

Komplexní zabezpečení velkoobchodu s nápoji fyzickými a technickými prostředky

Comprehensive security wholesale beverages physical and
technical means

Jan Skovajsa



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Jan SKOVAJSA**
Osobní číslo: **A10020**
Studijní program: **B3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **Komplexní zabezpečení velkoobchodu s nápoji
fyzickými a technickými prostředky**

Zásady pro vypracování:

1. **Popište bezpečnostní rizika v objektu a zpracujte projektový návrh kombinované ochrany objektu.**
2. **Popište prvky fyzické ochrany a jejich realizaci.**
3. **Popište prvky technické ochrany a jejich realizaci.**
4. **Vyřešte přenos signálů na dohledové a poplachové přijímací centrum.**
5. **Předložte konfiguraci služeb a materiálu s cenovou doložkou.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. KINDL, Jiří. Projektování bezpečnostních systémů I. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1
2. Normy řady ČSN EN 50130
3. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4
4. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9
5. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7

Vedoucí bakalářské práce:

JUDr. Vladimír Laucký

Ústav bezpečnostního inženýrství

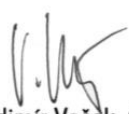
Datum zadání bakalářské práce:

25. února 2013

Termín odevzdání bakalářské práce:

30. května 2013

Ve Zlíně dne 25. února 2013


prof. Ing. Vladimír Vašek, CSc.
děkan




doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Teoretickou částí je čtenář seznámen se základní problematikou týkající se ochrany osob a majetku, stručného popisu a způsobů ochrany. Mezi způsoby ochrany je pak řazeno několik samostatných kapitol, které se věnují jednotlivým typům, mezi které patří fyzická a technická ochrana. Důležitou součástí, která je dále uvedena, jsou informace týkající se dohledových a poplachových přijímacích center.

V praktické části je pak zvolen samotný projektový návrh zabezpečení, ten je rozdělen na několik částí, mezi které v počátku patří popis objektu a bezpečnostní posouzení, z čehož se následně vychází při návrhu zabezpečení. V návrhu zabezpečení je pak logicky zařazena např. klasifikace prostředí, stupeň zabezpečení, volba a rozmístění komponent, způsob připojení na DPPC a další možná rozšíření. Posledním bodem je pak cenový rozpočet.

Klíčová slova: velkoobchod, sklad, fyzická ochrana, technická ochrana, kombinovaná ochrana, zabezpečení, bezpečnost, návrh

ABSTRACT

In the theoretical part of the thesis the reader is introduced to some basic issues relative to the protection of persons and property, brief description and methods of protection. Among the methods of protection are ordered several separate chapters that are devoted to different types, which include the physical and technical protection. An important part which is discussed below is information concerning the monitoring and alarm receiving center.

In the practical part of the thesis is selected project proposal of security, which is divided into several parts, which at the beginning includes a description and safety assessment. It is the basis for the design of safety. The draft security is then logically classified for example classification environment, security level, the deployment of components, how to connect to the ARC and other possible extensions. The last point is the budget.

Keywords: wholesale, warehouse, physical protection, technical protection, combined protection, security, safety, design

Poděkování a motto

Na tomto místě bych chtěl poděkovat svému vedoucímu práce, kterým byl JUDr. Vladimír Laucký, za poskytnutou pomoc, důležité rady a připomínky, které mi během práce významně pomohly. Také bych rád poděkoval firmě Jablotron za poskytnuté materiály.

„Když všichni mluví o nemožnostech, hledej možnosti.“

Tomáš Baťa

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	9
I TEORETICKÁ ČÁST	10
1 OCHRANA OSOB A MAJETKU	11
1.1 ZÁKLADY OCHRANY MAJETKU A OSOB	11
1.2 PREVENTIVNÍ ČINNOST	11
2 ORGANIZAČNÍ A REŽIMOVÁ OPATŘENÍ.....	14
3 FYZICKÁ OCHRANA.....	15
3.1 FORMY FYZICKÉ OCHRANY	16
3.1.1 Strážní služba	16
3.1.2 Bezpečnostní dohled.....	16
3.1.3 Bezpečnostní doprovod.....	17
3.1.4 Bezpečnostní průzkum.....	17
3.1.5 Kontrolní propustková služba	17
4 TECHNICKÁ OCHRANA	18
4.1 TECHNICKÉ NORMY	18
4.2 MECHANICKÁ OCHRANA.....	19
4.2.1 Mechanické zábranné systémy obvodové ochrany	20
4.2.2 Mechanické zábranné systémy plášťové ochrany	20
4.2.3 Mechanické zábranné systémy předmětové ochrany	20
4.3 ELEKTRONICKÁ OCHRANA.....	21
4.3.1 Poplachové zabezpečovací a tísňové systémy – PZTS.....	21
4.3.2 Kamerate systémy – CCTV	23
4.3.3 Systémy kontroly vstupů – ACS	25
4.3.4 Elektrická požární signalizace.....	25
4.3.5 Elektronická ochrana zboží.....	27
4.4 KOMBINOVANÁ OCHRANA	30
5 DOHLEDOVÁ A POPLACHOVÁ PŘIJÍMACÍ CENTRA	31
5.1 POPLACHOVÝ PŘENOSOVÝ SYSTÉM	32
5.2 TYPY PŘENOSU.....	32
5.2.1 Jednotná telefonní síť – analogová (JTS/PSTN).....	33
5.2.2 Digitální síť integrovaných služeb - ISDN	33
5.2.3 Globální systém pro mobilní komunikaci – GSM.....	33
5.2.4 Radiový přenos na vyhrazených frekvencích	34
5.2.5 Internet – KRONOS	34
II PRAKTICKÁ ČÁST.....	35
6 POPIS OBJEKTU.....	36
7 BEZPEČNOSTNÍ POSOUZENÍ.....	38
7.1 ANALÝZA RIZIK.....	38
7.1.1 Zabezpečované hodnoty.....	38
7.1.2 Budova	40
7.2 OSTATNÍ VLIVY	42
7.2.1 Vnitřní vlivy	42

