

Studie proveditelnosti inovace zabezpečovacího systému areálu firmy

Feasibility Study of The Innovation of a Firm's Plot Security System

Bc. Lucie Ambrožová



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lucie AMBROŽOVÁ**
Osobní číslo: **A10892**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Studie proveditelnosti inovace zabezpečovacího systému areálu firmy**

Zásady pro vypracování:

1. Zpracujte literární rešerši k tématu zabezpečovacího systému areálu firmy.
2. Analyzujte aspekty zajištění bezpečnosti provozu areálu.
3. Analyzujte stávající zabezpečovací systém.
4. Zpracujte studii proveditelnosti nového systému.
5. Analyzujte aspekty realizace nového systému a jejich zhodnocení technické, funkční i ekonomické.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

1. Sen Zekai: Solar Energy Fundamentals and modeling Techniques. London-Springer, 2008, ISBN -13:9781848001336.
2. Rybář P. a kol. Denní osvětlení a oslunění budov. Brno-ERA group spol.s r.o., 2002. ISBN 80-86517-33-0.
3. HRUŠKA, F. Projektování řídicích a informačních systémů. Učební texty. 1.vyd. Zlín: UTB ve Zlíně, 2010, s.175. ISBN 978-80-7318-979-2.
4. Křeček, S a kol.: Příručka zabezpečovací techniky / Stanislav Křeček a kolektiv. -- Vyd. 2., -- S.l. : Cricetus, 2003. -- 351 s. : il.; ISBN 80-902938-2-4.
5. Krejčířík A.: SMS : střežení a ovládání objektů pomocí mobilu a SMS : GSM pagery a alarmy : princip, použití, návody, příklady / Alexandr Krejčířík. -- 1. vyd.. -- Praha : BEN - technická literatura, 2004. -- 303 s. : il., ISBN 80-7300-082-2.
6. Schneider Electric CZ, I/NET Seven zabezpečovací a přístupový systém . Praha : Schneider Electric CZ, 2005.
7. Kindl, Jiří. Projektování bezpečnostních systémů : EPS, EZS. I.díl . Vyd.1. Zlín : Univerzita Tomáše Bati, 2004, 134 s. ISBN 80-7318-165-7.
8. Neil Comming. Security: A Guide to Security System Design and Equipment Selection and Installation, Second Edition. ISBN-10: 0750696249.

Vedoucí diplomové práce:

doc. Ing. František Hruška, Ph.D.

Ústav elektroniky a měření

Datum zadání diplomové práce:

24. února 2012

Termín odevzdání diplomové práce:

15. května 2012

Ve Zlíně dne 24. února 2012


prof. Ing. Vladimír Vašek, CSc.
děkan




doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá komplexním zabezpečením areálu firmy. V teoretické části jsou obecně popsány způsoby a možnosti zajištění bezpečnosti firmy. Cílem praktické části je analýza současného stavu zabezpečovacího systému firmy. Na základě zjištěných nedostatků s ohledem na požadavky investora je zpracována studie proveditelnosti inovace nového systému s využitím současných bezpečnostních prostředků dostupných na trhu. Následně jsou řešeny možnosti realizace nového systému z hlediska technického, funkčního i ekonomického.

Klíčová slova: poplachový zabezpečovací a tísňový systém, kamerový systém CCTV, přístupový systém ACS, PIR detektor, analýza, návrh, realizace

ABSTRACT

Diploma thesis deals with the comprehensive security company premises. The theoretical part generally described methods and possibilities of ensuring the safety of the company. Object of practical part is to analyze the current state of the security system company. On the basis of the identified shortcomings with regard to the requirements of the investor is a feasibility study of a new innovation system using current safety devices available on the market. Subsequently are solved the possibilities of realization of the new system in terms of technical, functional and economical.

Keywords: Intruder and hold-up alarm system, Closed Circuit Television CCTV, Access Control System ACS, PIR sensor, analysis, design, implementation

Ráda bych poděkovala vedoucímu diplomové práce doc. Ing. Františku Hruškovi, Ph.D za jeho vstřícný přístup, cenné rady a připomínky, které mi poskytl během zpracování diplomové práce. Dále chci poděkovat své rodině a zaměstnavateli za podporu během celého studia.

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

ÚVOD.....	10
I TEORETICKÁ ČÁST	11
1 ZABEZPEČOVACÍ SYSTÉM AREÁLU FIRMY	12
1.1 OCHRANA OBJEKTU	12
1.1.1 Mechanické prostředky ochrany.....	13
1.1.2 Technické prostředky ochrany.....	13
1.1.3 Fyzická ochrana.....	15
1.1.4 Režimová ochrana	15
1.1.5 Integrace bezpečnostních služeb	16
1.2 ZÁKLADNÍ SYSTÉMY TECHNICKÉ OCHRANY.....	16
1.2.1 Poplachový zabezpečovací a tísňový systém PZTS	16
1.2.1.1 Ústředna	16
1.2.1.2 Detektory (čidla, snímače apod.)	18
1.2.1.3 Signalizační zařízení	19
1.2.1.4 Napájecí zdroje	19
1.2.1.5 Ovládací zařízení	19
1.2.2 Kamerové bezpečnostní systémy CCTV	19
1.2.2.1 Kamera.....	20
1.2.2.2 Objektiv	21
1.2.2.3 Zařízení pro přenos a řízení videosignálu	22
1.2.2.4 Záznamové a zobrazovací zařízení	22
1.2.3 Systémy kontroly vstupů a docházkové systémy	24
1.2.4 Elektrická požární signalizace EPS.....	24
1.3 TECHNICKÁ OCHRANA OBJEKTU	25
1.3.1 Prvky obvodové ochrany	26
1.3.2 Prvky plášťové ochrany.....	27
1.3.3 Prvky prostorové ochrany.....	28
1.3.4 Prvky předmětové ochrany.....	29
1.3.5 Prvky tísňové ochrany	29
1.4 STUPEŇ ZABEZPEČENÍ.....	29
1.5 KLASIFIKACE PROSTŘEDÍ.....	30
1.6 TYP ZABEZPEČENÍ OBJEKTU.....	32
2 ZAJIŠTĚNÍ BEZPEČNOSTI PROVOZU AREÁLU.....	33

2.1	POSOUZENÍ LOKALITY OBJEKTU	33
2.2	POSOUZENÍ LOKALITY BUDOVY	33
2.3	VLIVY PŮSOBÍCÍ NA ZABEZPEČOVACÍ SYSTÉM A MAJÍCÍ PŮVOD UVNITŘ STŘEŽENÝCH OBJEKTŮ	34
2.4	VLIVY PŮSOBÍCÍ NA ZABEZPEČOVACÍ SYSTÉM A MAJÍCÍ PŮVOD VNĚ STŘEŽENÝCH OBJEKTŮ	35
2.5	KOMPLEXNOST OCHRANY PROVOZU AREÁLU	36
II	PRAKTICKÁ ČÁST	38
3	STÁVAJÍCÍ ZABEZPEČOVACÍ SYSTÉM	39
3.1	ZÁKLADNÍ PERIMETRICKÁ OCHRANA AREÁLU	39
3.2	POPLACHOVÝ ZABEZPEČOVACÍ SYSTÉM	39
3.2.1	Ústředna DIGIPLEX EVO192	40
3.2.1.1	Zhodnocení ústředny	41
3.2.2	Klávesnice Digiplex DGP2 - 641 BL	41
3.2.3	Magnetické kontakty SA-203	42
3.2.4	PIR detektor DG55	42
3.2.5	Kódovací systém	44
3.3	KAMEROVÝ SYSTÉM	46
3.4	PŘÍSTUPOVÝ A DOCHÁZKOVÝ SYSTÉM	46
3.5	ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE	48
3.5.1	Ústředna EPS	48
3.5.2	Automatický hlásič opticko-kouřový	49
3.5.3	Tlačítkový hlásič požáru	49
3.5.4	Kabelové rozvody a montáž zařízení	50
3.5.5	Shrnutí EPS	50
3.6	ZHODNOCENÍ STÁVAJÍCÍHO SYSTÉMU	50
3.6.1	Identifikované nedostatky	51
4	STUDIE PROVEDITELNOSTI NOVÉHO SYSTÉMU	53
4.1	ANALÝZA POŽADAVKŮ NA KOMPLEXNÍ BEZPEČNOSTNÍ SYSTÉM	53
4.2	PERIMETRICKÁ OCHRANA	53
4.2.1	Perimetr Locator	53
4.2.2	Maximum Guard	55
4.2.3	Vyhodnocení	56

4.3	SIGNALIZACE NEDOVOLENÉHO POHYBU, ČASTÉ POPLACHY	56
4.4	AKUSTICKÝ DETEKTOR TŘÍŠTĚNÍ SKLA	59
4.5	TÍSŇOVÝ HLÁSIČ K SIGNALIZACI NAPADENÍ OBSLUHY RECEPCE	61
4.6	VENKOVNÍ SIRÉNA.....	63
4.7	KAMEROVÝ SYSTÉM CCTV	66
4.8	KÓDOVACÍ SYSTÉM	69
4.9	SHRNUTÍ NOVĚ ZVOLENÝCH PRVKŮ PTZS.....	70
4.10	NÁVRH ŘEŠENÍ	70
5	ASPEKTY RELAIZACE NOVÉHO SYSTÉMU	72
5.1	PERIMETRLOCATOR.....	72
5.1.1	Technické a funkční zhodnocení.....	72
5.1.2	Ekonomické zhodnocení	72
5.2	KAMERY LG ELECTRONICS LT903PB	73
5.3	PIR DETEKTORY IR 120C	73
5.4	GLASSTREK 457, PARADOX PS-128, S 3040	73
5.5	INOVACE KÓDOVÁNÍ.....	74
5.6	SHRNUTÍ.....	74
	ZÁVĚR	75
	ZÁVĚR V ANGLIČTINĚ	76
	SEZNAM POUŽITÉ LITERATURY.....	77
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	80
	SEZNAM OBRÁZKŮ	82
	SEZNAM TABULEK.....	83
	SEZNAM PŘÍLOH.....	84

ÚVOD

V současnosti se vzrůstajícím počtem různých forem kriminality je zajištění ochrany života, zdraví, majetku osob určitou nutností. Co se týče komplexního zabezpečení objektu, musíme brát v úvahu nejen krádeže a neoprávněné vniknutí osoby do soukromého objektu, ale také např. požáry či jiné přírodní živly.

Dnešní moderní firmu si již neumíme představit bez bezpečnostního systému, jako jsou mechanické zábranné systémy MZS, poplachové, zabezpečovací a tísňové systémy PZTS doplněné o sledovací kamerové systémy CCTV, systémy kontroly vstupu ACCESS s návazností na docházkové systémy a v neposlední řadě pak elektrické požární signalizace EPS. Veškeré bezpečnostní systémy musí být projektovány dle právních předpisů a platných norem ČSN.

Cílem diplomové práce je návrh inovace nového zabezpečení firmy. Její nové sídlo bylo postaveno v roce 2007. Budova je poměrně nová, moderní s již existujícím zabezpečovacím systémem. Mým úkolem je po 5 letech provozu objektu zanalyzovat stávající stav komplexního zabezpečení firmy, poukázat na možné nedostatky a navrhnout řešení s ohledem na efektivnost a ekonomický přínos.

V první části diplomové práce jsou pospaná obecná hlediska, technické prvky a legislativa potřebná k zabezpečení firmy. Na základě těchto aspektů je následně zpracovaná analýza stávajícího bezpečnostního systému z pohledu ochrany obvodové, plášťové, prostorové a tísňové. Je poukázáno na silné a slabé stránky tohoto systému. S ohledem na připomínky investora je vypracovaný nový návrh zabezpečení s využitím vhodných stávajících komponentů, aby byla co nejméně zatížená ekonomická stránka investora. V poslední části diplomové práce je rámcově rozpracovaná implementace nového bezpečnostního systému s následným zhodnocením z hlediska funkčního, technického i ekonomického.

I. TEORETICKÁ ČÁST

1 ZABEZPEČOVACÍ SYSTÉM AREÁLU FIRMY

Cílem zabezpečovacího systému je ochrana života a zdraví osob, ochrana majetku a informací. K návrhu komplexního zabezpečovacího systému musíme znát předmět ochrany - co chceme chránit a cíl ochrany - proti čemu chceme chránit. V kapitole 1 se obecně seznámíme s prostředky pro zajištění ochrany firmy, které jsou v diplomové práci dále využity. [1]

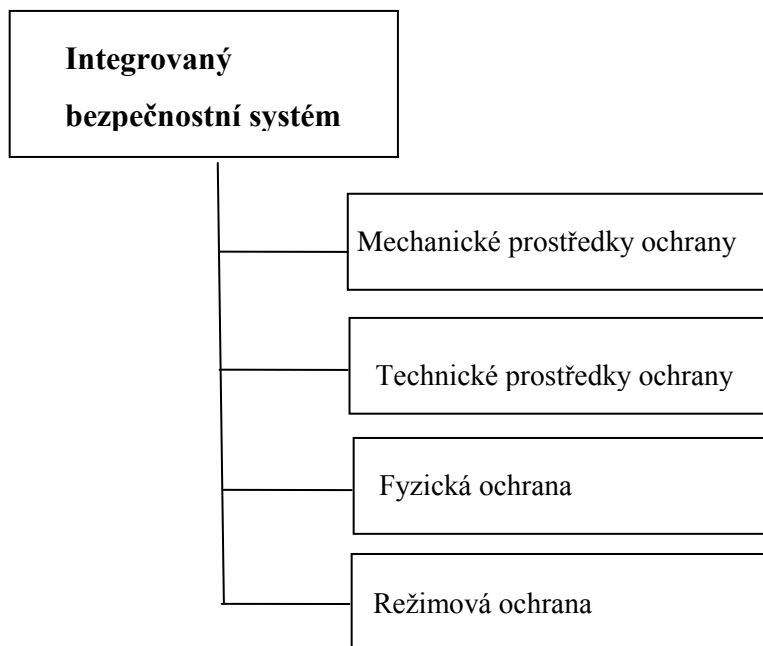
1.1 Ochrana objektu

Obecně si pod pojmem ochrana pro daný subjekt představujeme zabezpečené prostředí sladěním všech dostupných prostředků zajišťujících požadovanou nebo definovanou bezpečnost. [2]

Mezi základní prostředky ochrany objektu patří [3]:

- Klasická ochrana - mechanické zábranné systémy (zámky, mříže, závory)
- Technická ochrana - poplachové systémy (detektory, tísňové hlásiče)
- Fyzická ochrana (ostraha)
- Režimová ochrana (kontrola vstupů)

Nejúčinnější ochranou je kombinace výše uvedených typů. Mluvíme o integrovaném bezpečnostním systému, jehož výstupem je obraz situace, technologií a činností.



Obr. č. 1 Integrovaný bezpečnostní systém

1.1.1 Mechanické prostředky ochrany

Jedná se zejména o prostředky ohraničení vstupních prostor. Mluvíme o mechanických zábranných systémech (MZS), jež tvoří překážku pro pachatele vnikajícího do chráněného objektu. Důležitou roli hraje časový interval potřebný k překonání zábran.

$$\Delta t = t_2 - t_1 \quad [s]$$

kde t_1 určuje čas počátku napadení a t_2 dokončení napadení objektu. [2]

Jelikož jde o rozsáhlou oblast bezpečnostních zajištění, dělíme MZS do tří skupin: [3]

- **MZS obvodové ochrany** - zdi, oplocení, průchozí prvky zdí a plotů, vrcholová ochrana, podhrabové překážky, vstupy, vjezdy
- **MZS plášťové ochrany** - stavební prvky budov, otvorové výplně (dveře, okna, mříže)
- **MZS předmětové ochrany** - komerční úschovné objekty, trezory

1.1.2 Technické prostředky ochrany

Patří mezi základní bezpečnostní opatření objektu, jejichž cílem je odradit pachatele od jeho činu, případně jeho činnost ztížit a prodloužit dobu přístupu k chráněným aktivům. Sama o sobě tedy není ochranou, lze ji spíše charakterizovat jako detekční systém

předávající informace o stavu střeženého objektu a jeho případném napadení. Technické prostředky slouží také jako podpora režimových opatření a zkvalitnění činnosti fyzické ostrahy. [4]

Mezi technické prostředky ochrany řadíme:

- Poplachové zabezpečovací a tísňové systémy - PZTS
- Elektrická požární signalizace - EPS
- Kamerové systémy - CCTV
- Přenosová zařízení
- Ústředny
- Poplachová a přijímací centra - PPC

Kombinací technických prostředků se vytváří tzv. vícestupňová ochrana. Integrovaný celek je složený z různých technických prvků, jež jsou vzájemně propojeny (Uhlář)např. (přístupový systém ACS, poplachový zabezpečovací a tísňové systémy - PZTS, kamerové CCTV, protipožární signalizaci EPS, technické systémy budov jako klimatizace HVAC, osvětlení) a mnohé další. [5]



Obr. č. 2 Ukázka techniky integrovaného bezpečnostního systému

Zdroj: <http://www.aztech4security.com/images> [6]

Všechny poplachové systémy musí splňovat všeobecné požadavky na poplachové systémy. Ty jsou dány skupinou norem rady ČSN EN 5013x.

