpecnost_oken.pdf)>.
- [4] IVANKA, Ján. *Mechanické zábranné systémy*. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5.
- [5] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. Blatná : Blatenská tiskárna, 2006. 313 s. ISBN 80-902938-2-4.
- [6] IVNAKA, Ján; ČERNÝ, Josef. *Systematizace bezpečnostního průmyslu I*. Vyd. 2. Zlín : UTB ve Zlíně, 2006. 134 s. ISBN 80-7318-402-8.
- [7] *FAB ASSA ABLOY* [online]. c2005 [cit. 2011-05-18]. PYRAMIDA BEZPEČNOSTI. Dostupné z WWW: <<http://www.fab.cz/stranky/pyramida-bezpecnosti>>.
- [8] Česko. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. In Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2007, 13.310 - Ochrana proti zločinu, 40 s.
- [9] Materiály z přednášek z předmětu *Projektování bezpečnostních systémů*
- [10] Česko. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace*. In Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2011, 13.310 - Ochrana proti zločinu, s. 1-43.
- [11] Materiály z přednášek z předmětu *Projektování integrovaných systémů*

- [12] E-Pojistovna [online]. c2000 [cit. 2011-05-26]. Zabezpečení proti vloupání. Dostupné z WWW: <[http://www.e-pojistovna.cz/prod/noe\\_zabezpeceni.htm](http://www.e-pojistovna.cz/prod/noe_zabezpeceni.htm)>.
- [13] VARIANT plus specializovaný velkoobchod-elektronické systémy budov [online]. c2008 [cit. 2011-05-20]. Digiplex EVO48/2PGM. Dostupné z WWW: <<http://variant.cz/sekce28-evo48-2pgm.html?produkt=91>>.
- [14] Eurosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-26]. Instalační návod. Dostupné z WWW: <[http://www.eurosat.cz/UserFiles/Manual/Paradox/Digiplex/Ustredny/evo48\\_192\\_instal\\_v1\\_2.pdf](http://www.eurosat.cz/UserFiles/Manual/Paradox/Digiplex/Ustredny/evo48_192_instal_v1_2.pdf)>
- [15] VARIANT plus specializovaný velkoobchod-elektronické systémy budov [online]. c2008 [cit. 2011-05-20]. Expandéry . Dostupné z WWW: <<http://variant.cz/sekce57-zx8.html?produkt=161>>.
- [16] Eurosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-20]. Instalační návod. Dostupné z WWW: <[http://www.eurosat.cz/UserFiles/Manual/Paradox/Digiplex/Moduly/apr-zx8\\_rev10.pdf](http://www.eurosat.cz/UserFiles/Manual/Paradox/Digiplex/Moduly/apr-zx8_rev10.pdf)>.
- [17] Eurosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-20]. MG-RTX3 - bezdrátový modul. Dostupné z WWW: <<http://www.eurosat.cz/3311-mg-rtx3.html>>.
- [18] Eurosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-20]. PCS200 - GSM/GPRS komunikátor. Dostupné z WWW: <<http://www.eurosat.cz/4022-pcs200-gsm-gprs-komunikator.html>>.
- [19] Eurosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-26]. Instalační návod. Dostupné z WWW: <[http://www.eurosat.cz/UserFiles/Manual/Paradox/Prislusenstvi/pcs200\\_instal\\_navod.pdf](http://www.eurosat.cz/UserFiles/Manual/Paradox/Prislusenstvi/pcs200_instal_navod.pdf)>.

[20] VARIANT plus specializovaný velkoobchod-elektronické systémy budov [online]. 2010 [cit. 2011-05-26]. Venkovní sirény . Dostupné z WWW: <<http://variant.cz/sekce39-teknim-720wr.html?produkt=295>>.

[21] VARIANT plus specializovaný velkoobchod-elektronické systémy budov [online]. 2010 [cit. 2011-05-26]. Vnitřní sirény . Dostupné z WWW: <<http://variant.cz/sekce38-sa-913.html?produkt=292>>.

[22] Eurosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-26]. LCD klávesnice K641. Dostupné z WWW: <<http://www.eurosat.cz/217~K641-k641-dgp2-641bl.html>>.

[23] Eurosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-26]. Ovládací klávesnice K648. Dostupné z WWW: <<http://www.eurosat.cz/2004~K648-k648-dgp2-648bl.html>>.

[24] VARIANT plus specializovaný velkoobchod-elektronické systémy budov [online]. 2010 [cit. 2011-05-26]. Analogové PIR . Dostupné z WWW: <<http://variant.cz/sekce6-pro-plus-476.html?produkt=3>>.