7.2.2	Vnější vlivy	43
8	NÁVRH ZABEZPEČENÍ	45
8.1	KLASIFIKACE PROSTŘEDÍ	45
8.2	STUPEŇ ZABEZPEČENÍ	46
8.3	KOMPONENTY PZTS	47
8.3.1	Ústředna JA-106KR	48
8.3.2	Sběrníkový přístupový modul JA-114E	49
8.3.3	PIR detektor pohybu JA-110P	50
8.3.4	PIR detektor pohybu a rozbití skla JA-120PB	50
8.3.5	Venkovní PIR detektor pohybu JA-188P	51
8.3.6	Magnetický detektor otevření JA-111M	52
8.3.7	Kombinovaný detektor kouře a teploty JA-110ST	52
8.3.8	Vnitřní siréna JA-110A	53
8.3.9	Venkovní siréna JA-111A	53
8.4	ROZMÍSTĚNÍ KOMPONENTŮ	54
8.4.1	Zásady umístování komponentů	54
8.4.2	Rozmístění	55
8.5	KONFIGURACE SYSTÉMU	57
8.5.1	Rozdělení do sekcí a možnosti střežení	58
8.5.2	Zapojení komponent	58
8.6	VÝPOČET NÁHRADNÍHO ZDROJE NAPÁJENÍ	59
8.7	PŘIPOJENÍ NA DPPC	60
8.8	ZÁSAH	61
8.9	ÚDRŽBA A SERVIS	61
8.10	DOPLNĚNÍ O MECHANICKÉ ZÁBRANNÉ SYSTÉMY	62
8.11	OCHRANA ZBOŽÍ	63
8.12	ROZŠÍŘENÍ O CCTV	63
8.12.1	Vivotek IP8332	64
8.12.2	Vivotek IP7161	64
8.12.3	Netgear GS108P	64
8.12.4	IPCorder KNR-1004	65
8.12.5	CyberPower Value800ELCD-FR	66
8.13	FYZICKÁ OCHRANA	66
9	CENOVÉ ZHODNOCENÍ	67
10	VÝVOJ BEZPEČNOSTNÍCH SYSTÉMŮ	69
	ZÁVĚR	70
	ZÁVĚR V ANGLIČTINĚ	71
	SEZNAM POUŽITÉ LITERATURY	72
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	74
	SEZNAM OBRÁZKŮ	75
	SEZNAM TABULEK	76
	SEZNAM PŘÍLOH	77

ÚVOD

Cílem práce je vypracování návrhu komplexního zabezpečení fyzickými a technickými prostředky, popis jednotlivých způsobů ochrany a vyřešit přenos signálů na dohledové a poplachové přijímací centrum.

Jelikož je nutno dbát na finanční možnosti zákazníků, je vhodné navrhnou kompletní plnohodnotný systém, který je posléze možné postupně doplňovat a vylepšovat jeho možnosti dle přání a možností zákazníka.

Postup práce je zvolen tak, aby i lidé nezasvěcení do problematiky bezpečnostních technologií, byly schopni z předložených informací zjistit základní potřebné informace. V rámci teoretické části se práce věnuje obecnými informacemi, které souvisejí s ochranou osob a majetku. Jedna z prvních kapitol je věnována možnostem ochrany, mezi které patří zajisté organizační a režimová opatřeními, fyzická ochranou a technická.

Text související s technickou ochranou si klade za cíl popsat jednotlivé typy technické ochrany a jejich základní vlastnosti. Cílem není popsat podrobně fyzikální principy, ale uvést čtenáře do dané problematiky bez zbytečných rozvádějících detailů, které nejsou pro dané téma podstatné. Podstatnou částí jsou zajisté i zásady pro rozmísťování jednotlivých prvků PZTS, čemuž je věnována část praktické práce, kde jsou popsány zásady pro použité prvky při návrhu zabezpečení.