Tabulka 1 Seznam kategorií norem poplachových systémů [5]

Číslo normy (kategorie)	Název normy	Zkratka
ČSN EN 50 130 - x - y	Poplachové systémy	-----
ČSN EN 50 131 - x - y	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy	PZTS
ČSN EN 50 132 - x - y	Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích	CCTV
ČSN EN 50 133 - x - y	Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích	ACS
ČSN EN 50 134 - x - y	Poplachové systémy - Systémy přivolání pomoci	SAS
ČSN EN 50 135 - x - y	Obsaženo v: ČSN EN 50 131	-----
ČSN EN 50 136 - x - y	Poplachové systémy - Poplachové přenosové systémy a zařízení	ATS
ČSN EN 50 137 - x - y	Nahrazeno: ČSN CLC/TS 50 398	-----

Všeobecné požadavky na kombinované a integrované poplachové systémy jsou popsány normou ČSN CLC/TS 50398

Kapitola technických prostředků je velmi rozsáhlá a pro tuto diplomovou práci velmi důležitá, bude jí proto věnována zvlášť kapitola 1.2

1.1.3 Fyzická ochrana

Jedná se o nejstarší, nejefektivnější formu ochrany prováděnou živou silou. Cílem je ochrana objektů a jejich zařízení, ochrana osob pracujících v objektech, ochrana dodržování režimu v daném objektu. [7]

Největší výhodou je možnost okamžitého zásahu v případě ohrožení. Nevýhodou FO jsou poměrně vysoké režijní náklady. [1]

1.1.4 Režimová ochrana

Je souborem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro smysluplnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu. Dělíme na [1]:

- vnější režimová opatření - týkají se především vstupů a výstupů do objektu

- vnitřní režimová opatření - omezení pohybu osob a vozidel do vymezených částí prostor

1.1.5 Integrace bezpečnostních služeb

Cílem integrace výše uvedených bezpečnostních služeb je celek tvořený z různých mechanických a technických prvků PZS, EPS, ACS, CCTV v kombinaci s fyzickou ostrahou za účelem snížení počtu pracovníků fyzické ochrany, čímž se zvyšuje komfort a konstantní stabilita ochrany majetku zákazníka.

Významné uplatnění integrace bezpečnostních systémů máme zejména u velkých komerčních objektů, jejichž přínosem je univerzálnost, flexibilita, úspora energií, efektivní využití centrálního ovládání a monitorování. [5].

1.2 Základní systémy technické ochrany

Moderní zabezpečovací systém pro ochranu objektů je obvykle sestavený z různých subsystémů, které musí vedle sebe nějakým způsobem koexistovat a také vzájemně kooperovat. V této kapitole se seznámíme s dílčími subsystémy zabezpečovacího systému, zejména potom s prvky PZTS, CCTV, ACS a EPS.

1.2.1 Poplachový zabezpečovací a tísňový systém PZTS

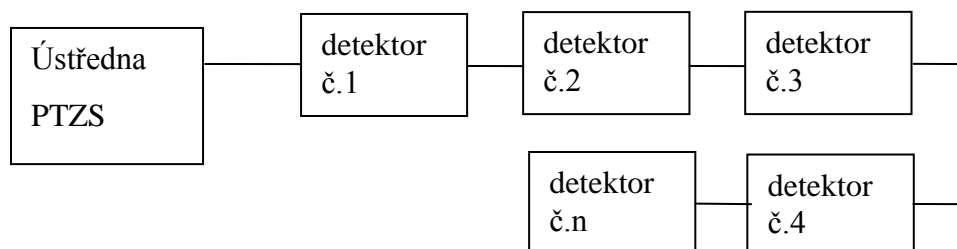
je dle ČSN EN 50131-1 [8] definován jako: "*poplachový systém sloužící k detekování a indikaci přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého prostoru.*" Jedná se o digitální elektronický systém, jež je schopný akusticky nebo opticky signalizovat narušení objektu. Zpravidla se poplachový zabezpečovací systém skládá z ústředny, detektorů, signalizačních a přenosových zařízení, napájecích zdrojů a ovládání. [4]

1.2.1.1 Ústředna

Je jádrem celého poplachového zabezpečovacího systému, jehož senzorickou součástí jsou detektory narušení. Informace z detektorů ústředna zpracovává a vyhodnocuje a v případě narušení vyhlásí poplach. Prostřednictvím poplachového přenosového systému může být ústředna připojena na poplachové přijímací centrum.

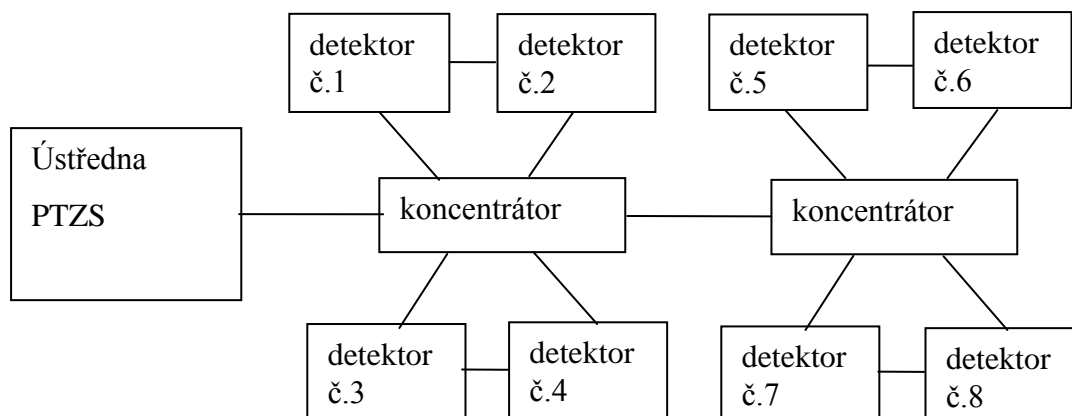
Z hlediska způsobu připojení detektorů rozlišujeme ústředny:

- **analogové (smyčkové)** - pro každou poplachovou smyčku existuje vstupní vyhodnocovací obvod. Změna odporu smyčky způsobená aktivací některého detektoru vede z vyvolání poplachu. Poplachové smyčky tvoří sériově zapojené rozpínací kontakty detektorů. Nevýhodou typu této ústředny je nutnost většího množství kabeláže, protože ke každému detektoru musí vést vodič pro napájení, pro poplachový a sabotážní kontakt čidla, vodiče dodatkových funkcí (typ paměti poplachu, test chůzí...) [3]
- **sběrníkové s přímou adresací čidel** - principem komunikace po datové sběrnici mezi ústřednou a detektory. Ústředna generuje adresy jednotlivých čidel, komunikuje právě s jedním prvkem systému, využívá tzv. časového multiplexu. Každý komponent musí mít v rámci systému přiřazené jedinečné ID. Výhodou tohoto systému je minimální kabelová síť (čtyřvodičové vedení - 2 vodiče pro napájení, 2 vodiče pro sběrnici) a vysoká odolnost proti sabotáži. [2]



Obr. č. 3 Blokové schéma sběrníkové ústředny [2]

- **koncentrátorové (smíšeného typu)** - využívá výhod dvou předchozích typů. Ústředna pracuje na principu komunikace ústředna - koncentrátor (sběrníkový modul smyček "podústředny") pomocí datové sběrnice. Detektory jsou ke koncentrátorům připojeny pomocí smyček. Je-li kapacita ústředny dostatečná, lze na smyčku jednotlivého koncentrátoru připojit právě jedno čidlo a takto realizovat systém až několika sty adresnými čidly. Tento typ ústředny je vhodný pro rozsáhlejší objekt. [2]



Obr. č. 4 Blokové schéma koncentrátorové ústředny [2]

- **bezdrátové ústředny** - jsou propojeny s detektory a ostatními komponenty PZTS bezdrátově. Jejich výhodou je snadná a rychlá instalace i do prostor, kde není možné vést kabeláž. Dalším pozitivem je snadné rozšíření systému o další prvky či snadná změna konfigurace. [2]

Při výběru ústředny musíme brát v úvahu požadovaný stupeň zabezpečení, fyzický rozsah objektu a jeho stavební provedení a samozřejmě finanční možnosti investora.

1.2.1.2 Detektory (čidla, snímače apod.)

Podle ČSN EN 50131-1 je detektor narušení definován jako: "*zařízení konstruované ke generování signálu nebo zprávy o vniknutí, jako reakci na nenormální stav detekující přítomnost nebezpečí*".[9] Detektory narušení reagují bezprostředně na fyzikální jevy související s narušením střeženého objektu, následně detektor vyšle poplachový signál. Detektory dělíme dle způsobu napájení na nenapájené a napájené (k činnosti vyžadují napájecí zdroj). Napájené detektory dále rozdělujeme na aktivní (vyzařují signál elektromagnetických nebo akustických vln - vyhodnocují narušení s využitím vyzařovaného signálu) a pasivní (pasivní reakce na fyzikální změny ve střeženém objektu). [4]

Podrobněji se věnuji detektorům v kapitole 1.3

1.2.1.3 Signalizační zařízení

Hlášení poplachu je možné uskutečnit pomocí lokálních signalizačních zařízení kam řadíme akustická výstražná zařízení (např. siréna, zvonek, hlasové zařízení) a optická výstražná zařízení (např. výbojky, žárovky) nebo poplachového přenosového systému (dálková hlášení). [1]

1.2.1.4 Napájecí zdroje

Musí napájet ústřednu a ostatní komponenty PZTS nepřetržitě. Napájecí zdroj musí splňovat požadavky pro jednotlivé stupně zabezpečení. Napájecí zdroj může být součástí PTZS ale i samostatný. Existují tři druhy napájecích zdrojů bez ohledu na stupeň zabezpečení [1]:

Typ A - energie dodávána z vnějšího zdroje, v případě výpadku z dobíjeného zdroje, který je automaticky dobíjen z vnějšího zdroje energie.

Typ B - energie dodávána z vnějšího zdroje, v případě výpadku z dobíjeného zdroje, který není automaticky dobíjen z vnějšího zdroje energie

Typ C - energie je dodávána pouze ze záložního zdroje

1.2.1.5 Ovládací zařízení

Slouží k jednoduché obsluze PTZS, aby mohl systém plnit svou funkci - např. klávesnice

1.2.2 Komerové bezpečnostní systémy CCTV

Kamerové systémy CCTV - Closed Circuit Television, systémy uzavřených televizních okruhů) slouží k monitorování, zaznamenávání, identifikaci a detekci osob v reálném čase v místě jejich instalace. Veškeré požadavky kladené na systémy CCTV pochází z norem ČSN EN 50132-X. Kamerový bezpečnostní systém se skládá z [4]:

- **kamer** - optický snímač, objektiv, procesor
- **zařízení na přenos a řízení videosignálu** - např. kvadrátory, multiplexory, děliče obrazu, kabeláž, switch, router, web, server, aj.

- **záznamové a zobrazovací zařízení** - analogový nebo digitální videorekordér, projekční /LCD,/plazmové monitory, barevné/černobílé obrazovky
- **příslušenství kamer** - např. kryty, polohovací hlavice, konzoly, IR/halogenové reflektory

1.2.2.1 Kamera

Je základním prvkem CCTV. Snímá senzorem CCD nebo CMOS obraz přes objektiv, který je následně převeden na elektrický signál. Kamery dělíme podle:

napájení - 12V DC, 12/24V AC, 230V AC

videosignálu - černobílé (B/W), barevné (Color)

druhu přenosu videosignálu - analogové, IP kamery, na LAN nebo USB

objektivu - výměnný, součástí kamery

použití v prostředí - venkovní montáž, vnitřní montáž

konstrukce - klasické s vyměnitelným objektivem, kompaktní (objektiv součástí kamery), vodotěsné, stropní (tzv. DOME kamery), PTZ kamery (uživatelské otáčení ve vertikálním i horizontálním směru a plynulá změna ohniskové vzdálenosti objektivu), miniaturní, deskové (jen deska s elektronikou a objektivem) a skryté (např. v PIR čidle).

Kritériem pro volbu kamer jsou obvykle následující parametry [3]:

- **rozlišovací schopnost** - závisí na počtu aktivních obrazových bodů snímacího senzoru (pixel), méně závislá je na formátu. Doporučená rozlišovací schopnost pro běžné aplikace a tam, kde je požadované vysoké rozlišení detailů je u čb kamer 560 - 580 řádků (možné využití v případě digitálního zpracování) a u barevných kamer 460 - 480 řádků.

- *citlivost* - je to určitá mez, při jaké intenzitě světla je ještě kamera schopna snímat obraz. Tato schopnost se měří jako "Lux" úroveň. Citlivost u čb kamer má hodnoty okolo 0,1 lx/F1,2 a u barevných kamer dosahuje hodnot 0,8 lx/F1,2
- *odstup signál/šum (S/N signal/ noise)* - měřítko úrovně šumu videosignálu. Je uváděn. Čím je číslo vyšší, tím lépe. Např. kvalita obrazu je výborná při odstupu 60 dB a při poměru užitečného a šumového signálu 1000:1
- *synchronizace* - zajištění synchronizace signálu se signály kamer používaných v CCTV. Dělíme ji na interní a externí synchronizaci.
- *napájení kamer* - souvisí se synchronizací. Obecně existují 4 varianty napájení a to stejnoměrné napájení (12 V), střídavého nízkovoltového napájení (16 -24 V), střídavé napětí ze sítě (230 V) a napájení po koaxiálním kabelu ze speciální napájecí jednotky či propojeného monitoru.
- *připojení objektivu* - 2 standardy připojení buď C-mount (normalizovaný odstup roviny čipu od roviny zadní čočky objektivu 17,526 mm) nebo CS-mount (normalizovaný odstup roviny čipu od roviny zadní čočky objektivu 12,497 mm)
- *řídící výstupy kamery* - existují 2 typy řízení a to videosignálem (AI) nebo stejnoměrným napětím (DC)

1.2.2.2 *Objektiv*

- zobrazení zorného pole na světlocitlivou plochu CCD nebo elektronky, měřítko zobrazení – ohnisková vzdálenost
- pevné nebo nastavitelné ohnisko – nastavitelné manuálně (2-3x) nebo motoricky (až 27x, tzv. motorzoomy)
- clona – ruční nebo motorické nastavení, regulujeme množství světla
- optická ostrost, různá subjektivní ostrost pro různá osvětlení
- IR filtry apod. [13]

1.2.2.3 *Zařízení pro přenos a řízení videosignálu*

Je možno provést několika různými způsoby. Hlavním kritériem při výběru je počet kamer, požadovaná vzdálenost jednotlivých komponentů video-systému, druh a vliv prostředí a cena, rychlost přenosu, objemu dat, druh připojení. Pro CCTV existují níže uvedené přenosové prostředky [3]:

Koaxiální kabel - potřebná šířka přenosového pásma 6,5 GHz, při přenosu musí být na vstupu i na výstupu připojeno zařízení s charakteristickou impedancí 75 Ω - nejrozšířenější způsob vedení pro vzdálenost několika desítek metrů

Symetrické vedení - jde o dvoudrátový systém realizovaný po kroucené dvojlince např. po UTP kabelu Cat5E používaný pro počítačové sítě. Umožňuje přenos videosignálu až do 1500 m. Nevýhodou je nemožnost přímého propojení kamery a monitoru a také vyšší cena (mimo kabeláže jsou potřeba 2 převodníky ke každé kameře - 1 pro převod videosignálu z kamery na kroucenou dvojlinku a druhý pro zpětný převod na videosignál)

Bezdrátový přenos - používá se zejména v místech, kde není možné táhnout kabeláž. Přenosová vzdálenost je v řádu jednotek kilometrů. Pro přenos je využíváno pásmo 2,4 GHz, v tomto pásmu jsou také provozovány WiFi sítě, proto dochází k poměrně velké míře rušení, což považujeme za první nevýhodu. Druhou nevýhodou je vyšší cena. Přenášený může být videosignál jak z analogových kamer tak i datový tok z IP kamer.

Optický kabel - jeden z nejspolehlivějších videosignálů na vzdálenost až několik desítek kilometrů. Nevýhodou je vyšší cena a technické nároky na instalaci. Přenášený může být opět videosignál jak z analogových kamer tak i datový tok z IP kamer.

Počítačová síť - obvykle realizována UTP kabelem Cat5E. Přenosová vzdálenost je v řádu stovek metrů. Opět je umožněn přenos datového toku jak z IP kamer tak webserverů, na něž jsou napojeny analogové kamery.

1.2.2.4 *Záznamové a zobrazovací zařízení*

Záznamová zařízení slouží k dokumentaci a archivaci záběrů kamer. Nejčastěji využíváme:

Digitální záznamové zařízení DVR (Digital Video Recorder) - zobrazují a ukládají videozáznam obraz z několika kamer pro pozdější prohlížení. Doplnují jej o řadu funkcí jako je detekce pohybu v obraze, přístup k záznamům přes internet, zasílání poplachových

hlášení emailem spolu s fotografií stavu, trvalé ukládání záznamů na externí prostředek. Stejně tak slouží k dokumentaci události a poskytují nástroje pro vyhledávání záznamů dle data, času a druhu poplachu. [10]

NVR (Network Video Recorder) - zaznamenává a uchovává digitální videozáznam z IP kamer. IP kamery jsou téměř totožné s analogovými, liší se zejména tím, že obrazová informace je digitální a je přenášena přes síťové rozhraní (konektor RJ-45). [11]



Obr. č. 5 Ukázka techniky NVR [11]

IR přísvit - umožňuje snímá obrazu i ve tmě. Zbytkové světlo přepne CCD čip do černobílého snímání a předradí se před něj IR filtr. Přepínání proběhne automaticky podle intenzity osvětlení. Při přechodu kamer do nočního vidění je zapnutý IR přísvit, který se skládá z IR LED diod umístěných v kruhu objektivu. Tím je eliminováno IR světlo o vlnové délce 810 - 940 nm. Tyto kamery jsou schopné vidět i v naprosté tmě.

K zobrazení dějů snímáných kamerou nebo zaznamenaných na videorekordéru jsou nejčastěji využívány **monitory** s vakuovou obrazovkou, další alternativou jsou zobrazovače z tekutých krystalů tzv. **LCD displeje**. Dalším nástupce vakuové obrazovky je **plazmový displej**.