[25] VARIANT plus specializovaný velkoobchod-elektronické systémy budov [online]. 2010 [cit. 2011-05-26]. 457 GLASSTREK. Dostupné z WWW: <<http://variant.cz/sekce10-457-glasstrek.html?produkt=537>>.

[26] Adi Global Distribution [online]. c2011 [cit. 2011-05-26]. GLASSBREAK FG-1625TAS. Dostupné z WWW: <[http://www.adiglobal.cz/iiWWW/en/produkty110.nsf/web\\_category\\_list1\\_cenik\\_as/c/346C34A634B38495C125735900628827](http://www.adiglobal.cz/iiWWW/en/produkty110.nsf/web_category_list1_cenik_as/c/346C34A634B38495C125735900628827)>.

[27] Magnetické kontakty [online]. 2010 [cit. 2011-05-26]. Asita spol.s ro. Dostupné z WWW: <[http://www.asita.cz/magneticke-kontakty\\_0-9.html?lang=cz](http://www.asita.cz/magneticke-kontakty_0-9.html?lang=cz)>.

[28] Seguro komunikační a bezpečnostní systémy [online]. c2011 [cit. 2011-05-26]. POŽÁRNÍ DETEKTORY VAR-TEC. Dostupné z WWW: <<http://www.seguro.cz/attachment/200906012030201636292946.pdf>>.

- [29] Eusosat specializovaný obchod na zabezpečovací technologie [online]. 2008 [cit. 2011-05-26]. Detektor plynu SD ECG-983. Dostupné z WWW: <<http://www.eurosat.cz/728/303~SD/ECG/983-detektor-plynu-sd-ecg-983.html>>.
- [30] Abbas Bezpečnostní systémy a slaboproudá zařízení [online]. 2008 [cit. 2011-03-12]. Menvier 1450. Dostupné z WWW: <<http://www.abbas.cz/produkty/Menvier-1450>>.
- [31] NEXT bezpečnostní dveře [online]. c2010 [cit. 2011-05-26]. Bezpečnostní dveře SD 101. Dostupné z WWW: <<http://www.next.cz/cs/produkty/pc-5-3-bezpecnostni-trida/pr-1-sd-101/>>.
- [32] NEXT bezpečnostní dveře [online]. c2010 [cit. 2011-05-26]. Pevné mříže. Dostupné z WWW: <<http://www.next.cz/cs/produkty/pc-3-bezpecnostni-mrize/pr-21-pevne-mrize/>>.
- [33] Stavíme dům [online]. c2009 [cit. 2011-05-26]. Zabezpečení rodinného domu. Dostupné z WWW: <<http://www.stavimedum.cz/guide.jsp?pg=zabezpeceni>>.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

EZS	Elektronický zabezpečovací systém.
PZS	Poplachový zabezpečovací systém.
PZST	Poplachové zabezpečovací a tísňové systémy.
MZS	Mechanické zábranné systémy.
I&HAS	Intruder and Hold-up Alarm Systém
IAS	Intruder Alarm Systém
HAS	Hold-up Alarm Systém
PCO	Pult centralizované ochrany
ČSN	Česká státní norma
EN	Evropská norma
TNI	Technická normalizační informace
GSM	Globální systém pro mobilní komunikaci
ČAP	Česká asociace pojišťoven
DC	Stejnoseměrný elektrický proud
AC	Střídavý elektrický proud
SMS	Krátká textová zpráva