Hlavním pilířem práce je praktická část, která je věnována samotnému projektovému návrhu. Zde je v počátku uveden základní popis objektu, kde jsou uvedeny podstatné informace o umístění apod. Dále je vypracováno bezpečnostní posouzení objektu, ve kterém jsou obsaženy veškeré potřebné informace a poslouží jako východisko pro návrh zabezpečení, které následuje hned jako další kapitola.

Kapitola návrhu zabezpečení je obsáhlá a je věnována několika bodům, mezi které je nutné zařadit klasifikaci prostředí a určení stupně zabezpečení podle platných norem. Následně jsou uvedeny vlastnosti jednotlivých komponentů a jejich rozmístění. Mezi výše uvedené patří i volba přenosu signálů na DPPC, určení způsobu zásahu apod. Posledními body této části práce jsou návrhy a doporučení o rozšíření pomocí mechanických zábranných systémů a kamerového systému.

Závěrem je práce věnována cenovému ohodnocení popsaného projektu, vlastnímu pohledu na budoucnost bezpečnostních systémů a osobním poznatkům z postupů práce.

I. TEORETICKÁ ČÁST

1 OCHRANA OSOB A MAJETKU

1.1 Základy ochrany majetku a osob

Největším a zásadním problémem v České Republice je zajisté v tom, že zde nemáme zákon přímo se týkající civilních bezpečnostních služeb. Z toho důvodu musíme hledat podmínky v platných právních normách. Soukromé bezpečnostní služby jsou komerčními službami, které nemohou zastávat mocenské složky státních orgánů.

Svou činnost vykonávají buď jako fyzické nebo právnické osoby. Nemají žádnou vyšší pravomoc a svou činnost opírají o právo podnikatelských subjektů na ochranu svého života a majetku, přičemž využívají právní možnosti dané ústavou, občanským zákoníkem, obchodním zákoníkem, trestním zákoníkem a živnostenským zákonem, který jako jediný definuje činnost firem průmyslu komerční bezpečnosti, když uvádí jako koncesovanou živnost „Poskytování technických služeb k ochraně majetku a osob, dále Služby soukromých detektivů a Podniky zajišťující ostrahu majetku a osob“. Tyto 3 faktory naší odborné podnikatelské činnosti mají tedy jasnou oporu v zákoně a to v zákoně živnostenském č. 455/1991 Sb. ve znění pozdějších úprav. Protože na rozdíl od ostatních států evropské unie či kandidátských zemí, je zde absence zákona o civilních bezpečnostních službách, musíme umět stávající zákony, umožňující nám v tomto oboru podnikat, totálně využít a to především zákon živnostenský. [1]

Formy soukromé bezpečnosti v PKB dělíme z hlediska použitých metod ochrany na:

- A) Ochranu osob
- B) Ochranu majetku

Přitom ochrana osob má vždy v činnosti PKB přednost před ochranou majetku a formy ochrany osob a majetku dále dělíme na:

- A) Fyzickou ochranu
- B) Technickou ochranu – mechanickou, elektronickou, smíšenou, speciální
- C) Kombinovanou ochranu [1]

1.2 Preventivní činnost

Ať už se jedná v celém PKB o ochranu fyzickou nebo technickou, je nejdůležitějším faktorem preventivní činnost, která má své základní zásady:

- Včasnost
- Rychlost
- Komplexnost
- Odbornost
- Permanentnost
- Součinnost

Preventivní činnost úzce souvisí s následnou cenou, kterou do zabezpečení chce vložit a je rozdíl, zda se jedná o obyčejnou veřejnost, která chce ochránit svůj majetek, nebo zda se jedná o podnikatele, který chce ochránit především majetek svého podniku. Z toho plynou i rozdílné zásady, které můžeme z velké části ovlivnit vlastními silami a prostředky.

Zásady preventivní činnosti pro občanskou veřejnost

- 1) Pohled na obydlí, dům, vilu, chatu nezakrývat vysokými zdmi a hustými ploty.
- 2) Počet vstupů do obydlí minimalizovat, rovněž tak počet oken a dalších stavebních otvorů, zejména v přízemí (do výše 4 m).
- 3) Opatřit objekt bezpečnostními dveřmi se zámkovým systémem, který je odolný proti vyhmatání, rozlomení, odvrtání, prokopnutí, prolomení a vysazení. Odborně zabezpečit i další stavební otvory na plášti objektu, zejména méně viditelné a málo používané (zadní dveře, sklepní okénka, technické světlíky apod.).
- 4) Mechanické zábranné prostředky doplnit vhodným zařízením elektrické zabezpečovací signalizace.
- 5) Při provádění zabezpečení objektu se obrátit na odbornou firmu s certifikací, zásadně spoléhat na vlastní síly a různé „fušery“.
- 6) Neukládat v domácnosti cenné předměty. Je-li to nezbytné, pak je zvlášť chránit jak mechanicky, tak elektronicky. Kromě toho je nutné pořídit si na takové věci dokumentaci (foto, popis).
- 7) Nepouštět do bytu (domu) neznámé osoby, vydávající se např. za údržbáře, odečítače měřičů apod., bez průkazu jejich totožnosti a příslušnosti k udávané firmě
- 8) Vyloučit příznaky dlouhodobé nepřítomnosti, jako je nevybraná schránka, stažené rolety, nezalité květiny, neodklizený sníh.
- 9) V okolí domu neponechávat nářadí vhodné k vloupání jako jsou sekery, kladiva, pily, žebříky apod.
- 10) Při krátké nepřítomnosti např. za účelem nákupu neopomenout zavřít okna v přízemí, sklepe a nižších podlažích a zamknout dveře. [2]