V současné době je velkým hitem **CCTV automatické sledování pohybujících se objektů**. Základem je uživatelsky ovladatelná pohyblivá kamera umožňující pohyb v horizontální i vertikální rovině a plynulou změnu ohniska objektivu. V případě vstupu osoby do střeženého prostoru, kamera automaticky zaostří a natáčí se tak, jak se osoba pohybuje. [13]

1.2.3 Systémy kontroly vstupů a docházkové systémy

Dle platné normy ČSN EN 50133-1 je systém kontroly vstupu (ACS) definován jako: "Systém obsahující všechna konstrukční a organizační opatření včetně těch, která se týkají zařízení nutných pro řízení vstupu." Používají se k řízení a kontrole vstupů do objektů. Každému uživateli jsou přidělena přístupová práva na základě personální politiky, stupně oprávnění či časovém harmonogramu aj. Přístup je povolen na základě jednoznačné identifikace uživatele po ověření přístupových práv. Speciálním případem přístupových systémů jsou systémy docházkové, u nichž je prvotním cílem monitorování času a důvodu průchodu daným místem. Přístupová a docházkové systémy mohou být integrované do jednoho celku. [4]

Základními funkcemi jsou [4]:

- **identifikace** - je možná třemi způsoby a to podle toho, zda subjekt disponuje znalostí kódu nebo hesla, či vlastní identifikační prvek (identifikační karta, přívěšek, RF ovladač, aj.) nebo svými charakteristickými rysy - biometrie
- **snímací zařízení (čtečky)** - volíme podle použitých identifikačních prvků. Existují *základní (neinteligentní) snímače* (přečtení čísla, zadání kódu), *polointeligentní snímače* (potřebné vstupy a výstupy pro ovládání místa prostupu, ale neprovádí vlastní porovnání o přístupu) a *inteligentní snímače* (potřebné vstupy a výstupy pro ovládání místa prostupu, obsahují paměť přístupových údajů a provádějí rozhodnutí o přístupu samostatně)
- **řídící jednotky** - (terminály) pracují na základě databáze s oprávněními jednotlivých osob a informací od snímacího zařízení o umožnění nebo zamítnutí vstupu.
- **centrální jednotka** - je propojená řídícími jednotkami. Monitoruje a řídí přístupový a docházkový systém. Základem je software propojený s řídícími jednotkami pomocí počítačové sítě.

1.2.4 Elektrická požární signalizace EPS

Při zpracování kapitoly jsem čerpala z literatury [1] a [3]. Elektrická požární signalizace slouží ke včasnému rozpoznání příznaků požáru a vyhlášení požárního poplachu. Díky EPS zařízení je možné snížení výše škod zapříčiněných požárem, jehož častou příčinou bývá

nedodržení technologických postupů a nedůsledná kontrola bezpečnostních předpisů. Veškeré náležitosti týkající se systémů EPS stanovuje série norem ČSN EN 54 - X. EPS je soubor technických zařízení, která se skládají z ústředny EPS, hlásičů požáru a doplňujících zařízení.

- **požární hlásiče** - rozdělujeme na *manuální* - tlačítkové (použity osobou, která zjistí požár), *automatické* (monitorují fyzikální nebo chemický jev, reagují na něj a předávají informaci do požární ústředny). Podle principů funkce rozeznáváme automatické ionizační, optické, teplotní, tlakové, odporové, kombinované.
- **ústředny EPS** - zařízení, která soustřeďují informace ze všech hlásičů. Informace z nich zpracovává a reaguje na ně odezvou (vyhlášení poplachu, signalizace poruchy, informace na PPC). Rozlišujeme ústředny *konvenční neadresné* (pokud je na smyčce více hlásičů, při požáru není možné zjistit, který hlásič byl aktivován), *konvenční adresné* (hlásič má jedinečné ID, je možné zjistit, který byl aktivován), *analogové* (adresné hlásiče připojeny kruhovou sběrnicí) a *interaktivní* (inteligentní adresné detektory vybavené mikroprocesory, které samy vyhodnotí situaci a do ústředny je poslána informace o nastalém stavu).
- **přenosové prostředky** - zajišťují přenos poplachové informace do ohlašovny požáru. Přenos může být buď místní, nebo vzdálený, v obou případech musí být učiněn co nejrychlejší zásah proti vznikajícímu požáru. Požární systémy jsou často napojené na specializované pulty požární ochrany.
- **vedení** - z hlediska umístění kabelu v prostoru dělíme linkové vedení na vnitřní, venkovní nadzemní a venkovní zemní. Dle typu umístění musí být vždy vytypovaný správný typ kabelu.

1.3 Technická ochrana objektu

Jedná se o jednu z nejhůře překonatelných ochran objektu pro pachatele. Slouží k detekci a indikaci přítomnosti vniknutí pachatele do střeženého objektu.

Z hlediska prostorového zaměření dělíme technickou ochranu na [1]:

- **obvodovou** - signalizuje narušení obvodu objektu - katastrální hranici obvykle vymezenou přírodními nebo umělými bariérami (vodní toky, ploty, zdi apod.)

- **plášťovou** - signalizuje narušení pláště objektu (celá budova nebo vyčleněný komplex místností či prostor ve větším objektu). Pachatel překonává mechanickou překážku, při níž je detekováno narušení konvenčních i nekonvenčních detektorů. Plášťová ochrana se obvykle realizuje zevnitř objektu.
- **prostorovou** - pomocí detektorů signalizuje narušení v chráněném prostoru.
- **předmětovou** - složí k signalizaci napadení nebo neoprávněné manipulace s chráněnými předměty.
- **tísňovou** - signalizuje ohrožení života napadením, zdravotními problémy, nebo působením živlů (plyn, požár, voda)

1.3.1 Prvky obvodové ochrany

Mají za úkol signalizovat narušení vnějších částí objektu, k čemuž jsou využívány různé typy detektorů, které musí být konstruovány s ohledem na venkovní použití. Je třeba brát v úvahu vlivy jako je vlnění travního porostu, pohyb listů a větví stromů či keřů, vibrace oplocení ve větru, vítr, sníh, déšť, pohyb zvěře či dopravní ruch. Základním požadavkem na prvky perimetrické ochrany je nezávislost funkce na klimatických podmínkách. Mezi základní sortiment prvků obvodové ochrany patří [3]:

Mikrofonické kabely - při mechanickém namáhání nebo při záchvěvech citlivého mikrofonického kabelu generují na svém výstupu elektrický signál, který je dále zpracováván a na základě akustického odposlechu je možné rozeznat i přesný typ narušení (nadzvednutí, přelézání, nebo přestřihnutí pletiva).

Infračervené závory a bariéry - jsou realizovány jako jeden set dvou detektorů. Na jedné straně je část vysílací a na druhé straně je část přijímací, mezi nimi probíhá jeden či více infračervených paprsků. Přerušením jednoho z nich dochází k vyhodnocení poplachu. Dosah závor je desítky až stovky metrů. Infračervené bariéry jsou tvořeny z více IR závor umístěných nad sebou do podoby jakéhosi sloupku.

Mikrovlnné bariéry - mezi přijímačem a vysílačem je vytvořené elektromagnetické pole, jehož narušení je detekováno a vyhodnocováno přijímačem. Typickým tvarem je elipsoid s rotací okolo velké a malé osy, kdy poměr vzrůstá se zvětšením vzdálenosti mezi vysílačem a přijímačem. Výhodou je větší rozsah bariér cca 200 až 300 m.

Štěrbinové kabely - instalovány do země v hloubce asi 30 cm a vzdálenosti asi 2 m od sebe. Po celém povrchu vodiče jsou vytvořeny otvory ve tvaru kosočtverce tzv. štěrby. Jeden kabel vytváří a vyzařuje elektromagnetické pole, druhým kabelem jsou jeho změny vyhodnocovány.

Zemní tlakové hadice - jedná se o dvojici paralelně položených pružných natlakovaných hadic, naplněných nemrznoucí kapalinou v rozteči asi 1 m, zakopány asi 30 cm hluboko. Tlak je neustále monitorován a v případě změny je vyhlášen poplach.

Perimetrická PIR čidla - vyhodnocují změny záření paprsků dopadajících na detektor. V případě, že se v zorném poli detektoru pohybuje těleso s jinou teplotou než má okolí, detektor vyhodnotí změny, vyšle signál a vyhlásí poplach. Dosah je 150 až 200 m. [4]

Plotová vibrační čidla - skládají se z perimetru, který je provlečen oplocením, může tvořit až kilometr dlouhé úseky. Senzorický kabel je realizován dvouvodičovou linkou s vibračními čidly. Řídící jednotka do něj vysílá krátké impulzy a zároveň obdržené signály vyhodnocuje. Podle jejich charakteru je možné rozeznat stav detekčního vedení a při narušení s přesností 20 m určit místo, kde k němu došlo. [2]

Laserové závory - pracují na stejném principu jako infračervené závory a bariéry s rozdílem v použití laserového paprsku o vlnové délce 850 nm. Dosahuje až 1 km.

1.3.2 Prvky plášťové ochrany

Pro vypracování kapitoly byla použita literatura [2] a [3]

Magnetické kontakty - slouží k detekci narušení dveří, oken (neslouží k detekci jejich výplní), otevření bran, mříží a závor nebo také k detekci sejmutí důležitých částí systému ze zdi (například demontáž napájecího zdroje). Jde o jednoduché rozpínací kontakty, jako jsou mikrospínače.

Vibrační čidla - pro hlídání průrazu stěn a stavebních konstrukcí. Základem je elektromechanický měnič s vyhodnocovací elektronikou. Osazují se podle konstrukčního provedení na riziková místa průchodu zdí, luxfery či rámy dveří a oken.

Poplachové folie, tapety, polepy a poplachová skla - pracují na principu přerušení vodivého média uvnitř folie, tapety, pásků aplikovaných samostatně na povrchu hlídané plochy

Čidla na ochranu skleněných ploch - fungují na principu detekce zvuku, které vyvolává tříštění skla, čidlo může být přilepeno přímo na skleněnou plochu a snímá zvuk šířící se hmotou skla. Praktičtější řešení je využití akustických čidel rozbití skleněných ploch. V tomto případě se čidlem detekuje akustický efekt charakteristický pro tříštění skla. Výhodou tohoto řešení je to, že čidlo není přilepeno na povrch skla, ale bývá umístěno v blízkosti skleněné výplně a dokáže tak detekovat všechny okenní výplně v místnosti.

1.3.3 Prvky prostorové ochrany

Mluvíme-li o prvcích prostorové ochrany, mluvíme o detektorech pohybu. Rozdělujeme je na čidla aktivní a pasivní. Některé detektory mohou být navíc vybaveny o funkci antimasking (ochrana vyřazení čidla z provozu překrytím nějakým předmětem nebo přestříkáním barvou). Mezi základní prostorové prvky patří [2], [3]:

Pasivní infračervené detektory (PIR - Passive Infrared Receiver) - vyhodnocuje změny v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Pyroelektrický snímač detekuje změny záření dopadající na detektor. Jsou nejrozšířenějším druhem detektorů pohybu. Jsou nenáročné na konstrukci a mají nízkou spotřebu energie. Jejich nevýhodou může být narušení osvětlením či slunečním zářením.

Mikrovlnné detektory (MW - Microwave sensors) - k detekci pohybu využívají Dopplerova jevu. Pracují v kmitočtovém pásmu 2,5 GHz, 10 GHz a 24 GHz. Patří mezi aktivní prvky. Vysílač i přijímač se nachází v jednom plastovém krytě. Typickým dosahem ve vnitřním prostředí je 15 - 30 m. Oproti PIR detektorům detekují lépe pohyb ve směru k detektoru, od detektoru se mohou vzájemně negativně ovlivňovat. Největším problémem jsou obvykle kovové a hladké plochy.

Ultrazvukové detektory (US - Ultrasound detectors) - k detekci pohybu využívají akustického signálu. Patří mezi aktivní detektory. Pracují rovněž na aplikaci Dopplerova jevu, vysílají ultrazvukové vlny o kmitočtu 40 kHz. Opět jsou nejcitlivější na pohyb k a od detektoru.

Aktivní infračervené detektory (AIR - Active infrared detectors) - vysílají infračervené paprsky, následně vyhodnocují jejich odraz. Nedetekují malý pohyb nebo pohyb tělesa, které nevyzařuje teplo. Mohou být případně využity v objektech s rychlými teplotními změnami.

Kombinované detektory (Duální) - jejich hlavním cílem je snížení planých poplachů a zvýšení spolehlivosti zabezpečovacího systému. Detektor je složený ze 2 částí pracujících na rozdílném typu detekce. Narušení je detekováno pouze v případě narušení obou aktivních částí detektoru. Nejčastější kombinací jsou PIR a MW detektory.

1.3.4 Prvky předmětové ochrany

Kontaktní detektory - slouží k ochraně v kategorii nízkých rizik, jedná se o tlakové a tahové kontakty, mikropsínače a magnetické kontakty

Kapacitní kontakty - deskové kondenzátory, jejichž dielektrikem je vzduch a elektrody kovové části předmětu a zem. Dotelem či přiblížením k předmětu dochází ke změně kapacity, což následně řídící jednotka vyhodnotí jako narušení.

Tlakové akustické detektory - snímají a vyhodnocují vibrace vzniklé při destrukci chráněných ploch

Bariérové detektory - reagují na narušení vysílajících paprsků s "bariérovou" vyzařovací charakteristikou např. PIR, AIR detektory nebo laserové detektory či infračervené závoje

Trezorové detektory - jde o siezmická čidla, která jsou schopná rozpoznat všechny druhy útoků na trezory. Jsou schopná detekce použití rukou, tak elektrického nářadí (např. vrták) či tepelného nářadí nebo výbušnin. [2]

1.3.5 Prvky tísňové ochrany

Prvky tísňového hlášení - slouží k ochraně osob v případě přímého ohrožení. Mohou být instalovány skrytě anebo veřejně. Manuálním stiskem tlačítka je vyvolán poplach. Tísňová tlačítka pracují na principu magnetického kontaktu nebo mikropsínače. Pokud jsou hlásiče umístěny na veřejném a viditelném místě, musí být chráněny např. ochranným sklíčkem před neúmyslným vyhlášením poplachu. [2]

1.4 Stupeň zabezpečení

Abychom objekt zabezpečili vhodnými prvky PZTS z pohledu přístupové úrovně, provozování, vyhodnocení, detekci, napojení zabezpečení proti sabotáži, monitorování, propojení, záznamu událostí, musíme stanovit stupeň zabezpečení s ohledem na požadavky

investora. Dle normy ČSN EN 50131-1 rozlišujeme 4 stupně zabezpečení. Jejich klasifikace je uvedena v tabulce 2. [4]

- Stupeň 1: Nízké riziko
- Stupeň 2: Nízké až střední riziko
- Stupeň 3: Střední až vysoké riziko
- Stupeň 4: Vysoké riziko

Tabulka 2 Stupně zabezpečení

Stupeň	Míra rizika	Narušitel	Typ objektu
1	nízké	narušitelé mají malou znalost PTZS a že mají k dispozici omezený sortiment snadno dostupných nástrojů	rodinné domky, garáže, kiosky, byty, chaty...
2	nízké až střední	narušitelé mají určité znalosti o PTZS a že použijí základní sortiment nástrojů a přenosných přístrojů.	komerční objekty
3	střední až vysoké	narušitelé jsou obeznámeni s PTZS a mají úplný sortiment nástrojů a přenosných elektronických zařízení	zbraně, ceniny, informace, narkotika...
4	vysoké	narušitelé jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků PTZS	jaderné elektrárny, sklady výbušnin, velké galerie...

V případě rozdělení PTZS do subsystémů, může každý subsystém obsahovat prvky různého stupně zabezpečení. V takovém případě je stupeň subsystému stanoven podle nejnižšího stupně použitého prvku v subsystému. Stupeň celého systému PTZS je stanovený podle nejnižšího stupně jeho subsystému.

1.5 Klasifikace prostředí

Při výběru vhodného zabezpečení je třeba zvážit prostředí, do kterého bude daný komponent aplikován. Dle ČSN EN 50131 - 1 ed. 2 určujeme 4 třídy prostředí. Výrobce v dokumentaci uvádí třídu, pro kterou je zařízení určeno. [1]

Třída I: Prostředí vnitřní

Komponenty PZS musí správně pracovat při působení vlivů prostředí, které se vyskytuje ve vytápěných místnostech. Předpokládají se změny teplot v rozmezí $+ 5^{\circ}\text{C}$ až $+ 40^{\circ}\text{C}$ při střední relativní vlhkosti okolo 75% bez kondenzace.

Třída II: Prostředí vnitřní všeobecné

Komponenty PZS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně v objektech, kde není udržována stálá teplota. Předpokládají se změny teplot v rozmezí $- 10^{\circ}\text{C}$ až $+ 40^{\circ}\text{C}$ při střední relativní vlhkosti okolo 75% bez kondenzace.

Třída III: Prostředí venkovní chráněné

Komponenty PZS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty PZS nejsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí $- 25^{\circ}\text{C}$ až $+ 50^{\circ}\text{C}$ při střední relativní vlhkosti okolo 75% bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85% až 95% bez kondenzace.

Třída IV: Prostředí venkovní všeobecné

Komponenty PZS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty PZS jsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí $- 25^{\circ}\text{C}$ až $+ 60^{\circ}\text{C}$ při střední relativní vlhkosti okolo 75% bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85% až 95% bez kondenzace.

1.6 Typ zabezpečení objektu

Instalační firma navrhuje typ zabezpečení investorovi s ohledem na hodnotu zabezpečovaného majetku. Investor se rozhoduje na základě svých finančních možností opět s ohledem na hodnotu zabezpečovaného majetku. V případě vysokého rizika napadení může zasahovat do kategorie zabezpečení třetí strana např. pojišťovna, která se řídí směrnicí ČAP P 2333. Tato směrnice umožňuje optimalizovat zabezpečení majetku.