## SEZNAM OBRÁZKŮ

<i>Obr. 1. Prostorové členění technické ochrany [2]</i> .....	17
<i>Obr. 2. Způsoby vloupání do rodinných domů [3]</i> .....	18
<i>Obr. 3. Způsoby vloupání do bytů v bytových domech [3]</i> .....	18
<i>Obr. 4. Pyramida bezpečnosti [7]</i> .....	22
<i>Obr. 5. Schéma PZS</i> .....	25
<i>Obr. 6. Možný způsoby předání poplachová informace</i> .....	30
<i>Obr. 7. Vývojový diagram činností při zřizování PZS [10]</i> .....	37
<i>Obr. 8. Bezpečnostní analýza jako součást bezpečnostní politiky</i> .....	40
<i>Obr. 9 Vazby v analýze rizik</i> .....	42
<i>Obr. 10. Příklad pojištění proti vloupání v závislosti na pojistné hodnotě [12]</i> .....	51
<i>Obr. 11. Pohled na přední stranu objektu</i> .....	57
<i>Obr. 12. Pohled na západní stranu objektu</i> .....	58
<i>Obr. 13. Rozdělení přízemí objektu</i> .....	58
<i>Obr. 14. Vstupní dveře do bytové části objektu</i> .....	63
<i>Obr. 15. Vstupní dveře do prodejny č. 1</i> .....	64
<i>Obr. 16. Ústředna Digiplex Evo48 [13]</i> .....	66
<i>Obr. 17. Příklad zapojení ústředny [14]</i> .....	68
<i>Obr. 18. Základní deska expandéru ARP-ZX8 [15]</i> .....	68
<i>Obr. 19. Příklad zapojení modulu [16]</i> .....	69
<i>Obr. 20. Bezdrátový modul MG-RTX3 [17]</i> .....	70
<i>Obr. 21. Komunikační modul PCS200</i> .....	72
<i>Obr. 22. Zapojení modulu [19]</i> .....	73
<i>Obr. 23. Siréna Teknim-720WR [20]</i> .....	74
<i>Obr. 24. Siréna SA-913 [21]</i> .....	75
<i>Obr. 25. LCD klávesnice K641 [22]</i> .....	75
<i>Obr. 26. LED klávesnice K648 [23]</i> .....	77
<i>Obr. 27. Paradox Pro 476 [24]</i> .....	78
<i>Obr. 28. Detekční charakteristika [24]</i> .....	79
<i>Obr. 29. GLASSTREK 457 [25]</i> .....	80
<i>Obr. 30. Detekční úhly [25]</i> .....	81
<i>Obr. 31. Flex Gard FGI625TAS [26]</i> .....	82
<i>Obr. 32. Optimální instalace detektoru [26]</i> .....	84

<i>Obr. 33. MAS 333 [27]</i> .....	84
<i>Obr. 34. Pracovní diagram detektoru [27]</i> .....	85
<i>Obr. 35. VAR-TEC FDR-26-S [28]</i> .....	86
<i>Obr. 36. SD- ECG 983 N [29]</i> .....	87
<i>Obr. 37. Instalace detektoru [28]</i> .....	88
<i>Obr. 38. Menvier 1450 [30]</i> .....	89
<i>Obr. 39. Bezpečnostní dveře [31]</i> .....	91
<i>Obr. 40. Popis prvků dveří [31]</i> .....	92
<i>Obr. 41. Bezpečnostní mříže Next Typ B [31]</i> .....	93
<i>Obr. 42. Podsystem 3 – přízemí</i> .....	98
<i>Obr. 43. Podsystem 2, částečně podsystem 1 – přízemí</i> .....	99
<i>Obr. 44. Podsystem 1 – 1. Patro</i> .....	100
<i>Obr. 45. Podsystem 2 – druhé patro</i> .....	101



**SEZNAM TABULEK**

Tab. 1. Bezpečnostní třídy o odporový čas otvorových výplní [6].....	21
Tab. 2. Stupně zabezpečení [8] .....	33
Tab. 3. Třídy prostředí [8] .....	33
Tab. 4. Komponenty na které se vztahuje detekce sabotáže [8].....	35
Tab. 5. Požadavky na detekci možných způsobů sabotáží [8].....	35
Tab. 6. Minimální doba napájení náhradním napájecím zdrojem [8] .....	36
Tab. 7. Doba nabíjení náhradního napájecího zdroje [8] .....	36
Tab. 8. Minimální rozsah střežení [10] .....	48
Tab. 9. Normy pro PZS .....	53
Tab. 10. TNI pro PZS .....	54
Tab. 11. Elektrotechnické normy .....	55
Tab. 12. Normy pro MZS .....	56
Tab. 13. Trestná činnost v obci Brumov-Bylnice .....	64
Tab. 14. Počet vloupání v obci Brumov-Bylnice dle typu objektu.....	65
Tab. 15. Technické parametry ústředny [13].....	67
Tab. 16. Technické parametry modulu [15] .....	69
Tab. 17. Technické parametry modulu [17] .....	71
Tab. 18. Technické parametry modulu [18] .....	72
Tab. 19. Technické parametry sirény [20].....	74
Tab. 20. Technické parametry [21] .....	75
Tab. 21. Technické parametry [22] .....	76
Tab. 22. Technické parametry [23] .....	77
Tab. 23. Technické parametry [24] .....	78
Tab. 24. Technické parametry [25] .....	81
Tab. 25. Technické údaje [26] .....	83
Tab. 26. Technické parametry [27] .....	84
Tab. 27. Technické parametry [28] .....	86
Tab. 28. Technické parametry [29] .....	88
Tab. 29. Technické parametry [30] .....	89
Tab. 30. Konfigurace zón v podsystému 1 .....	95
Tab. 31. Konfigurace zón v podsystému 2 .....	96
Tab. 32. Konfigurace zón v podsystému 3 .....	97

Tab. 33. Celková cena za komponenty PZS .....	102
Tab. 34. Celková cena za komponenty MZS .....	103