Zásady preventivní činnosti pro podnikatele

- 1) Dobře zhodnoťte, zda chcete pracovat v bezpečí, aby se Vaše zařízení, zboží, zásoby, stroje, přístroje a ostatní prostředky podnikání nestaly snadnou kořistí lupičů a přesně vymezte, co chcete proti nim chránit.
- 2) Nezapomeňte, že základem každého zabezpečení objektu jsou mechanické zábrany, jako jsou bezpečnostní dveře, zámky, fólie, trezory, mříže, bezpečnostní schránky.
- 3) Zkušenosti ukazují, že kvalitní mechanický zábranný systém musí být doplněn poplachovými zabezpečovacími a tísňovými systémy, eventuálně CCTV uzavřenými TV sledovacími a střežícími systémy k přesné dokumentaci pachatele na místě. Často jsou nezbytné i systémy kontroly přístupu a systému pro elektronickou ochranu zboží, eventuálně i elektrické prvky požární ochrany.
- 4) Každý poplachový zabezpečovací a tísňový systém neobstojí pouze se signalizací lokální (siréna, maják), ale je třeba signál vyvést na poplachové přijímací centrum objektů a to buď policii ČR, obecní policie, ale zejména soukromých bezpečnostních služeb (SBS).
- 5) Systémy ochrany budujte v případě nedostatků financí postupně podle nejohroženějších míst. Začněte mechanickými zábrannými systémy přes PZTS, ACCES až po CCTV. Řada firem poskytuje splátkový systém nebo leasing.
- 6) Na komplexní systém nechte zpracovat kvalifikovaný projekt odborně způsobilou osobou a nechte si předložit nabídku od případného dodavatele.
- 7) Veškeré instalace vyžadujte od autorizovaných firem, jen z certifikovaných prostředků schválených odbornými pracovišti, které respektují pojišťovny.
- 8) Při vyhodnocování nabídek berte v úvahu, že nejlevnější nemusí být nejlepší. Rozhodující je komplexnost nabídky, záruční a pozáruční servis. Nabídky konzultujte s pojišťovnou.
- 9) Neopomeňte se nechat řádně proškolen k obsluze instalačního bezpečnostního zařízení a překontrolujte své spolupracovníky, že obsluhu zařízení skutečně znají.
- 10) Při výstavbě nového objektu nebo zásadní rekonstrukci nechte zabezpečovací techniku již zakomponovat do zpracování základního projektu. Zásadně tím ušetříte. Dbejte na to, aby dodavatel zabezpečovací techniky byl z důvodu diskrétnosti a návazných servisních služeb a jejich operativnosti Vaším přímým dodavatelem. [2]

2 ORGANIZAČNÍ A REŽIMOVÁ OPATŘENÍ

Organizační opatření obsahují informace o provádění kontrol, organizace kontrol, sledování plnění úkolů, harmonogramy řízení práce, přepravy, výstavby, oprav a servisních služeb, zkoušek a revizí, provozních odstávek, výcviku a školení, tréninku a střeleb, fyzických a odborných prověrek, inspekcí, auditů apod. [3]

Režimová opatření jsou bezpečnostní směrnice, které prostřednictvím zavedených systémů opatření zajistí ochranu majetku, osob a jiným zájmů. Jde o soubor organizačně-administrativních opatření, která mají předcházet nežádoucímu jednání osob nacházejících se v chráněném objektu a zajistit správné fungování zabezpečovacího systému. [4]

Režimová opatření můžeme dělit z prostorového hlediska na vnější a vnitřní.

Vnější režimová opatření – zajišťují hlavní vstupní a výstupní prostory chráněného objektu. Jde především o vchody pro osoby, vjezdy pro vozidla a jiné vstupní brány. Zde dochází ke kontrole osob, vozidel a věcí nacházejících se u osob nebo ve vozidle.