2 ZAJIŠTĚNÍ BEZPEČNOSTI PROVOZU AREÁLU

Cílem zajištění bezpečnosti provozu areálu je vytvoření stabilního, relativně předvídatelného prostředí, ve kterém jedinec nebo skupina jedinců může vykonávat svou práci bez rušení anebo poškození a bez strachu z takového rušení nebo poškození. Z toho důvodu musíme zvolit odpovídající zabezpečovací systém firmy na základě analýzy jednotlivých možných rizik ve střeženém objektu s ohledem na požadavky investora. Musíme posoudit lokalitu objektu i budovy, vymezit možné vlivy působící vně a uvnitř areálu. [4]

2.1 Posouzení lokality objektu

Míra rizika vloupání do střeženého objektu závisí na charakteru střeženého majetku. Při bezpečnostním posouzení musíme brát v úvahu faktory jako je druh majetku, hodnota majetku, objem majetku, historie krádeží, stávající nebezpečí. [5]

V našem případě se jedná o moderní firmu s nadstandardním vybavením, která se zabývá výrobou a distribucí kabelů a kabelového příslušenství. Tato činnost je doplněna nezbytnou administrativou. Z důvodu hodnoty mědi obsažené v kabelech je tato část majetku firmy pro pachatele atraktivní. V minulosti došlo k vloupání a odcizení většího množství kabelu s vysokou hodnotou mědi.

2.2 Posouzení lokality budovy

Při zpracování návrhu zabezpečení je určujícím faktorem struktura střežených objektů. Cílem je odhalit slabá místa v rámci stavební dispozice objektu. (Valouch)

Posuzovaný objekt se nachází ve východním okraji města v nově vznikající průmyslové zóně. Je oplocený drátěným pletivem, na jižní straně osazen posuvnou bránou a vstupní brankou. Budova půdorysného tvaru L se skládá z dvoupodlažní administrativní části a z jednopodlažního skladu, v jehož části je vytvořeno druhé podlaží. Budova nemá žádné sklepní prostory. Před administrativní částí objektu je umístěno parkoviště pro návštěvy. Za skladovou částí je umístěn zásobovací dvůr. Parkoviště i příjezdové komunikace jsou osvětlené.

Co se týče konstrukce objektu, obvodový plášť je proveden z plechových sendvičových panelů, pultová střecha je postavena z trapézového plechu, výplně otvorů v obvodovém plášti jsou hliníková okna a dveře, zateplená sekční vrata a dveře. Objekt má 2 vstupy.

Budova je opatřena následujícími technickými prvky ochrany:

- Přístupová kontrola a docházkový systém - zaměstnanci mají umožněný přístup pomocí čipové karty, areál otevřený pro veřejnost od 7 hod. -17 hod. Vstup do budovy přes recepci
- Poplachové zabezpečovací a tísňové systémy - komplexní plášťová a prostorová ochrana určených prostor s aplikací infrapasivních detektorů a magnetických kontaktů. Systém je napojený na přijímací a poplachové centrum bezpečnostní služby.
- Kamerový systém - periferní ochrana kamerami okolo budovy, obrazový signál kamer soustředěný na monitoru v budově
- Elektrická požární signalizace - v prostorech budovy jsou nainstalovány automatické optickokouřové hlásiče, únikové cesty jsou vybaveny tlačítkovými hlásiči požáru. Systém EPS je napojen na poplachové a přijímací centrum hasičského záchranného sboru.

2.3 Vlivy působící na zabezpečovací systém a mající původ uvnitř střežených objektů

Uvnitř objektů existuje řada faktorů majících vliv na funkci zabezpečovacího systému, proto při výběru, umístění a nastavení komponentů musíme brát tyto faktory v úvahu [1]:

- **vodovodní potrubí** - pohyb vody v potrubích může mít vliv na MW detektory
- **Vytápění, ventilace, vzduchotechnika** - vliv na UV detektory
- **závěsné tabule a ostatní předměty** - vliv možného pohybu předmětů v zorném poli detektorů
- **výtahy** - možné vibrace mající vliv na strojní zařízení
- **světla** - zejména zářivky mohou rušit MW detektory, reflektory po nasměrování na čočku (zrcadlo) způsobují planý poplach PIR detektorů

- **elektromagnetické rušení** - všechna elektrická zařízení mohou být, ať už záměrně nebo neúmyslně zdrojem elektromagnetického rušení, které může ovlivnit provoz zařízení PZS (např. elektrické svařovací soupravy, elektrické generátory a motory, vysokofrekvenční spojovací zařízení, mobilní telefony)
- **vnější zvuky** - zařízení, jež generují zvuky, mohou mít negativní vlivy na ultrazvukové detektory
- **domácí zvířata a škůdci** - negativní vliv v případě použití detektorů pohybu
- **průvan** - ultrazvukové detektory vnímají vzduch jako prostředek pro přenos UV energie, PIR detektory reagují na náhlou změnu teploty
- **uspořádání skladových předmětů** - možnost zastínění průzoru detektoru, při přemísťování předmětů způsobení planého poplachu
- **struktura střežených objektů** - posuzuje se konstrukce střech, podlah a sklepů, stavební materiál, usazení oken, dveří

2.4 Vlivy působící na zabezpečovací systém a mající původ vně střežených objektů

Jde o faktory, které nemůže uživatel ovlivnit. V případě negativního vlivu na provoz některého zařízení nebo PZS jako celku, musíme pečlivou volbou a rozmístěním zařízení vyloučit vliv těchto podmínek. Jedná se zejména o

- **dlouhodobé faktory** - nepředpokládáme změnu po dlouhý časový interval, například několik let. Řadíme sem silnice, železnice, podzemní dopravní systémy a letecké dopravy, dále parkoviště automobilů jak podzemní, tak i nadzemní,
- **krátkodobé faktory** - vlivy konstrukce budov sousedících se střeženými objekty
- **vlivy počasí** - vlivy počasí, které mohou působit na střežené objekty na místech s výskytem silných větrů a dešťů nebo na místě s nadměrným působením blesků.
- **vysokofrekvenční rušení** - z blízkých stožárů vysílačů veřejné rozhlasové sítě nebo televize, antén civilních nebo vojenských radarů, základních stanic systému

mobilních telefonů, stožárů vysílačů pohotovostních služeb nebo antén amatérských vysílačů

sousední objekty - zvláště těžké stroje, které mohou při provozu způsobovat vibrace nebo zařízení generující vysokou hladinu elektromagnetického rušení. [1]

2.5 Komplexnost ochrany provozu areálu

Komplex ochrany areálu je soubor konkrétních praktických opatření sloužících k zajištění ochrany celého areálu. V úvahu vždy bereme [7]:

- **Bezpečnost osob** - bez ohledu na to zda jde o zákazníka či zaměstnance firmy. Hodnotíme rizika při násilných případech, jako je teror, loupež a nenásilných případech jako je vydírání, požár, havárií a katastrofách, rizika běžné pracovní činnosti jako je bezpečnost práce, ekologická ochrana. V případě naší firmy považujeme za nejvyšší riziko možnost vzniku požáru v kancelářích firmy, který by mohl mít vážné primární i sekundární následky. EPS je již ovšem ve firmě realizována a zákazník ji nehodlá měnit. Péče o bezpečnost práce zaměstnanců je předmětem provozního řádu firmy, na základě kterého se zaměstnanci podrobují řadě školení a zaučení, jsou seznamováni jak s provozním systémem firmy, tak i s bezpečností práce.
- **Bezpečnost majetku** - jak majetku klientů tak i vlastního při násilných případech – loupež tak i nenásilných – krádeže, podvody, požáry, havárie, běžné pracovní nebo podnikatelské činnost. Bezpečnost majetku a optimální zpracování technické bezpečnosti je hlavním úkolem této práce. Zvažujeme zejména hodnoty jednotlivých nemovitých věcí, které se v areálu nacházejí. Jedná se jak o majetek obchodní (kabely a kabelové příslušenství), provozní (vybavení kanceláří, skladu, stroje) tak i o finanční hotovost. Mimo již zmiňované EPS je nutné zabezpečit firmu proti vloupání, krádeži, poškození zboží a prostředků firmy a také případné ohrožení pracovníků při manipulaci s penězi. Mezi nejzranitelnější místa patří průstupy na plášti objektu v 1.NP – vstupní dveře, nouzový východ, sekční vrata, okna a v 2. NP - terasy, balkónové dveře, okna, světlíky. Zabezpečení bude navrženo efektivně s ohledem na dobu přítomnosti a nepřítomnosti pracovníků

firmy. Po vyhodnocení způsobu možného neoprávněného vniknutí do areálu a s tím souvisejících možností škod jsme zařadili objekt firmy do stupně zabezpečení 2.

- **Bezpečnost informací** - a to informací o zákaznících i vlastních zaměstnancích při narušení spolehlivosti faktorů, neúmyslným působením vlastního personálu, úmyslným působením vlastního personálu a jiných osob. Zaměstnanci jsou seznámeni se všeobecnými zásadami při práci s citlivými daty, vstupními kódy a dalšími informacemi ohledně zabezpečení. Jsou řádně proškoleni.

II. PRAKTICKÁ ČÁST

3 STÁVAJÍCÍ ZABEZPEČOVACÍ SYSTÉM

Administrativně logistické centrum firmy bylo postaveno v roce 2007, svou činnost zahájilo v roce 2008. Jde o poměrně novou budovu již opatřenou bezpečnostním systémem, který však vykazuje jisté nedostatky. Na základě informací, které nám firma poskytla, zanalyzujeme stav současného komplexního zabezpečovacího systému, poukážeme na jeho kvality a nedostatky. Výsledky této kapitoly následně použijí ke zpracování studie návrhu nového zabezpečení. Z důvodu zajištění bezpečnosti, která by mohla být ohrožena zveřejněním práce, nebyly poskytnuty přesné informace o stávajícím zabezpečovacím systému firmy, avšak poskytnuté informace jsou dostačující pro zpracování studie.

3.1 Základní perimetrická ochrana areálu

Základní perimetrickou ochranu areálu tvoří oplocení, které je provedeno z drátěného poplastovaného pletiva o výšce 150 cm. Průměr železného drátu je cca 2,5 mm. Pletivo je upevněno pomocí ocelových poplastovaných sloupů zakotvených do základových patek. Na jižní straně pozemku je pro vjezd vybudovaná posuvná brána a pro vstup branka vybavená dorozumívacím zařízením na recepci a čtecí hlavou čipových karet RFID. Brána i branka jsou pro veřejnost otevřeny v době 7 - 17 hod. Na jihozápadní straně se nachází malá vstupní branka určená pro vstup zaměstnanců do areálu, která je také opatřena čtecí hlavou čipových karet RFID. Branky jsou osazeny magnetickými vratovými kontakty napojenými na ústřednu PZTS.

Jako doplněk PZS je oplocení vzhledem k ceně vyhovující. Nevýhodu vidím v relativně snadném překonání této zábrany, což dokazuje vloupání do objektu v minulosti. Při krádeži bylo toto oplocení pachateli bez problémů překonáno. Oplocení bylo rozstřiženo a materiál byl vyvezen ven z areálu.

3.2 Poplachový zabezpečovací systém

Jádrem PZTS je ústředna, v našem případě Digiplex EVO 192 od firmy Paradox, doplněná klávesnicí Digiplex DGP2 - 641 BL -. Na ústřednu jsou zapojeny všechny zabezpečovací

detektory, v našem případě pouze magnetické kontakty, PIR detektory a kódování celého systému.

3.2.1 Ústředna DIGIPLEX EVO192

Ústředna DIGIPLEX EVO192 je určena pro střední a velké objekty do maximálního počtu 192 zón a 8 podsystémů. Jde o plně adresovatelný sběrniceový systém, do kterého lze zařadit až 254 sběrniceových modulů (klávesnice, bezdrátová nadstavba, expandéry, PGM výstupy, doplňkové zdroje, posilovač sběrnice, hlasová nadstavba) i samostatné sběrniceové detektory BUS. Vedle klasických NC zón s výstupem relé (připojené na vstupy ústředny, expandérů nebo klávesnic) a zón tvořených sběrniceovými detektory (PIR vnitřní i venkovní, magnetický kontakt, detektor tříštění skla, stropní detektor) lze tvořit i bezdrátové zóny připojením bezdrátové nadstavby RTX3. Bezdrátová komunikace je obousměrná a lze pro ni využít následující bezdrátové vysílače MAGELLAN, bezdrátové pohybové detektory, požární detektor, magnetické kontakty až 999 bezdrátových klíčenek REM1, REM2 a REM3 ,bezdrátové PGM (2WPGM).

Ústředna je uložena v boxu ESPRIT BOX D. Příslušenství je záložní akumulátor BASIC 12V/18Ah (z výpočtu), součástí je také kabeláž (6 – žilový kabel Ka6x - 2x0.6+4x0.4, sběrniceový kabel UTP CAT3 2P Cu, 2x2x0.5.) [12]



Obr. č. 6 Digiplex EVO 192 [12]

3.2.1.1 *Zhodnocení ústředny*

Průzkumem trhu jsem zjistila, že ústředna Digiplex EVO 192 patří díky svým vlastnostem a možnostem k nejvíce využívaným ústřednám středně velkých firem. Její kvality mi také potvrdili technici bezpečnostní firmy. Důležitým faktor pro další využití je, že lze do sběrnice systému zařadit až 254 modulů, tudíž jsme schopni bez problémů připojit k ústředně další detektory a zařízení. Ústředna tedy splňuje veškeré požadavky zákazníka, bude jí využito v další části práce.

3.2.2 Klávesnice Digiplex DGP2 - 641 BL

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



Obr. č. 7 Digiplex DGP2 - 641 BL [26]

Ve firmě jsou instalovány 3 klávesnice - jedna se nachází přímo v oblasti umístění ústředny, slouží především pracovníkům bezpečnosti agentury k programování. Další klávesnice je umístěna v oblasti administrativní budovy. Zde je k dispozici určitému okruhu pracovníků, kteří mají oprávnění ke kódování budovy. Poslední klávesnice je instalovaná v zázemí pracovníků ADM. Je určena ke kódování samostatné zóny tohoto zázemí. Klávesnice je naprosto vyhovující.

3.2.3 Magnetické kontakty SA-203

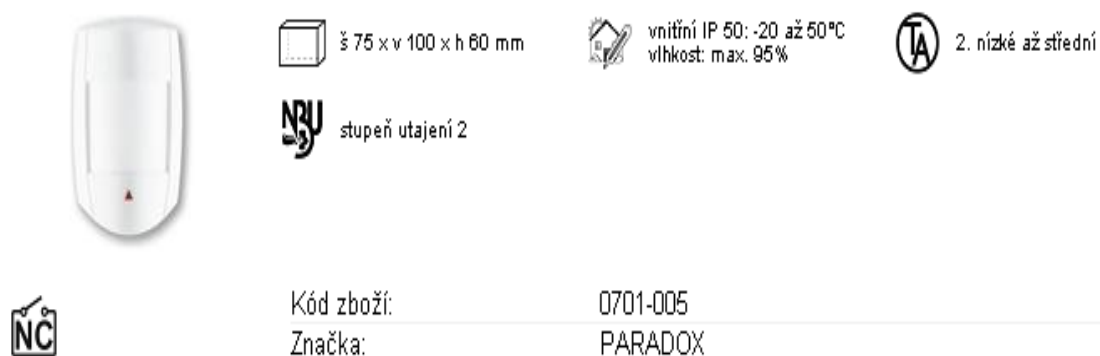
Magnetické kontakty SA-203 byly osazeny do všech dveří a oken. Tyto kontakty jsou dle investora i servisních techniků vyhovující, nevykazují žádné potíže.



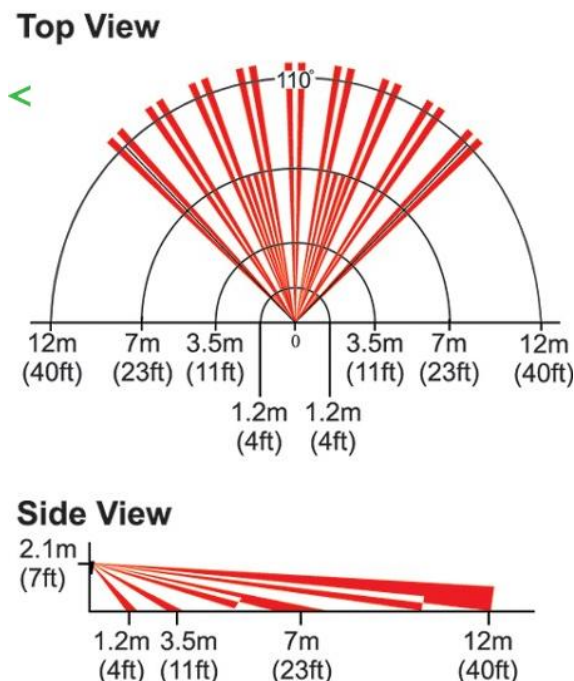
Obr. č. 8 Magnetické kontakty SA-203 [27]

3.2.4 PIR detektor DG55

Pro prostorovou ochranu byly do kanceláří umístěných podél oken a terasy aplikované infrapasivní detektory ve výšce cca 2,3 m od podlahy. V halové části je tímto způsobem řešena ochrana světlíků ve střešní konstrukci. Jedná se o digitální PIR detektory **DG55** - Duální infrapasivní detektor s plně digitálním zpracováním signálu, s digitální softwarovou teplotní kompenzací, softwarovou ochranou „SHIELD“ se dvěma stupni nastavení, obsahuje také digitální automatický čítač pulsů, významným parametrem je vysoká odolnost proti RF rušení. [13]



Obr. č. 9 DG55 (0701-005) - DUAL [13]



Obr. č. 10 DG55 DUAL - oblast pokrytí [13]

Pro zabezpečení kanceláří jsou obvykle postačující jednoduché PIR detektory, které reagují na vyzařování lidského těla. Jsou modulované v přijímací části přerušováním zón, kterými v prostoru místnosti prochází. Obecně výhodu PIR detektorů vidím zejména ve snadné montáži a seřízení, malé spotřebě energie, vysoké spolehlivosti a odolnosti proti planým poplachům. Další velkou výhodou je možnost instalace více PIR čidel do jednoho prostoru, protože nevyzařují žádnou energii. V případě nutnosti úplného vykrytí prostoru se doporučuje instalace více čidel k vzájemnému překrytí detekčních zón, bez nebezpečí vzájemného ovlivňování. Nevýhodou může být možnost překonatelnosti některých druhů čidel a vliv některých faktorů jako je světelné rušení (slunce svítící oknem dovnitř místnosti, světlomety automobilů), rychlé teplotní změny (podlahové topení, technická zařízení v místnosti) nebo proudění vzduchu (průvan, ventilace, klimatizace), zařízení místností (pohybující se závěsy a žaluzie), zvířata.

Co se týče nainstalovaných PIR detektorů DG55, investor si stěžuje na časté falešné poplachy z různých subsystémů budovy. Ani po servisním seřízení v některých částech budovy nedošlo k eliminaci poplachů. Zejména potom v části skladu a spisovny, které jsou umístěny v 1. NP budovy. V této části budovy dochází k častým teplotním změnám. V praktické části bude řešením výměna spolehlivějším PIR detektorem.

Dle mého názoru PZS není dostatečný. V 1. NP jsou velké prosklené plochy, chybí akustické detektory rozbití skla. Zvažovala bych také akustickou signalizaci a v oblasti recepcie tísňovou signalizaci.

3.2.5 Kódovací systém

Zabezpečovací systém pracuje ve dvou základních fázích arm (PZS zapnutý) a disarm (PZS vypnutý). Fáze jsou dány režimovým opatřením firmy. Pracovník bezpečnostní služby vždy před příchodem a po odchodu zaměstnanců budovu kóduje. Součástí přístupového systému je tedy také rozdělení kódů. Přístupové kódy vlastní pouze určitý počet zaměstnanců, ostatní zaměstnanci mají umožněný přístup do budovy pouze v pracovní dny v době od 6:30 do 17:30.

Kódovací systém je rozčleněn do čtyř podsystémů 0,1,2,3.

Podsystém 0 zahrnuje kódování celé budovy. Toto je umožněno jedinému pracovníku společnosti, který vlastní tzv. master kód. Do podsystému 1 je zařazena administrativní část budovy. V tomto případě vlastní svůj kód management firmy. Do podsystému 2 patří sklad, držitelé kódů jsou 2 vedoucí pracovníci skladu. Podsystém 3 tvoří zázemí pracovníků ADM (byt) s vlastním vchodem a klávesnicí. Držiteli kódů je 13 osob.

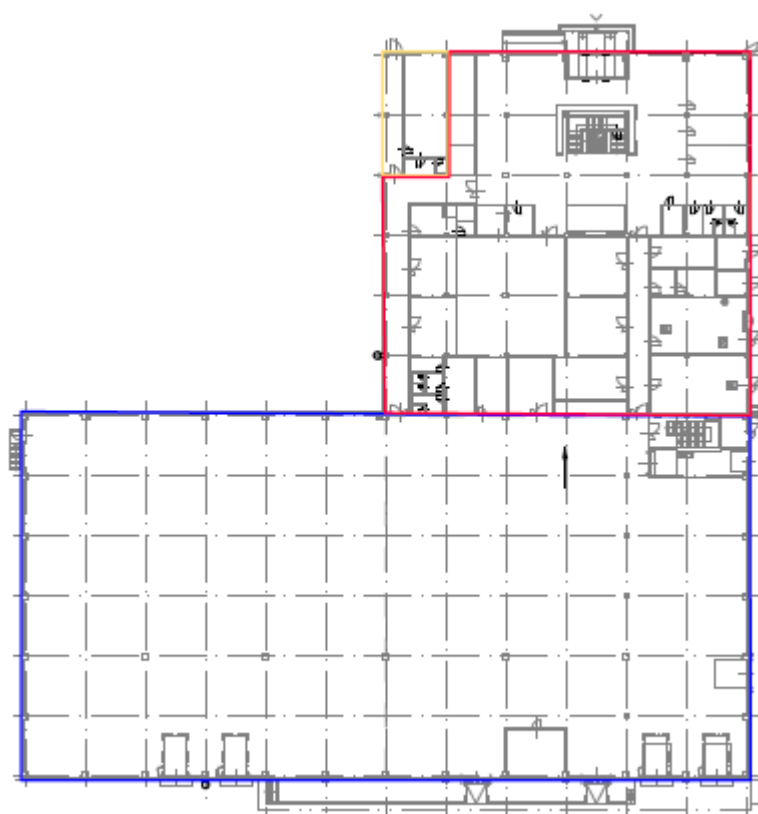
Na obrázku č. 11 je vidět barevné rozdělení do subsystémů:

0 - master kód

1 - administrativní část budovy

2 - sklad

3 - zázemí ADM



Obr. č. 11 Subsystemy budovy firmy

V kódovacím systému vidím 3 základní nedostatky:

1. Problém v kódování nastává zejména u pracovníků skladu, kteří v případě nutnosti příchodu do skladu v jinou než pracovní dobu, musí kromě skladu také odkódovat administrativní část budovy, protože v budově jsou přístupné pouze 2 klávesnice a to v administrativní části a v části zázemí pro ADM.
2. Další nedostatek vidím v tom, že každý držitel kódu se může dostat do všech kanceláří a místností v budově, mimo kanceláře managementu, pokud nejde zrovna o management firmy. Velký problém vidím v dostupnosti těchto osob do místnosti serveru, kde je umístěné jádro bezpečnostního systému.
3. I přes fluktuaci zaměstnanců ve firmě je novým pracovníkům přiřazený stejný kód jako měl pracovník předešlý. Od počátku je mezi pracovníky rozděleno 20 kódů.

3.3 Kamerový systém

Pro zvýšení úrovně bezpečnostní ostrahy areálu a rovněž pro potřebu provozu je ve firmě instalován kamerový systém Siemens s kamerami, které v denním režimu pracují s barevným obrazem v nočním režimu v černobílém provedení obrazu. Budova je osazena 10 kamerami CCB5 1345- CP, které sledují pouze plášť budovy, jsou nastaveny na trvalý záznam. Kamery jsou statické, s pevným objektivem typu CLVM a s pevnými konzolami, bez infrapřisvitu. Pro ochranu proti povětrnosti jsou osazeny ve venkovních temperovaných krytech. Obrazový signál kamer je soustředěn na Video monitoru LCD CMCT 1720 umístěném v servrovně. Firma využívá digitálního záznamového zařízení SISTORE AX 16. Jedná se o flexibilní zařízení se snadnou instalací a následnou obsluhou. Má snadný přístup k obrazovému záznamu a účinné vyhledávací funkce. Mezi hlavní přednosti tohoto zařízení patří nahrávání rychlosti až 100 snímků za sekundu, efektivní MPEG4 videokomprese, intuitivní ovládání, přenosy LAN, možnost integrace se systémem kontroly vstupu, sledování a vyhledávání s použitím RAS, integrované ovládání funkcí kamer PTZ, triplexní provoz, několik možností uchovávání záznamu.

Velkou nevýhodou dosavadního systému je, že jsou kamery statické a sledují pouze plášť budovy. Díky tomuto nastavení nebyl žádný viditelný záznam krádeže, který v minulosti proběhl. Digitální ústředna i LCD monitor budou využité při návrhu nového kamerového systému, jelikož splňují všechny požadavky potřebné k funkčnosti nového systému.

3.4 Přístupový a docházkový systém

Pro řízení, kontrolu, zpracování pohybů a přístupů osob je ve firmě zabudovaný systém ACCESS, který pracuje na principu identifikačních karet s využitím podpůrného hardwaru (zejména různých typů snímačů, identifikačních karet) a souboru programových modulů na příslušných počítačích.

Každý zaměstnanec firmy má svou vlastní bezdotykovou identifikační kartu, která slouží ke vstupu do areálu, vstupu do budovy firmy a také k přístupům do kanceláří. Hlavní vstupy do objektu jsou osazeny čtecími hlavami RFID, dle potřeby typem H PRO nebo H PRO/K, u příjezdové posuvné brány je navíc instalované dorozumívací zařízení Helios Intercom. V budově jsou přístupy do kanceláří umožněny pomocí čtecí hlavy H PRO/WE.



Obr. č. 12 Bezkontaktní čtecí hlava H PRO, H PRO/K a H PRO/WA [15]

ACCESS je integrován s docházkovým systémem PASSPORT na úrovni společné databáze, shodných komunikací se snímáči a předáváním docházkových dat o průchodech pro zpracování v rámci evidence docházky. V oblasti recepcce a bočního výstupu je umístěný docházkový terminál REI ST s grafickým displejem a klávesnicí, kde každý zaměstnanec zaznamenává svou docházkovou činnost. Mezi základní docházkové akce řadíme příchod, odchod, přestávku na oběd, návštěvu lékaře, služební cestu, dovolenou nebo další naprogramované akce jako je např. jazykový kurz nebo kuřácká pauza.



Obr. č. 13 Ukázka přístupového terminálu [16]

Výsledná data zpracovaná systémem PASSPORT jsou vyhodnocovaná v tzv. modelu pracovní doby. Ve firmě používají intranetový model zpracování docházky WATT. WATT řeší okruh zpracování vyhodnocení docházky, její editace, případně tisky výsledných dat, definice modelů a jejich nastavení v systému PASSPORT. Na docházkový systém je navázaný stravovací systém CARDPAY. Je založen na objednávkách jídel podle jídelníčku a jejich odběru v době výdeje v rámci výdejových snímačů. Výdej stravy je většinou realizován prostřednictvím snímače s externím oboustranným sedmisegmentovým displejem pro zobrazení čísla objednaného jídla.

Přístupový a docházkový systém měnit nebudeme. Přístupový systém úzce souvisí se rozdělením přístupových kódů. Budeme s tím tedy nadále pracovat.

3.5 Elektrická požární signalizace

V souladu s požárně-bezpečnostním řešením objektu je ve firmě instalován systém elektrické požární signalizace dle ČSN EN 54 (34 2710). Jednotlivé prostory jsou chráněny opticko-kouřovými automatickými hlásiči. Na únikových cestách v objektu jsou instalované tlačítkové hlásiče požáru. Ústředna systému je osazena v servrovně. V případě požáru systém EPS ovládá spuštění zařízení pro odvod kouře a tepla, otevření automatických dveří pro únik osob, vypínání provozní vzduchotechniky a určených rozvodů NN. EPS snímá polohu požárních klapek ve vzduchotechnickém potrubí.

3.5.1 Ústředna EPS

Ve firmě je realizovaná ústředna EPS systému Siemens. Jedná se o ústřednu řízenou mikroprocesorem. Je vybavena potřebným počtem hlásičových linek, vstupů, výstupů pro ovládání navazujících zařízení a systémů. Ústředna slouží k vyhodnocení poplachových signálů z automatických i tlačítkových hlásičů, umožňuje adresování jednotlivých hlásičů nebo skupin hlásičů zapojených do smyček. K ústředně je připojen klíčový trezor a OPPO. V případě výpadku elektrického proudu je ústředna automaticky přepnuta na vlastní náhradní zdroj. Ústředna je napojena na poplachové a přijímací centrum HZS.

3.5.2 Automatický hlásič opticko-kouřový

Opticko-kouřový hlásič reaguje na kouřové zplodiny vznikajícího požáru. Při vniknutí zplodin do měrné komory dochází k lomu světelných paprsků infračervené LED diody na kouřových zplodinách, čímž je vyhlášen poplach. Automatické opticko-kouřové hlásiče jsou osazeny do jednotlivých vytypovaných prostor firmy. Jsou rozmístěny v souladu s ČSN 73 08 75 při stanovení max. plochy na jeden hlásič a maximální vzdálenosti mezi hlásiči a vzdálenosti hlásič-stěna.



Obr. č. 14 Opticko-kouřový hlásič FDOOT221 [17]

3.5.3 Tlačítkový hlásič požáru

Tlačítkový hlásič požáru je určen k ohlášení požáru manuálně osobou, která požár zjistí. Po rozbití sklíčka a zmáčknutí tlačítka je ústředně EPS předán signál o vzniku požáru a zpětně je v tlačítkovém hlásiči signalizováno opticky, že ústředna vyhlášení požáru provedla. Tlačítkové hlásiče jsou ve firmě instalovány zejména na chodbách, schodištích a u východů budovy.



Obr. č. 15 Tlačítkový hlásič požáru FDM223 [18]

3.5.4 Kabelové rozvody a montáž zařízení

Rozvody k hlásičům a vlastním přístrojům EPS musí být propojeny kabely. V našem případě je použitý kabel JE-H(ST)H 2x2x0,8. Kabely jsou umístěny na povrchu v trubkách o průměru 16 mm, případně v kabelových žlabech

3.5.5 Shrnutí EPS

Prostory firmy jsou rozděleny do požárních úseků a do kouřových sekcí. Jsou doplněny o veškeré potřebné prvky nutné pro zajištění požární ochrany. Mimo výše uvedené se jedná o přenosné hasicí přístroje, požární žebříky, klapky pro odvod kouře, požární klapky. Systém EPS firmy je navržen dle potřeb a požadavků firmy v návaznosti na legislativu a normy ČSN. Systém požární ochrany je pro firmu dostačující.

3.6 Zhodnocení stávajícího systému.

V posledních letech je využíváno různých možností integrace poplachových systémů. Pokud navštívíme jakoukoli webovou stránku zejména zahraniční firmy, nabízejí nám integrované systémy PTZS, ACCESS, evidence docházky, výdej stravy s dalšími moduly automatizace, jako je měření a regulace. Za největší výhody těchto systémů jsou považovány modulární řešení s nízkými pořizovacími náklady, centralizované ovládání, přinášející nízké provozní náklady a v neposlední řadě také možnost customizace.

Firmy nabízejí různé možnosti integrace. Jednou z možností integrace je nadřazený PZTS s moduly automatizace. Kromě klasických bezpečnostních prvků obsahují speciální moduly

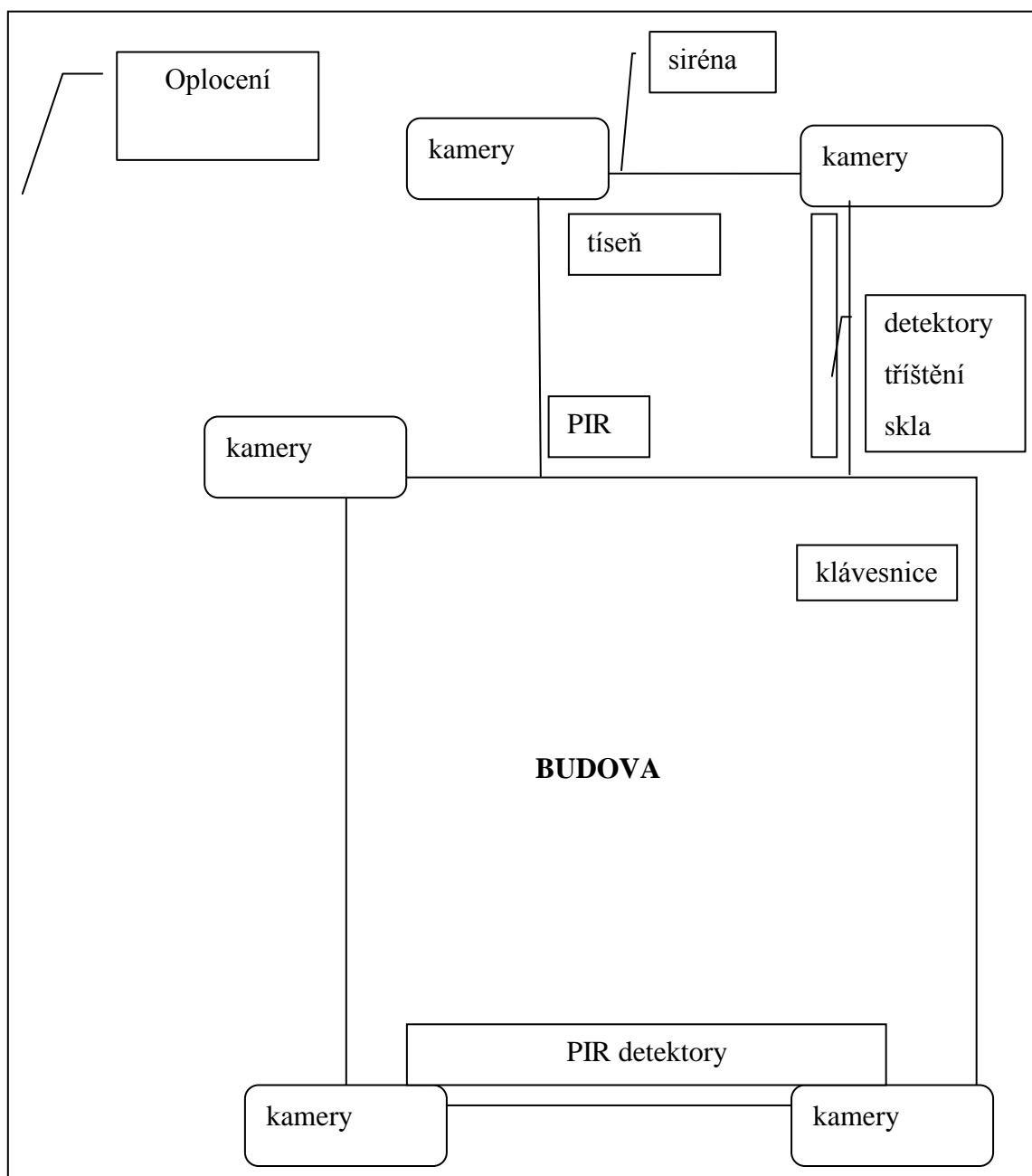
pro ovládání výtahů, klimatizace, vytápění, osvětlení, kontroly vstupu, atd. Nejvýznamnějšími systémy z této kategorie jsou např. systémy Genesis a Concept. Oba pochází z Austrálie. V posledních letech je na trhu prosadil také systém Imperial od Paradoxu z Kanady. Centrem těchto velkých systémů je ústředna. Řídí celkový chod veškeré použité technologie pomocí značného množství různých expandérů a zabezpečuje přímou komunikaci objektu s obsluhou pomocí vlastního vizualizačního SW (místně i vzdáleně). Přednost těchto systémů spočívá v centrální správě informací a technologické jednotnosti použitých prvků. Odpadají také problémy komunikace mezi hlavní ústřednou a vizualizačním SW (tentýž výrobce). Naopak nevýhodou je centrální řízení. V případě poruchy ústředny přestává fungovat veškerá technologie v objektu. Další možností integrace je nadřazený automatizační systém s prvky PZTS. Je v podstatě opakem předchozího systému. Hlavním prvkem je zde PLC automat. Ten zajišťuje řízení veškeré technologie. Zástupcem této skupiny je např. systém Inels. Velká nevýhoda tohoto systému spočívá v tom, že jednotlivé prvky PZTS které jsou sice certifikované dle norem, jsou připojeny na sběrnici, která není z hlediska bezpečnostních systémů nijak atestována, a proto nelze tento systém považovat za plnohodnotný PZTS. Nejvyužívanějšími systémy integrace jsou systémy propojené datovou sběrnici s externí vizualizací tzn. propojení samostatných systémů přes komunikační sběrnici. Systémy se vzájemně neovlivňují a žádný systém není nadřazený, jedná se jen o určení priorit. Správa, řízení i vizualizace je řízena přes nadstavbový software na externí počítač. Tento systém se jeví jako nejvýhodnější. [14]

Všechny subsystémy bezpečnostního systému firmy jsou realizovány zvlášť, je nutné je řídit zcela odděleně, proto se tedy vzájemně negativně neovlivňují, a také žádný z nich není nadřazený nad ostatními. Výpadek některého ze systému neznámá kolaps ostatní použité technologie, což můžeme považovat za výhodné. Musíme brát v úvahu, že investor měl má své důvody, proč nemůže integraci systému využít, proto nebudeme o integraci systému uvažovat.