Vnitřní režimová opatření – zajištění se týká vnitřních prostor objektu, kde se jedná především o omezení pohybu osob nebo vozidel přímo v daném objektu. Vnitřní režimová opatření se také týkají monitorování pohybu materiálu a výrobků, či zajištění osvětlení v určitých částech objektu. [4]

Pro zabezpečení těchto opatření je několik důležitých aspektů:

- vstupní a výstupní režim osob a vozidel,
- materiálový a expediční režim, který zabraňuje rozkrádání majetku,
- provozní režim, jehož cílem je zajistit plynulost a bezpečnost provozu,
- klíčový režim. [4]

Základní pravidlo pro dodržování režimových a organizačních opatření:

- školení zaměstnanců,
- vytváření bezpečnostního povědomí zaměstnanců,
- články v rámci partnerských a pracovních smluv,
- vytváření bezpečnostní dokumentace. [4]

Dodržování režimových opatření si vyžaduje vypracování různých dokumentů režimové ochrany podle své důležitosti. Zde řadíme dokumenty obsahující: statut organizace, organizační pořádek, pracovní pořádek, spisovní pořádek a skartační pořádek.

3 FYZICKÁ OCHRANA

Jedná se o nejstarší a nejpoužívanější formu ochrany osob a majetku. Zajišťování fyzické ochrany ostrahou bývá prováděno strážnými, hlídači, hlídací službou či policisty a jedná se nejnákladnější způsob zajištění bezpečnosti, ale vychází-li adekvátní reakce ze zkušeností speciálně přepravených osob, bývá zpravidla nejjednodušší a hlavně nejefektivnější. Cílem fyzické ochrany je především v případě nutnosti okamžité provedení zásahu, odhalení a zadržení narušitele, zamezení vzniku škod a jejich minimalizace, realizaci protipožárních a havarijních opatření apod.

Fyzickou ochranu můžeme dělit v závislosti na různých faktorech a to zejména:

Podle časového působení:

- v době pracovní doby,
- permanentní,
- nárazovou.

Podle druhu výkonu:

- stacionární,
- dohledová,
- doprovodná,
- víceúčelová,
- přehledově dozorová,
- revírní.

Podle způsobu zajištění:

- fyzická ochrana z řad vlastních pracovníků,
- na smluvním základě,
- smíšená (kombinovaná).

Podle způsobu výstroje a výbroje:

- ozbrojená
- neozbrojená,
- uniformovaná,
- civilní,
- skrytá (detektivní). [1]

3.1 Formy fyzické ochrany

3.1.1 Strážní služba

Rozlišujeme různé strážní služby podle jejich způsobu provádění:

- statická (na pevných stanovištích)
- pohyblivá (hlídková na pohyblivých stanovištích)
- revírní (namátková kontrola stanoveného území)

Pracovník při vykonávání strážní služby plní především následující úkoly:

- ochrana majetku proti krádežím, vloupání, vandalismu, teroristickým akcím,
- pozorování objektu a přilehlého okolí, komunikací, parkovišť a také pozorováním činnosti v okolí objektu, která by mohla vést k narušení bezpečnosti,
- zabránění vzniku mimořádných událostí,
- plnění další specifické úkoly.

3.1.2 Bezpečnostní dohled

Bezpečnostní dohled je prováděn pracovníkem SBS převážně uvnitř střeženého objektu, kde dohlíží, na pevně stanovená místa, prostory, budovy nebo jiné objekty spadající do celého střeženého objektu firmy. Bezpečnostní dohled může být prováděn dvěma následujícími způsoby jako:

- přímý dohled konaný pracovníkem SBS
- dohled dálkový konaný pracovníkem SBS za využití monitorovacích systémů s fyzickým výjezdem k místu události, při jejím zjištění.

Bezpečnostní dohled plní následující úkoly:

- kontrola pohybu a činnosti osob,
- dodržování vnitřního režimu,
- doprovázení cizích osob po objektu,
- dozor nad pracovníky dodavatelů, kteří plní úkoly v objektu,
- uzavírání, uzamykání, zajišťuje a pečeti určené prostory,
- monitorování a kontrola svěřených prostor,
- plní další specifické úkoly podle smlouvy.

3.1.3 Bezpečnostní doprovod

Jedná se o činnost SBS zajišťující ochranný doprovod majetku a osob při přesunech, cílem je zajistit bezpečný doprovod zásilky, včetně osob zákazníka, kteří ji doprovázejí, za využití obranných opatření, která umožňuje zákon a nepřipustit odcizení či poškození zásilky a zajistit ochranu života a zdraví doprovázejících osob zákazníka. Bezpečností doprovod lze tedy rozdělit na doprovod: [1]

- osob,
- peněžních hotovostí a cenností
- kamionové dopravy.

Bezpečnostní doprovod lze v činnosti SBS realizovat:

- pěším způsobem,
- s využitím dopravních prostředků.

3.1.4 Bezpečnostní průzkum

Cílem bezpečnostního průzkumu je prověření, prozkoumání či rekognoskování terénu, situace, místa, objektu, kde bude následně prováděna další činnost SBS. Řeší se především před samotným střežením, před přijetím zakázek, transportem peněz nebo přijetím bezpečnostních opatření. Bezpečnostní průzkum se provádí jako:

- fyzický,
- technický nebo
- kombinovaný.