3.6.1 Identifikované nedostatky

Základní nedostatky v zabezpečení firmy spočívají v nedostatečné perimetrické ochraně. V době uložení materiálu ve venkovních prostorách musí být využíváno pracovníka

bezpečnostní agentury. Tuto službu považuji za dosti neekonomickou. Další negativum spočívá v poplachové zabezpečovací a tísňové signalizaci - časté poplachy PIR detektorů, chybějící akustické detektory tříštění skla, siréna a tísňová ochrana v zázemí recepce. Významný problém vidím v nedokonalém kamerovém systému, který v době uskutečněné krádeže na pozemku nezaznamenal jedinou zprávu o spáchaném činu. Uvažovat bychom určitě měli také změně přístupů a kódování firmy.



4 STUDIE PROVEDITELNOSTI NOVÉHO SYSTÉMU

V následující kapitole se zaměřím na možnosti inovace stávajícího systému. Průzkumem trhu vyberu vhodná zařízení a navrhnu řešení pro efektivnější zabezpečení firmy, které vychází samozřejmě i z požadavků investora.

4.1 Analýza požadavků na komplexní bezpečnostní systém

Pro návrh nového systému a jeho komponent si musíme nejdříve určit veškerá kritéria, která budou předmětem řešení:

- zvýšit účinnost perimetrické ochrany - signalizace narušení vnějšího pláště areálu
- zvolit jiný typ PIR detektoru - signalizace nedovoleného pohybu v budově firmy
- doplnit PZTS o akustický detektor tříštění skla - signalizace vniknutí do prostor budovy firmy
- doplnit PZTS o venkovní sirénu - signalizace nedovoleného pohybu v areálu firmy
- doplnit PTZS o tísňový hlásič do zázemí recepce - signalizace napadení obsluhy recepce
- nový kamerový systém CCTV - monitoring a signalizace neoprávněného pohybu v objektu
- inovace v procesu přístupů a kódování

4.2 Perimetrická ochrana

Jedním z nejslabších článků zabezpečení ochrany objektu je perimetrická ochrana - její oplocení. Pro zvýšení ochrany navrhuji využít otřesových čidel nainstalovaných na oplocení. Otřesová čidla zachytí jakékoliv narušení plotu, je tedy velmi obtížné tuto ochranu překonat. Další variantou může být plotový systém založený na vyhodnocení mechanických ruchů pomocí senzorického kabelu.

4.2.1 Perimetr Locator

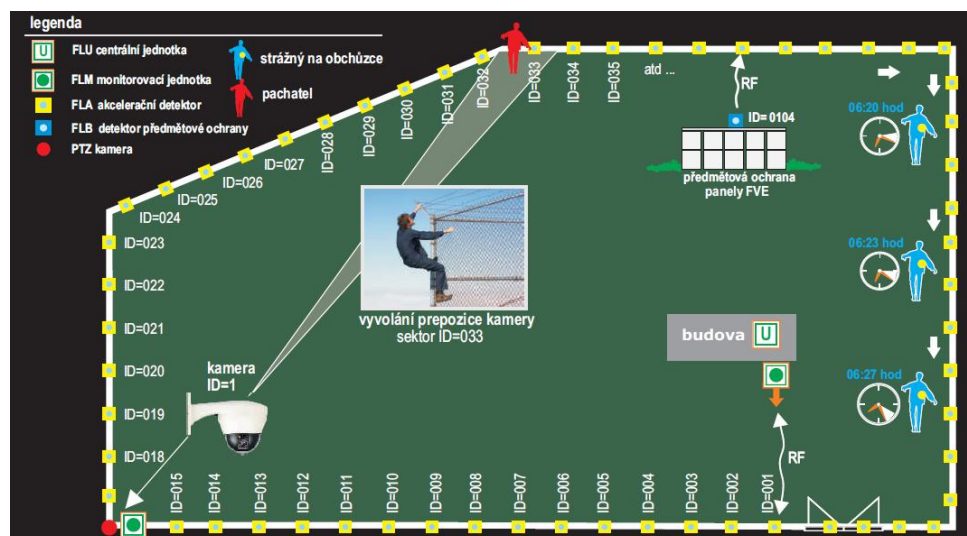
PerimetrLocator umožňuje střežení plotu pomocí speciálních akceleračních RFID tagů připevněných na pletivu a vratech. Akcelerační RFID tagy nevyžadují napájení a jejich

životnost je min 10-15 let. Díky tomu, že systém nevyžaduje vůbec žádnou kabeláž, je instalace extrémně snadná, rychlá a hlavně nenákladná. Je vhodný pro všechny typy plotů a vrat a také pro všechny typy a tvary perimetru. Má velmi vysokou odolnost proti rušení a není mu přiřazována ani jedna z nevýhod konvenčních (kabelových) perimetrických systémů. Na plot se umístí pouze akcelerační detektory FLA. Monitorovací jednotka FLM komunikuje s RFID detektory FLA, s nejnižší a nejvyšší ID adresou. Jednotka FLM je propojena s centrální jednotkou FLU, prostřednictvím které se systém konfiguruje. Systém podporuje prostřednictvím modulu FLE také propojení s jakoukoliv EZS ústřednou. Modul FLE má 6 log. vstupů a 16 logických dvojic vyvážených EOL výstupy. Ústředna PTZS posílá perimetrickému systému informace, které oblasti mají být střeženy a naopak perimetrický systém posílá prostřednictvím logických výstupů do EZS informaci, v kterých oblastech byl narušen perimetr, sabotáže, poruchy. [19]

Akcelerační detektory perimetrické ochrany snímají časové a dynamické změny v poloze pletiva, které jsou typické pro přelézání plotu narušitelem. Díky paralelnímu vyhodnocování signálu, umí systém eliminovat falešné poplachy způsobené větrem, deštěm či krupobitím. Detektory FLA mají v sobě sofistikovaný algoritmus analýzy pohybu ve 3 osách, díky kterému umí detekovat jakoukoliv snahu o odcizení detektoru nebo jeho sabotáž demontáží a to i v denním (DisArm) režimu. [19]

Systém Perimetr Locator umí komunikovat se všemi typy PZTS ústředen, tedy i ústřednou instalovanou ve firmě. Umožňuje realizovat také předmětovou ochranu střežení věcí uvnitř perimetru díky akceleračním RFID tagům FLB. Této možnosti však v našem návrhu nevyužijeme. Naopak využijeme možnosti naprosto přesného navádění průmyslových PTZ kamer na místo incidentu s přesností $\pm 2\text{m}$. [19]

Uvedený popis můžeme považovat jako velké výhody tohoto systému. Nevýhodu jsou vyšší pořizovací náklady, přestože bychom ušetřili za kabeláž.



Obr. č. 16 Ukázka základní dispozice perimetrické ochrany [19]

4.2.2 Maximum Guard

Perimetrický zabezpečovací systém Maximum Guard určený pro střežení obvodového oplocení a venkovních prostor. Mechanické ruchy jsou vyhodnocovány pomocí senzorického kabelu KeyTech.



Obr. č. 17 Senzorický kabel KeyTech [20]

Poplach je vyvolán v případě, že se narušitel pokusí:

- přelézt přes plot
- prostříhat pletivo
- nadzvednout pletivo nebo konstrukci plotu
- vstoupit do střeženého prostoru

Systém se skládá z vyhodnocovací jednotky KeyFORCE nebo GeFORCE II řídicí ústředny Station One. V menších aplikacích se může vyhodnocovací jednotka použít samostatně, při náročnějších, rozsáhlejších aplikacích využijeme sběrnice systému RS485 řídicí ústředny a vyhodnocovací jednotky. Obě jednotky, jak KeyFORCE, tak KeyMASTER můžeme integrovat s jiným systémem pomocí reléových výstupů [20]

Výhody tohoto systému

- vysoká odolnost proti planým poplachům
- ochrana proti elektromagnetickému a rádiovému rušení
- stejná citlivost po celé délce střežené zóny
- jednoduchá a snadná instalace

4.2.3 Vyhodnocení

Doporučuji využít systému Perimetr Locator. Jelikož budeme měnit i kamerový systém, je dobré využít vlastnosti navádění kamer na místo narušení.

4.3 Signalizace nedovoleného pohybu, časté poplachy

V oblastech budovy, kde dochází k častým falešným poplachům, bych doporučila výměnu stávajících pasivních infračervených detektorů DG55 za PIR detektory **IR120C** od firmy Siemens, které mají diskrétní ergonomické provedení a hodí se do každého prostředí. Vyznačuje se velmi dobrou odolností proti pohybu domácích zvířat. Disponuje funkcí pokročilého vyhodnocování signálu. Detektor IR120C považuji za ideální řešení pro obytné i menší komerční objekty.

Základní vlastnosti [21]:

- dosah 12 m při použití zrcadla s vějířovou charakteristikou nebo 20 m při použití záclonového zrcadla
- necitlivost na pohyb domácích zvířat do 40 kg
- pravá teplotní kompenzace
- digitální obvod vyhodnocování signálu AMASIC

- účinné filtrování bílého světla prostřednictvím optické soustavy s triplexním zrcadlem
- výběr ze čtyř nastavení citlivosti, indikace krokového testu LED



Obr. č. 18 PIR detektor IR120C [21]

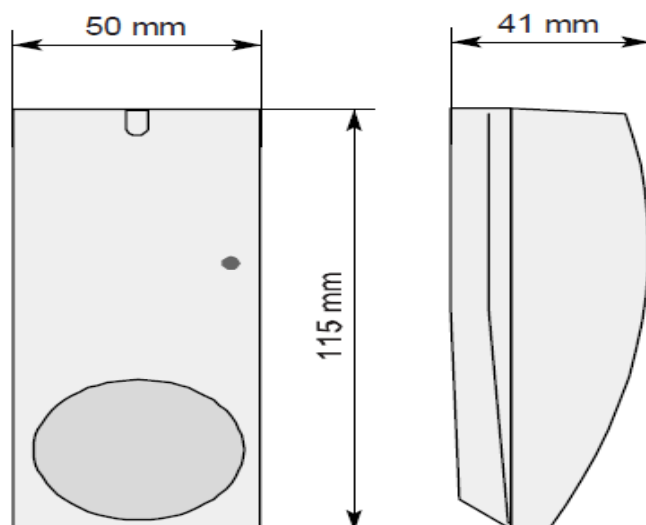
Výhodou IR120C je [21]:

- *snadná a bezpečná instalace* - univerzální kryt detektoru je uzpůsoben pro přímou montáž na stěnu, pod úhlem 45° i v rozích, a to bez použití dalších montážních součástí.
- *vynikající odolnost* - stoprocentní účinností detekce doprovázena vysokou odolností proti vlivům okolního prostředí.
- *bezpečná detekce* - optická soustava s triplexním zrcadlem, která je rozdělena do 52 zón, zaručuje vysoce spolehlivou detekci, systém analýzy signálu využívající více kritérií inteligentně a spolehlivě rozlišuje mezi vetřelci a rušivými signály

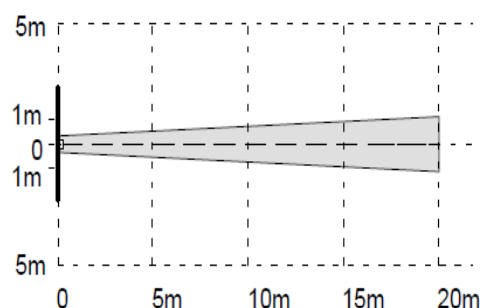
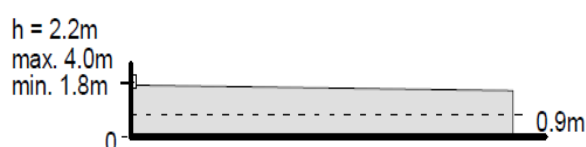
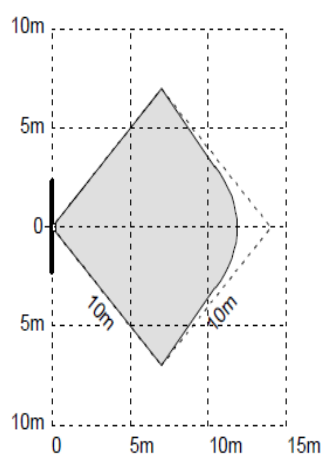
V následující tabulce jsou uvedeny technické údaje detektoru IR120C. Následují obrázky s rozměry a oblastí pokrytí.

Tabulka 3 Technické údaje IR120C 1 [21]

PIR IR 120C	
Napájecí napětí (12 V jmen.)	8,0 ... 16,0 V _{ss}
– Max. zvlnění (0–100 Hz)	2,0 Všpičkové
– Kontrola napětí	Výstraha při < 6,0 ... 8,0 V
Odběr proudu (při 8,0–16,0 V _{ss})	
– Klidový stav / při poplachu (LED)	6 mA / 6 mA
Poplachový výstup, kontakt relé	30 V _{ss} / 100 mA / R _i < 33 _
Sabotážní kontakt	30 V _{ss} / 50 mA
Vstupy kontrolních signálů (průchodový test)	nízká ≤ 1,5 V / vysoká ≥ 3,5 V
Rychlost chůze	
– Vějíř / záclonové zrcadlo, IRS122	0,2 ... 3,0 m/s / 0,2 ... 4,0 m/s
Odolnost proti pohybu domácích zvířat	< 20 kg
– při použití maskovacího klipu IRMC104	< 40 kg
Provozní teplota	–20 ... +55 °C
Skladovací teplota	–20 ... +60 °C
Vlhkost (EN60721)	< 95 % rel. vlhkost, bez kondenzace
Odolnost proti EM rušení do 1 GHz / 1–2 GHz	> 30 V/m / > 10 V/m
Krytí (EN60529, EN50102)	IP41 / IK02
Třída prostředí podle VdS	II
Schválení, třída B podle VdS	Č. G 101521
– Za použití IRS122	Č. G 101524



Obr. č. 19 Rozměry IR120C [21]



Obr. č. 20 Oblast pokrytí IR120C [21]

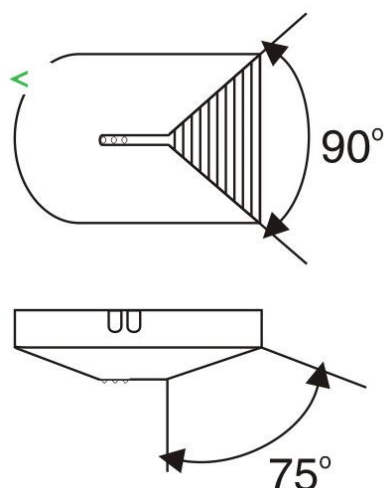
4.4 Akustický detektor tříštění skla

Pro ochranu vniku do budovy přes skleněné plochy byl zvolen moderní digitální detektor rozbití skla **GLASSTREK 457**. Využívá pokročilou technologii detekce a identifikace tříštění skla. Detekce je založená na analýze tlakové vlny vzniklé prolomením skleněné plochy a na analýze následného tříštění skla. Výstup detektoru poskytuje zapojení NC zóna s relé pro klasické instalace. Detektor lze provozovat ve dvou režimech citlivosti s

dosahem 4,5 nebo 9 m. Hlídaná skleněná plocha musí být větší než 40 x 60 cm, strop musí být nižší než 5 m a místnost musí být větší než 3 x 3 m. Bližší technické parametry jsou uvedené níže v tabulce. [22]