3.1.5 Kontrolní propustková služba

Za využití fyzické a technické ostrahy slouží k zabezpečení především režimových opatření při vstupu (vjezdu) a výstupu (výjezdu) do/z objektu. Úkoly této služby jsou:

- kontrola a evidence procházejících osob projíždějících vozidel,
- zabránuje vnášení a vynášení výrobků, polotovarů a materiálu,
- poskytuje návštěvníkům potřebné informace a zajišťuje dodržování režimu návštěv,
- vede knihu příchodů a odchodů,
- ve stanovený čas odemyká či uzamyká vchody a vstupy do objektu,
- vydává oprávněným osobám klíče podle stanovených zásad a pravidel,
- slouží také jako ohlašovna požárů a ekologických havárií,
- plní další specifické úkoly.

4 TECHNICKÁ OCHRANA

4.1 Technické normy

Význam používání technických norem a normalizace spočívá ve schopnosti dorozumění. Už od samého začátku své existence sloužila k účelu, kterým je právě dorozumění partnerů v oblasti techniky. Technické normy jsou tedy dohody, které obsahují technické specifikace nebo jiná kritéria používaná jako pravidla, směrnice, pokyny nebo definice charakteristik zajišťující, že materiály, výrobky, postupy a služby vyhovují danému účelu.

Používání mezinárodních norem, označovány zkratkou ISO, přispívá k odstraňování technických překážek a jsou tak důležitým předpokladem pro vznik jednotného trhu a především možnost expanze firem do zahraničí. V EU se k tomuto účelu používají evropské normy, označovány zkratkou EN, které mnohdy vycházejí z norem mezinárodních. V naší zemi se používají mnohdy normy převzaté (harmonizované) z norem evropských a jsou označovány např. ČSN EN 50130.

Základní technické normy používané v průmyslu komerční bezpečnosti představuje řada norem ČSN EN 50130. Tato řada norem obsahuje všeobecné požadavky na poplachové systémy (obsahem jsou například požadavky na elektromagnetickou odolnost). Následující související řada evropských norem uvádí ostatní požadavky (například požadavky na jednotlivé komponenty, aplikace a provedení), které jsou použitelné pro specifické typy poplachových systémů, kterými jsou:

- ČSN EN 50131 Poplachové systémy – PZTS
- ČSN EN 50132 Poplachové systémy – Systémy CCTV
- ČSN EN 50133 Poplachové systémy – Systémy kontroly vstupu
- ČSN EN 50134 Poplachové systémy – Systémy přivolání pomoci
- ČSN EN 50135 Poplachové systémy – Systémy tísňové
- ČSN EN 50136 Poplachové systémy – Systémy přenosové
- ČSN EN 50137 Poplachové systémy – Systémy kombinované nebo integrované
- ČSN EN 54 Elektrická požární signalizace

Dále pak byly provedeny nové vydání norem podle vzorů z EU a změnilo se také názvosloví. Dále jsou uvedeny příklady nejnovějších vydání norem, se kterými se lze běžně v průmyslu komerční bezpečnosti setkat, a měli by se v bezpečnostních technologiích dodržovat:

- ČSN EN 50131-1 ed. 2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky
- ČSN CLC/TS 50131-7 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy Část 7: Pokyny pro aplikace
- ČSN EN 50132-1 Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích; Část 1: Systémové požadavky
- ČSN EN 50132-5 Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích; Část 5: Přenos videosignálu
- ČSN EN 50132-7 Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích; Část 7: Pokyny pro aplikaci
- ČSN EN 50133-1 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích; Část 1: Systémové požadavky
- ČSN EN 50133-7 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích; Část 7: Pokyny pro aplikace

Pro mechanické zábranné systémy pak platí například česká norma vstupující v platnost dne 1. 2. 2012, která nahrazuje předchozí normu ČSN P ENV 1627:

- ČSN EN 1627 Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace

Technická ochrana v sobě zahrnuje ochranu mechanickou, elektronickou a smíšenou.

4.2 Mechanická ochrana

Jedná se o ochranu majetku a osob za využití mechanických prvků, respektive zábranných prostředků či systémů. Mechanické zábranné systémy (MZS) považujeme za základní prvek ochrany objektů a osob v průmyslu komerční bezpečnosti. Pod MZS řadíme veškeré mechanické prvky, které stěžují násilné vniknutí nepovolené osoby do chráněné zóny nebo objektu především přes oplocení nebo cestou dveřních nebo okenních otvorů, případně manipulací nepovolané osoby s chráněnými předměty v zabezpečeném objektu. [5]

MZS patří mezi základní ochranu a setkáme se s nimi u každého objektu, i když nebyla ochrana řešena na profesionální úrovni. Důležité je si uvědomit, že jakýkoliv bezpečnostní elektronický systém je zbytečný, bez předchozího mechanického zabezpečení objektu. Z výše uvedené definice MZS vyplývá, že se jednotlivé prvky jsou schopny odolávat napadení po určitou dobu, kterou v PKB označujeme jako průlomovou odolnost MZS.

Mechanická ochrana se dělí na MZS obvodové, plášťové a předmětové ochrany.