Tabulka 4 Technické parametry GLASSTREK 457 [22]

457 GLASSTREK	
Typ detektoru	digitální audio
Kompatibilita	TESTTREK2 - tester pro testování detektoru
Napájení	11 - 16VDC
Proudový odběr (klid / max)	min. 15 mA, max. 23 mA
Náběh detektoru	po zapojení 4min. testovací režim
Dosah detekce od skla	min 1,2 m, nízká citlivost 4,5 m vysoká citlivost 9 m
Rozměry (š×v×h)	66 x 90 x 25mm
Pracovní teplota	-20 až + 50 °C
Krytí	IP40
Úhel záběru	vertikálně 90°, horizontálně 70°
Testovací režim	ano (odpojení napájení - propojka)
Paměť poplachů	ano
Poplachový výstup	28VDC 100mA
Tamper výstup	28VDC 100mA
Optická indikace	červená/zelená LED
Barva krytu	bílá



Obr. č. 21 Úhle záběru GLASSTREK 457 [22]

Detektor rozbití skla navržený pro profesionální zabezpečovací aplikace. Přístroj prošel 100% kontrolou kvality, což garantuje správnou funkčnost a dlouhodobou spolehlivost. Inovovaný detektor obsahuje nejmodernější detektor zvuku rozbití skla a podzvukovou rázovou analýzu v plném spektru. Detektor umí rozeznat charakteristický zvuk při rozbití skla. Plynulé nastavení citlivosti umožní vyloučení falešných alarmů. [22]



Obr. č. 22 GLASSTREK 457

4.5 Tísňový hlásič k signalizaci napadení obsluhy recepce

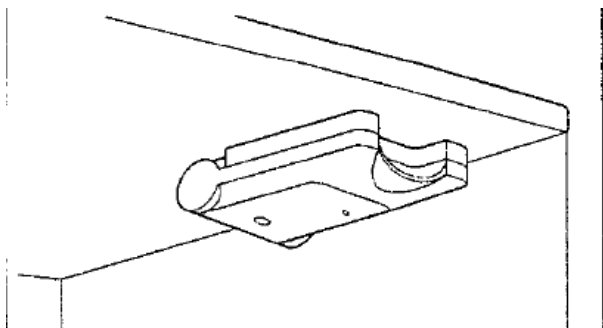
Pracovníci firmy byli upozorněni policií na zvýšenou kriminalitu v okolí objektu. Nejen z toho důvodu navrhuji instalaci tísňového hlásiče do zázemí recepce, kde dochází k nejvyšší

frekvenci osob a je zde také předpokládána manipulace s penězi. Za přiměřené považují skryté nouzové tlačítko napojené přes ústřednu na poplachové přijímací centrum. Z nabízených produktů byl vybrán výklopný tísňový spínač s pamětí poplachu **S 3040**. Elegantní výklopné tlačítko pro instalaci na zeď nebo hranu stolu. Jeho aktivace je velmi tichá což poskytuje osobám větší pocit bezpečí. [23]

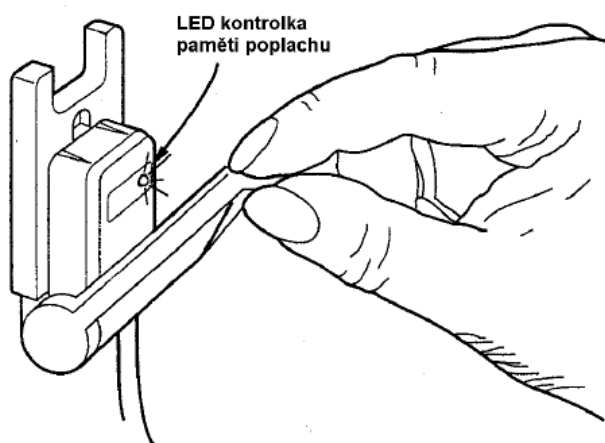


Obr. č. 23 Výklopný tísňový hlásič S 3040 [23]

Tlačítko se nejčastěji montuje na spodní hranu stolu, avšak podle pracovních zvyklostí uživatele a v jeho dosahu ale tak, aby nebudil pozornost. Neměl by být normálně vidět. Tísňový spínač musí být upevněn ve svislé nebo vodorovné poloze tak, aby LED indikace paměti aktivace nebyla zastíněna nějakou překážkou. Pokud je rameno otevřeno mezi 20° - 45 °, přepne se přepínací poplachový kontakt a rozsvítí se LED indikace paměti poplachu. [23]



Obr. č. 24 Ukázka umístění na spodní stranu desky [23]



Obr. č. 25 Spuštění S 3040 [23]

Tabulka 5 Technická specifikace S3040 [23]

Výklopný tísňový hlásič S3040	
Jmenovité napájení	12V ss / 6 mA
Pracovní napětí	7 až 15 V ss max. 8 mA
Rozsah pracovních teplot	-18 °C až 48 °C
Hmotnost	43 g
Rozměry	š 45 x d 73,7 x v 19,3 mm

Výhody tísňového spínače s pamětí poplachu S3040 jsou zejména v jednoduchém ovládání, v aktivaci tichého poplachu a v paměti poplachu.

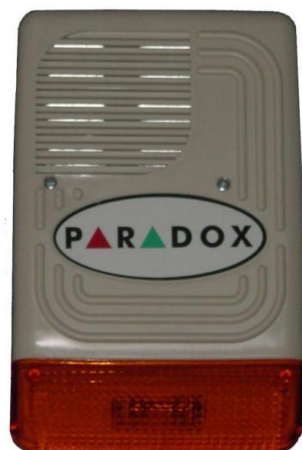
4.6 Venkovní siréna

Pro objekt byla zvolena venkovní zálohovaná siréna řízená mikroprocesorem **Paradox PS-128**. Na trhu byla označena za špičkový výrobek mezi zálohovanými sirénami a to zejména proto, že je opatřena výstupem Report, ten předává do ústředny informace o stavu baterie, reproduktoru a světla. Obsahuje servisní vstup sirény, který přepíná sirénu do servisního módu, ve kterém lze sirénu bezpečně otevřít a jakkoliv s ní manipulovat. Mód úspory

energie zabraňuje úbytku na zvukové a světelné intenzitě a prodlužuje životnost baterie. Pokud je při první montáži nízké napětí na baterii, siréna vás na to upozorní tichým dlouhým signálem a nezačne pracovat, dokud baterie nebude poskytovat požadované napětí. Siréna ohlašuje poplach pomocí zvukové a světelné signalizace. Díky zvukové charakteristice varovného signálu je tento zvukový signál daleko silnější než u sirén s podobným výkonem, přičemž doba znění sirény je maximálně 3,5 minuty. [24]

Základní vlastnosti sirény [24]:

- Siréna je uložena v protipožárním krytu, který má vnitřní ocelovou krabici upravenou proti násilnému vniknutí a odtržení
- Balení obsahuje předvrtávací šablonu pro upevnění
- Vysoce efektivní reproduktor o výkonu 40 W
- Vlastní testování řízené mikroprocesorem
- Vydává hlasitý zvukový efekt 128 dB / 900 - 2400 Hz
- Speciální funkce blikání pro zvýšení poplachového efektu
- Testování stavu baterie, žárovky a reproduktoru
- Servisní vstup a servisní funkce určené pro instalaci
- Obsahuje mód na úsporu energie a šetření baterie
- Chráněné vstupní svorky
- Několik různých zapojení pro nahrazení starších typů sirén
- Kryt z vysoce kvalitní stálobarevné a mechanicky odolné hmoty



Obr. č. 26 Paradox PS - 128 [24]

Technická specifikace sirény je uvedena v tabulce níže, montážní návod je připojen v příloze P

Tabulka 6 Technická specifikace Paradox PS-128 [24]

PARADOX PS – 128	
Rozměry: 295/200/100 mm	12V ss / 6 mA
Váha	3 kg
Krytí	IP 34
Napájení	13,6 – 14,8V
Baterie	12V / 1,2 až 7,0 AH
Typ světla	12V / 18 W
Odběr při klidovém stavu	5 mA
Průměrný odběr reproduktoru	1,2 A
Maximální odběr	2,8 A
Hlasitost sirény	128 dB
Zvuková frekvence	900 – 2400 Hz
Maximální doba spuštění sirény	3,5 min.

Zapínací polarita	+ / - (dá se nastavit)
Délka zapínacího pulsu	200 ms minimálně
Aktivování spínače světla	zápornou hodnotou, 200ms minimálně
Výstup zpráv	Maximálně 200 mA
Typ výstupu zpráv	N.O. (v klidu otevřeno)
Typ ochranného kontaktu	N.C. (v klidu zavřeno)

4.7 Kamerový systém CCTV

Přestože je na budově firmy nainstalováno 10 kamer, ani jedna z nich nezaznamenala akci krádeže v areálu firmy, proto byla nově zvolená otočná kamera PTZ LG Electronics LT903PB. Dalším kritériem volby této kamery bylo již zmiňované automatické navázání na perimetrický systém PerimerLocator.

Venkovní otočná kamera LG LT903PB se vyznačuje velkou světelnou citlivostí a velkou rychlostí při otáčení. Mezi její základní vlastnosti patří [25]:

- Vestavěný optický zoom x37 - umožňuje plynulou změnu ohniskové vzdálenosti v rozsahu $f = 3,5 - 129 \text{ mm}$
- Optická část - CCD čip velikosti $1/4''$ s rozlišovací schopností 540 TV řádků
- Citlivost od 0,0001 (v B/W modu) - vychází z funkce pokročilého DSP procesoru
- Digitální zoom x12
- Až 62dB WDR, HSBLC
- Funkce Den/Noc automaticky na základě vyhodnocení intenzity světla
- 8x alarmový vstup / 4x alarmový výstup
- Horizontální pohyb: $0^\circ \sim 360^\circ$, Max $240^\circ/\text{Sec}$
- Vertikální pohyb: $0^\circ \sim 180^\circ$, Max $240^\circ/\text{Sec}$
- 8 soukromých oblastí, 128 nastavitelných pozicí

- Komunikace po RS485
- Komunikační protokoly Pelco D, Pelco P a LG Multix



Obr. č. 27 LG LT903PB [25]

Tabulka 7 Technická specifikace LG LT903PB [25]

LG LT903PB	
Model	LT903N/P
Systém	NTSC/PAL
Snímací zařízení	1/4 EX-view HAD CCD
Celkový / Efektivní počet pixelů	NTSC - 410K / PAL - 470K
Počet řádků	540 TV Line
Objektiv	x37 Zoom, F1.5(W) F4.1(T), f=3.5mm~129mm
Poměr S / N (signál / šum)	Více jak 50dB (AGC off)
Den a Noc	Den / Noc / Auto
Minimální osvětlení	Color: 0.003 (0.6, Sens-up off) B/W: 0.0001 (0.1, Sens-up off)
Digitální Zoom	x12
Sync System	Interní
Vyvážení bílé	Auto/ATW/One Push/Manual(1800k~10,500K).

Zapínací polarita	+ / - (dá se nastavit)
Ovládání	RS-485
EIS	Ano (elektronická stabilizace obrazu)
Alarm vstupy	8 Kanálů
Video výstup	Composite Output 1Vp-p(75Ω Terminated))
Uzávěrka	NTSC: 1/60 ~ 1/90,000 Sec PAL: 1/50~1/90,000 Sec
Flickerless Mode	Dostupný
Ovládání clony	Auto/Ruční
Široký dynamický rozsah	Duální závěrky (62dB) / HSBLC
Horizontální pohyb	0°~360°, Max 240°/Sec
Vertikální pohyb	0°~180°, Max 240°/Sec
Privátní zóny	8 nastavitelných oblastí
Předvolby	128 Pozicí/ 256
Záznam pohybu	Max 8 minut
Skupiny prepozic	Max 9 skupin
Provoz teplota / vlhkost	-25°C ~ 55°C, 0%RH~60%RH
Skladovací teplota / vlhkost	-30°C ~ 60°C, 0%RH~85%RH
Napájení	AC 24V
Spotřeba energie	Max. 20W
Rozměry (øx D)	Ø230 mm x 332 mm(H)
Hmotnost	cca 3.3Kg

4.8 Kódovací systém

Přestože je systém rozdělen do podsystémů, není kódování těchto zón dodrženo. Pracovníci skladu musí kódovat část skladu z administrativní budovy, protože v této části je instalovaná klávesnice. Proto, aby byl systém kódování dodržen, navrhuji instalaci další klávesnice do vstupních prostor skladu. Použijeme dosud instalované klávesnice Digiplex DGP2 - 641 BL, o níž je zmínka již v kapitole 3.2.2.



Obr. č. 28 Digiplex DGP2 - 641 BL [26]

Základní vlastnosti této klávesnice jsou [26]:

- 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

Tabulka 8 Technická specifikace Digiplex DGP2 - 641 BL [26]

Digiplex DGP2 - 641 BL	
Napájení 9 - 16V	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 stavu AC	READY
Rozměry	145x122x34 mm

4.9 Shrnutí nově zvolených prvků PTZS

V kapitole 4 jsme se seznámili podrobněji se zvolenými komponenty, které využijí k proveditelnosti nového systému. Všechny uvedené prvky byly zvoleny jak podle potřeb vyššího zabezpečení, tak podle požadavků investora. Nejvyššími parametry pro volbu těchto komponentů byly jejich technické vlastnosti, možnost propojení se stávající ústřednou, reference jiných firem i servisních techniků bezpečnostní služby.

4.10 Návrh řešení

Navrhuji instalaci výše popsaných prvků dle výkresů v elektronické příloze.

- Perimetr Locator v celém obvodu oplocení
- 5 kusů PTZ kamer s nastavením na navádění na místo narušení za použití Tracking Box MF-AT100, s napojením na stávající digitální zařízení a pult centrální ochrany
- vybraného typu sirény s napojení ústřednu

- tísňového hlásiče s napojením na ústřednu
- detektoru tříštění skla
- PIR detektorů
- klávesnice
- rozdělení kódů zaměstnancům firmy dle nové číselné řady

5 ASPEKTY REALIZACE NOVÉHO SYSTÉMU

Cílem této kapitoly je stručný popis možného způsobu možné realizace jednotlivých subsystémů PZTS. Součástí také bude zhodnocení nového systému po stránce funkční, technické i ekonomické.

5.1 PerimetrLocator

Na oplocení firmy by bylo zapotřebí 75 detektorů FLA, které se za pomoci montážních dílů instalují svisle dolů na pletivo. Oplocení se musí osadit monitorovací jednotkou FLM, která komunikuje s detektory. Monitorovací jednotka musí propojena s centrální jednotkou FLU (sběrnice RS-485) umístěnou uvnitř budovy. Tato zařízení je nutná propojit čtyřpárovým stíněným kabelem typu LYNX FTP 4x2x0,5. Následně je zařízení připojeno na ústřednu PTZS. Výše uvedené parametry mohou sloužit k vypracování poptávky a k realizační dokumentaci.

5.1.1 Technické a funkční zhodnocení

Z technického hlediska vidím tento systém jako velmi podařený, moderní a nadčasový. Jeho velkou výhodou je snadná instalace, jelikož není zapotřebí kabeláže. Použité FLA detektory jsou bezúdržbové a díky krytí odolávají povětrnostním podmínkám a různým klimatickým vlivům. Veškeré technické a funkční parametry jsou popsány v kapitole 4.2. Co se týče funkčnosti systému, z vlastní zkušenosti ji nemůžu posoudit, ale z informací dostupných na internetu se tento systém pyšní vysokou spolehlivostí zabezpečení prostor. Je zařazený do stupně zabezpečení 3.

5.1.2 Ekonomické zhodnocení

Systém PerimetrLocator byl navržen k posílení perimetrické ochrany, zejména z důvodu nutnosti zaměstnávání fyzické ostrahy v době umístění materiálu ve venkovních prostorech firmy. Požadavkem investora bylo navrhnout možné technického řešení namísto zaměstnávání lidí navíc, což je finančně náročné. Dalším aspektem poptávky po technickém řešení je plánované rozšíření firmy o výrobní halu, což vede investora k zamyšlení nad vyšším zabezpečením firmy. Pokud byla fyzická ostraha zajišťována celoročně v době, kdy se v areálu nenacházejí lidé, cena by se vyšplhala cca na 250 000

korun za rok. Cenová kalkulace technického řešení PerimetLocator vychází asi na 280 000 CZK. Pořizovací cena je sice vysoká, ale odpovídá kvalitě zabezpečení na několik let.

5.2 Kamery LG Electronics LT903PB

V případě realizace výměny kamer kamerového systému je zapotřebí věnovat se zapojení modulů pro automatické sledování pohybu takzvaný tracking box, který analyzuje pohyb v obraze z kamery, dále pak je nutné věnovat pozornost ovládacího pohybu kamer, tudíž je nutné použití UTP kabelu. Ostatní zařízení, jako je monitor a záznamové zařízení SISTORE AX 16, by byly dále využity. V tomto případě by nejvíce stála 5 kamer, tracking boxu a ovládací kabeláže. Cenová kalkulace vychází přibližně na 240 000 CZK. V tomto případě jde opět o vyšší prvotní investici s časovou návratností s ohledem na vynikající bezpečnostní parametry.

5.3 PIR detektory IR 120C

PIR detektory IR120C byly navrženy jako řešení častých poplachů stávajícího zabezpečení. V tomto případě se investor rozhodl tyto detektory použít. V současné době probíhá realizace. Byla kontaktována bezpečnostní agentura zajišťující servis PTZS. Firma se dohodne na základě poptávky o dodání a instalaci těchto čidel. Výměna je efektivní nejen z praktického, ale i finančního hlediska - nebude neustále platit za příjezdy bezpečnostní agentury v případech falešných poplachů.

5.4 GLASSTREK 457, Paradox PS-128, S 3040

K realizaci by bylo zapotřebí 3 ks detektoru tříštění skla Glasstrek 457, jedenkrát sirénu paradox a jedenkrát Paradox PS-128 a jedenkrát tísňový hlásič S3040. Bylo by nutné kontaktovat firmu zajišťující servis a na základě poptávky uskutečnit dodávku a montáž těchto bezpečnostních zařízení s napojením na ústřednu. V případě tísně S 3040 musí bezpečnostní firma zaškolit pracovníka recepce ohledně manipulace s tímto zařízením. Cenová kalkulace všech uvedených prvků je celkem asi 5100 CZK. Realizace je velmi

reálná. Investor si uvědomuje, že za téměř minimální investici ochrání bezpečně svůj majetek a zejména zajistí bezpečí pracovníků recepce.

5.5 Inovace kódování

K realizaci je zapotřebí instalace klávesnice Digiplex DGP2 - 641 BL do prostor přístupu skladu. Cenová kalkulace za zařízení je asi 2900 CZK. V tomto případě opět stačí za pomoci poptávky kontaktovat stávající firmu poskytující servis investorovi. Ta by zařízení dodala, provedla montáž a instalaci. V tomto případě by také nakonfigurovala do příslušného softwaru novou číselnou řadu a rozdala kódy zaměstnancům firmy, kteří by byly řádně proškoleni, což by také potvrdili svým podpisem na předávacím protokolu. Myslím, si že toto řešení je systémově správné a pomůže investorovi v hodnocení při auditu kvality.

5.6 Shrnutí

Uvedené komponenty a jejich zapojení do stávajícího systému PTZS jsou navrženy podle potřeb i finančních možností investora. Celková cenová kalkulace vychází téměř na 530.000 CZK a naprosto odpovídá kvalitě. Realizací projektu firma posílí zabezpečení majetku, osob i informací a také upraví proces přístupů do firmy., což bylo cílem této studie.

K drobnějším realizacím může firma využít poptávky u stávající zabezpečovací firmy, která provede drobné úpravy v technické dokumentaci, dodá veškeré komponenty, provede montáž a instalaci, následně provede zaškolení zodpovědné osoby a předá předávací protokol. U rozsáhlejšího projektu jako je PerimetrLocator a nový kamerový systém je nutné připravit novou realizační dokumentaci. V tomto případě investor zadá poptávku, kde vydefiniuje požadavky na technické řešení, požadavky na dobu realizace, obchodní podmínky a rozsah zpracování nabídky. Následně jsou nabídky zpracovány a proběhne výběrové řízení, následně se zpravidla provádí definitivní rozhodnutí o realizaci. [28]

ZÁVĚR

Cílem této diplomové práce byl návrh inovace komplexního zabezpečovacího systému firmy na základě zpracované analýzy stávajícího systému firmy.

V obecné části práce jsem popsala předpisy, prostředky a postupy používané v oblasti zabezpečení objektů. Následně jsem provedla analýzu stávajícího zabezpečovacího systému firmy. Přesně jsem specifikovala zabezpečovací systémy firmy, jejich prvky a komponenty. Definovala jsem kladné a záporné stránky stávajícího systému. Mezi největší nedostatky jsem zařadila perimetrickou ochranu objektu a kamerový systém. V zabezpečení firmy jsem postrádala akustickou signalizaci, detektory tříštění skla a tísňovou signalizaci pro obsluhu recepce. Řešila jsem také otázku falešných poplachů v některých částech budovy. Zajímala jsem se o nedostatky v systému kódování budovy a přístupů do objektu nebo částí budovy. S ohledem na potřeby a požadavky investora a zjištěné nedostatky jsem provedla průzkum trhu za účelem volby nových komponent pro každou problémovou oblast. K odstranění uvedených nedostatků jsem zvolila komponenty v patřičném rozsahu a kvalitě. Snažila jsem se vybrat moderní prvky jako je propojení perimetrického systému s automatickým naváděním PTZ kamer na místo narušení perimetru, což považuji za velmi užitečné a zajímavé řešení. U každého prvku jsem uvedla výhody, vlastnosti a technickou specifikaci, kterou prvky disponují. Rámcově jsem navrhla implementaci nového řešení, jež splňuje technické, uživatelské i ekonomické aspekty.

Výsledky diplomové práce považuji za úspěšné. Na jejich podnětech právě probíhají některé úpravy stávajícího stavu a to zejména v oblasti kódování a falešných poplachů. Další myšlenky uvedené v této práci budou zpracovány v prováděcí dokumentaci při rekonstrukci bezpečnostního systému firmy.

Díky této diplomové práci jsem si mohla v praxi ověřit své teoretické znalosti dosažené v průběhu studia. Získala jsem aktuální přehled o technických produktech a službách nabízených na trhu komerční bezpečnosti. Měla jsem možnost zjistit, jak vnímají otázku zabezpečení pracovníci firmy. Jejich případné pochybnosti mě vedly k návrhu řešení, což se podařilo v zázemí recepce.

Tato práce mi poskytla zcela nový komplexní pohled na oblast elektronické zabezpečovací signalizace v průmyslu komerční bezpečnosti

ZÁVĚR V ANGLIČTINĚ

The aim of this thesis was the design of a comprehensive company security system innovation based on processed analysis of existing system of company.

In the general part I describe the rules, means and procedures used in building security. Then I analyze the current company security system. I precisely specified the company security systems, their elements and components. I defined the positive and negative aspects of the existing system. I have included the building perimeter protection and CCTV system amongst the biggest flaws. I missed the acoustic alarm, glass break detectors and emergency alarm service for the reception in company security system. I have dealt with the issue of false alarm in some parts of the building. I was interested in the weaknesses in the coding system of the building and access to the building or parts of building. With regard to the needs and requirements of the investor and the shortcomings I have carried out market research for the purpose of choosing new components for each problem area. To eliminate these shortcomings, I chose the components in the proper range and quality. I tried to choose modern features such as links of perimetric guidance system with automatic PTZ cameras directed to the disruption of perimeter, which I think is very useful and interesting solutions. For each element I have set out the advantages, features and technical specifications, which elements have. Generally I proposed to implement a new solution that meets the technical and economic aspects of the user.

The results of the thesis I consider to be beneficially successful. Thanks to the initiatives, some adjustments of the current situation, especially in the area of coding and false alarms are underway. Other ideas presented in this work will be processed in the implementation documents for the reconstruction of the company security system.

With this thesis, I was able to verify in practice their theoretical knowledge acquired during the study. I got up to date on technical products and services offered on the commercial security market. I had the opportunity to find out how employees perceive the issue of security companies. Their possible doubts led me to design solutions, which managed to reception facilities.

This work gave me a whole new perspective on the complex area of electronic security systems in the commercial security industry.

SEZNAM POUŽITÉ LITERATURY

- [1] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.
- [2] UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Praha: Policejní akademie české republiky, 2005, 229 s. ISBN 80-725-1189-0.
- [3] KŘEČEK, Stanislav a kol. *Příručka zabezpečovací techniky*. Vyd. 3. Blatná.: Cricetus, 2006, 314 s. ISBN 80-902938-2-4.
- [4] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.
- [5] VALOUCH, Jan. *Projektování integrovaných systémů*. Zlín, 2010. Prezentace z přednášky, nepublikované. UTB ve Zlíně
- [6] *Aztech Security Systems Inc* [online]. 2008 [cit. 2012-04-12]. Dostupné z: <http://www.aztech4security.com/>
- [7] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2003, 64 s. ISBN 80-731-8119-3.
- [8] ČSN EN 50131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy: Část 1: Systémové požadavky*. Praha: Český normalizační institut, 2007. 40s.
- [9] ČSN EN 50131-1. *Systémové požadavky*. Praha: Český normalizační institut, 2007. Dostupné z: 2007. 40 s
- [10] *Digitální záznamová zařízení*. Praha, 2008. Dostupné z: <ftp://ftp.asm.cz/ASM/Katalog/CCTV2008-2009/18-23%20-%20DVR.pdf>
- [11] Network Video Recorder. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2012 [cit. 2012-04-28]. Dostupné z: http://en.wikipedia.org/wiki/Network_Video_Recorder
- [12] *VARIANT plus, spol. s r. o.* [online]. 2008 [cit. 2012-04-29]. Dostupné z: <http://www.variant.cz/zbozi/0702-178-evo192-panel>

- [13] *VARIANT plus, spol. s r. o.* [online]. 2008 [cit. 2012-04-29]. Dostupné z: <http://www.variant.cz/zbozi/0701-005-dg55>
- [13] *Základy CCTV*. Praha, 2010. Dostupné z: <http://www.micro.feld.cvut.cz/home/X34Ezs/prednasky/Zaklady%20CCTV.pdf>
- [14] VÁCL, Pavel. *Integrovaný poplachový systém*. Zlín, 2011. Diplomová práce. UTB ve Zlíně Fakulta aplikované informatiky. Vedoucí práce Ing. Jan Valouch, Ph.D.
- [15] COMINFO, a.s. *Čtecí hlava RFID: Bezkontaktní čtecí hlava H PRO, H PRO/K a H PRO/WA* [online]. 2010 [cit. 2012-05-13]. Dostupné z: <http://www.cominfo.cz/cz/kategorie/cteci-hlavy-rfid.aspx>
- [16] COMINFO, a.s. *Docházkový systém PASSPORT: Identifikační systém INFOS* [online]. 2010 [cit. 2012-04-29]. Dostupné z: <http://www.cominfo.cz/cz/kategorie/dochazkovy-system.aspx>
- [17] SIEMENS. *Hlásiče EPS: Multikriteriální hlásič FDOOT221* [online]. 2007 [cit. 2012-04-29]. Dostupné z: https://www.cee.siemens.com/web/cz/cz/corporate/portal/home/infrastructure-cities/IBT/integrované_systemy/pozarni_a_bezpecnostni_systemy/eps/Pages/hlasice_fdo221_fdt221_fdoot221.aspx
- [18] SIEMENS. *Hlásiče EPS: Tlačítkové hlásiče FDM221, FDM223, FDM224* [online]. 2007 [cit. 2012-04-29]. Dostupné z: https://www.cee.siemens.com/web/cz/cz/corporate/portal/home/infrastructure-cities/IBT/integrované_systemy/pozarni_a_bezpecnostni_systemy/eps/Pages/tlacitkove_hlasice_fdm221_fdm223_fdm224.aspx
- [19] MARSYAS DEVELOPMENT. *PerimetrLocator* [online]. 2010 [cit. 2012-04-29]. Dostupné z: http://www.7md.cz/docs/perimetrlocator/Datasheet_Perimetr_Locator.pdf
- [20] INTERNATIONAL DIAMONDS TECHNOLOGY. *Perimetrické zabezpečovací systémy Maxim Guard* [online]. 2010 [cit. 2012-04-29]. Dostupné z: <http://www.diamondtech.cz/plotove-zabezpecovaci-systemy.html>

- [21] SIEMENS. *Pasivní infračervený detektor IR120C* [online]. 2011 [cit. 2012-04-29]. Dostupné z:
http://www.orsec.cz/user/data/slovník/IR120_C/Datasheet_IR120C_CZ.pdfbezpečovací-systemy.html
- [22] KELCOM. *GLASSTREK 457* [online]. 2010 [cit. 2012-04-29]. Dostupné z:
<http://www.kelcom.cz/paradox-glasstrek-457-1674.html>
- [23] KELCOM. *S 3040* [online]. 2010 [cit. 2012-04-29]. Dostupné z:
<http://www.kelcom.cz/sentrol-s-3040-1669.html>
- [24] CLR S.R.O. *PARADOX PS – 128* [online]. 2011 [cit. 2012-05-01]. Dostupné z:
<http://www.cctv-prodejce.cz/navody/ps128.pdf-1669.html>
- [25] EUROSAT CS. *LG Electronics LT903PB* [online]. 2010 [cit. 2012-05-01]. Dostupné z: <http://www.eurosat.cz/3797-lg-electronics-lt903.html>
- [26] EUROSAT CS. *Digiplex DGP2 - 641 BL* [online]. 2010 [cit. 2012-05-01]. Dostupné z: <http://www.eurosat.cz/217-k641-dgp2-641bl.html>
- [27] JABLOTRON. *SA-203 - detektor magnetický kontakt mini samolepící* [online]. 2007 [cit. 2012-05-01]. obrázek ve formátu jpg. Dostupné z:
<http://www.jabloshop.cz/sa-203-detektor-magneticky-kontakt-mini-samolepici>
- [28] HRUŠKA, František. *PROJEKTOVÁNÍ ŘÍDICÍCH A INFORMAČNÍCH SYSTÉMŮ*. 1.vyd. Zlín: UTB ve Zlíně, 2010. ISBN 978-80-7318-979-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AIR	Active infrared detectors - aktivní infračervené detektory
ACS	Acces Control Systém – systém kontroly vstupu
ATS	Alarm Transmission Systems - poplachový přenosový systém.
ADM	pracovník oblastního zastoupení
CCD	Charge-Coupled Device - zařízení s vázanými náboji.
CCTV	Closed Circuit Television - uzavřený přenos televizního signálu.
CMOS	Complementary Metal Oxide Semiconductor – doplňující
ČAP	Česká asociace pojišťoven - volné sdružení pojišťoven
ČSN EN	Česká technická norma přejímající evropskou normu.
DSP	Digital Signal Processing - Digitální signální procesor
DVR	Digital Video Recording - Digitální videorekordér
DOME	Kopulovitý tvar vnějšího ochranného krytu video kamery
EEPROM	Electrically Erasable PROM - Elektricky vymazatelná PROM paměť
EPS	Elektronické požární signalizace
GPS	Global Position System - Globální triangulační systém
GSM	Global System for Mobile communications - Globální systém pro mobilní komunikaci
IR	Infrared (Infrared Radiation) - infračervené záření
MW detektor	Micro Wave Detector - Mikrovlnný detektor
LAN	Lokální síť (počítačová) Local Area Network
LCD	Displej z tekutých krystalů - Liquid Crystal Display
NC	Normally Closed - přirozeně zavřené (stav kontaktů relé)
NO	Normally Open - přirozeně otevřené (stav kontaktů relé)
LED	Světlo emitující dioda - Light Emitting Diode
PIR detektor	Pasivní infračervený detektor - Passive Infrared Detector

VHS	System domácího videa - Video Home System
VRC	Videorekordér - Video Cassette Recorder
PZST	Poplachové zabezpečovací a tísňové systémy
PZS	Poplachový zabezpečovací systém.
PTZ	Pan Tilt Zoom - natáčecí, naklápěcí a přibližovací kamera
PPC	Poplachové přijímací centrum - obdoba jako PCO
DC	Stejnoseměrný elektrický proud
AC	Střídavý elektrický proud
US	Ultrasound detectors - ultrazvukové detektory
WiF	Lokální bezdrátové síť - Wireless LAN
SAS	Social Alarm Systems - systémy přivolání pomoci
Zoom	Objektiv s proměnnou ohniskovou vzdáleností - transfokátor
SW	Software - označuje veškeré programové vybavení PC

SEZNAM OBRÁZKŮ

Obr. č. 1	Integrovaný bezpečnostní systém.....	13
Obr. č. 2	Ukázka techniky integrovaného bezpečnostního systému	14
Obr. č. 3	Blokové schéma sběrníkové ústředny [2]	17
Obr. č. 4	Blokové schéma koncentrátorové ústředny [2].....	18
Obr. č. 5	Ukázka techniky NVR [11]	23
Obr. č. 6	Digiplex EVO 192 [12].....	40
Obr. č. 7	Digiplex DGP2 - 641 BL [26]	41
Obr. č. 8	Magnetické kontakty SA-203 [27].....	42
Obr. č. 9	DG55 (0701-005) - DUAL [13].....	42
Obr. č. 10	DG55 DUAL - oblast pokrytí [13].....	43
Obr. č. 11	Subsystémy budovy firmy.....	45
Obr. č. 12	Bezkontaktní čtecí hlava H PRO, H PRO/K a H PRO/WA [15].....	47
Obr. č. 13	Ukázka přístupového terminálu [16]	47
Obr. č. 14	Opticko-kouřový hlásič FDOOT221 [17].....	49
Obr. č. 15	Tlačítkový hlásič požáru FDM223 [18].....	50
Obr. č. 16	Ukázka základní dispozice perimetrické ochrany [19]	55
Obr. č. 17	Senzorický kabel KeyTech [20].....	55
Obr. č. 18	PIR detektor IR120C [21]	57
Obr. č. 19	Rozměry IR120C [21].....	59
Obr. č. 20	Oblast pokrytí IR120C [21]	59
Obr. č. 21	Úhle záběru GLASSTREK 457 [22]	61
Obr. č. 22	GLASSTREK 457	61
Obr. č. 23	Výklopný tíšňový hlásič S 3040 [23].....	62
Obr. č. 24	Ukázka umístění na spodní stranu desky [23]	62
Obr. č. 25	Spuštění S 3040 [23].....	63
Obr. č. 26	Paradox PS - 128 [24].....	65
Obr. č. 27	LG LT903PB [25].....	67
Obr. č. 28	Digiplex DGP2 - 641 BL [26]	69

SEZNAM TABULEK

Tabulka 1 Seznam kategorií norem poplachových systémů [5]	15
Tabulka 2 Stupně zabezpečení.....	30
Tabulka 3 Technické údaje IR120C 1 [21]	58
Tabulka 4 Technické parametry GLASSTREK 457 [22]	60
Tabulka 5 Technická specifikace S3040 [23]	63
Tabulka 5 Technická specifikace Paradox PS-128 [24]	65
Tabulka 6 Technická specifikace LG LT903PB [25]	67
Tabulka 7 Technická specifikace Digiplex DGP2 - 641 BL [26]	70

SEZNAM PŘÍLOH

Součástí je elektronická příloha 1NPEZS-MODEL. pdf a 2NPEZS-MODEL.pdf