4.2.1 Mechanické zábranné systémy obvodové ochrany

Slouží k ochraně obvodu objektu, především ochrana samotné hranice pozemku. Mezi mechanické zábranné systémy obvodové ochrany patří například:

- bezpečnostní oplocení,
- brány,
- branky,
- závory,
- hřebenové bariéry,
- zastavovací pásy,
- zpomalovací retardéry, zábrany,
- turnikety apod.

4.2.2 Mechanické zábranné systémy plášťové ochrany

Plášťová ochrana se vztahuje, jak již název napovídá, na bezpečnost samotného pláště budovy, tj. na stavební otvory, okna, dveře, zdi apod. Mezi mechanické zábranné systémy plášťové ochrany řadíme například:

- otvorové výplně, okna, dveře,
- mříže, rolety a žaluzie,
- bezpečnostní a ochranné fólie,
- bezpečnostní skla,
- cylindrické vložky,
- přídavné zámky,
- dveřní řetízky, zastavovače a kukátka apod.

4.2.3 Mechanické zábranné systémy předmětové ochrany

Jedná se o ochranu samostatných předmětů především uvnitř objektu, jako jsou peníze a cennosti nebo i jiné cenné předměty, které chceme ochránit. Do mechanických zábranných systémů předmětové ochrany patří například:

- komorové, skříňové, účelové, vestavěné, vhozové trezory,
- komerční úschovné objekty,
- ohnivzdorné, ocelové a kartotéční skříně,
- trezory na zbraně,
- příruční pokladničky,
- manipulační schránky apod. [5]

4.3 Elektronická ochrana

Jde o podporu mechanických zábranných systémů, za použití moderních technologií a elektrických (elektronických) prvků. Samostatná elektronická ochrana není schopna pachatele zastavit, má za úkol především signalizaci narušení bezpečnosti střeženého objektu. Jedná se o velmi spolehlivou ochranu, která je při správném použití v kombinaci s MZS velmi obtížně překonatelná. Do elektronické ochrany patří zejména:

- poplachové zabezpečovací a tísňové systémy (PZTS),
- uzavřené kamerové systémy (CCTV),
- systémy kontroly vstupů (ACS),
- elektrická požární signalizace (EPS),
- elektronická ochrana zboží,
- biometrické identifikační systémy,
- satelitní vyhledávání vozidel,
- ochrana dat a informací,
- systémy tísňové,
- systémy přenosové. [1]

4.3.1 Poplachové zabezpečovací a tísňové systémy – PZTS

Poplachové zabezpečovací a tísňové systémy jsou komplexem čidel, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových, zapisovacích a ovládacích zařízení a dalších prvků, jejichž hlavním cílem je detekce nebezpečí při vloupání nebo vniknutí do střeženého objektu a optické nebo akustické signalizování této skutečnosti. Vždy jde o informování majitele nebo jiné pověřené osoby o vzniklé situaci.

Každý PZTS se skládá z několika základních částí, mezi které patří:

- ústředna,
- detektory,
- signalizační zařízení,
- přenosové prostředky,
- ovládací zařízení,
- napájení.

PZTS se dělí dále do dílčích kategorií, podle toho, jakou část objektu mají střežit, jedná se tedy o ochranu obvodovou, plášťovou, prostorovou a předmětovou.

Detektory lze dělit podle mnoha hledisek, mezi hlavní lze považovat rozdělení podle způsobu napájení na detektory:

- napájené
- nenapájené

Napájené detektory pak dále lze rozdělit na aktivní a pasivní.

- Pasivní detektory při zjišťování charakteristických vlastností napadení reagují na fyzikální změny, jsou energeticky méně náročné, těžce zjistitelné a nevznikají problémy se vzájemným rušením nebo ovlivňováním při kooperaci více detektorů.
- Aktivní detektory si vytvářejí vlastní pracovní prostředí, z toho plyne vyšší spotřeba, snadnější zjistitelnost a možné vzájemné rušení. Princip je založen například na Dopplerově jevu, tj. změně frekvence odraženého signálu apod.

Podle použitého fyzikálního signálu a principu je lze dále dělit na detektory:

- elektromechanické,
- elektromagnetické (např. MW, IR),
- elektroakustické (např. US).

Prvky prostorové ochrany - detekují pohyb uvnitř budov na strategických místech, jako jsou chodby, schodiště, místnosti apod. a patří zde prvky jako:

- pasivní nebo aktivní infračervená čidla,
- ultrazvuková čidla,
- mikrovlnná čidla
- duální čidla. [6]

Prvky plášťové ochrany - sledují otevření, průnik nebo destrukci vstupních otvorů, nebo samotného pláště budovy využívající:

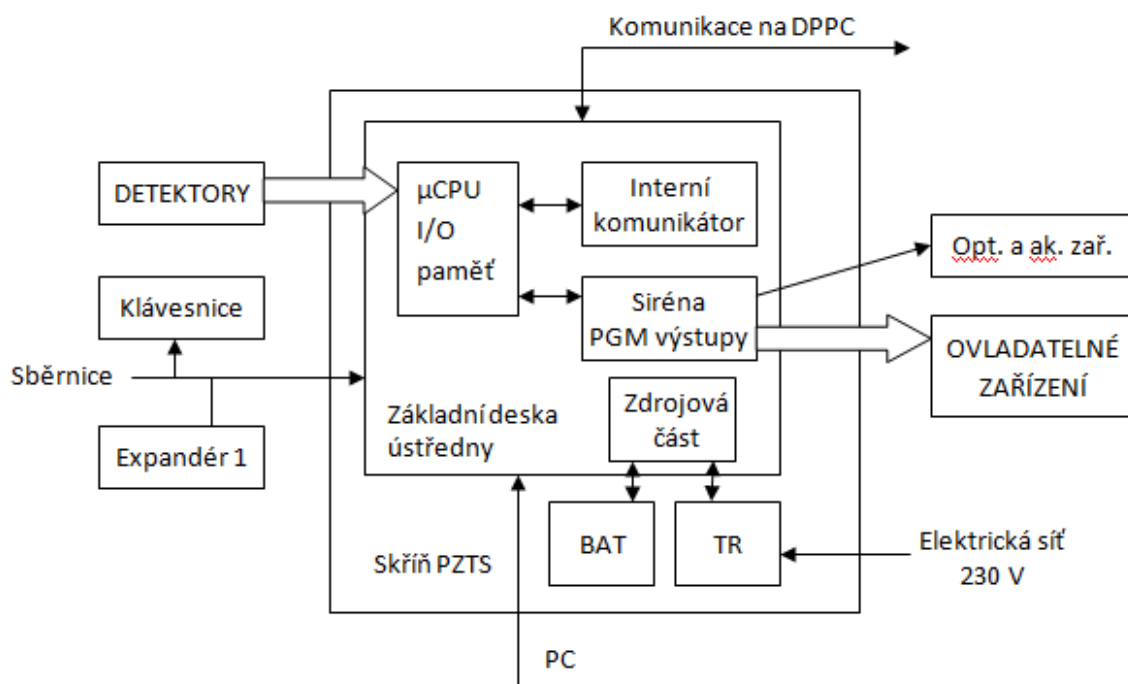
- mechanické nebo magnetické kontakty,
- čidla na ochranu prosklených ploch,
- drátová, vibrační čidla,
- fólie, tapety, polepy,
- rozpěrné tyče. [6]

Prvky obvodové ochrany - cílem je odstrašení možných pachatelů, jejich odhalení a signalizace v případě narušení obvodu objektu. Detektory pro obvodovou ochranu mají delší dosahy než detektory pro plášťovou nebo prostorovou ochranu a musí splňovat náročnější požadavky vycházející ze zhoršených klimatických podmínek a musí být odolné

vůči planým poplachům, což je i za použití moderních technologií problematické. Mezi prvky obvodové ochrany patří např.:

- infračervené závory a bariéry
- mikrovlnné bariéry
- šterbinové kabely
- perimetrická PIR čidla. [6]

Ústředna – jde o centrální část poplachových systémů. Ústředna má za úkol sběr a vyhodnocování informací získaných od jednotlivých čidel. Jedná se o plošný spoj, který obsahuje mikroprocesor, napájení, záložní napájení, vstupy zón, programovatelné výstupy, vnitřní sirénu, komunikátory a sběrnici, přes kterou lze ústřednu pomocí ovládacích prvků ovládat a rozšířit pomocí expandérů. Základní schéma struktury ústředny obsahuje následující obrázek.



Obr. 1: Blokové schéma ústředny PZTS

4.3.2 Komerové systémy – CCTV

CCTV (Closed Circuit TeleVision) představuje, jak již název napovídá uzavřený televizní okruh, který se skládá ze základních částí, mezi které řadíme:

- kamery,
- přenosová zařízení,
- záznamová zařízení a
- zobrazovací zařízení.

Uzavřené kamerové systémy se využívají pro monitoring pohybu osob a předmětů v hlídané nebo sledované oblasti. Kamerové obrazy lze využít v závislosti na aplikaci buďto přímo při sledování obrazovky nebo později s pomocí videozáznamu.

Hlavním rozdělením kamerových systémů, které je zásadním faktorem pro volbu komponentů, je způsob technologie záznamu obrazu kamery. Zde rozlišujeme dvě hlavní skupiny, kamery analogové a IP (digitální). Nejpodstatnějším rozdílem obou typů je zde pouze způsob přenosu informací. Způsob získávání obrazu a jeho fyzikální a optické principy jsou již velmi podobné.

Analogové kamery využívají analogový přenos signálů, prakticky totožný s televizním vysíláním, jehož norma je stará více než 50 let. Jejich záznam je prováděn na DVR s HDD, což jsou digitální videorekordéry s vlastním pevným diskem.

IP kamery používají pro přenos běžné počítačové sítě, které mají k dispozici větší šířku pásma, tudíž zde nedochází k takovému omezení, jako u předchozího typu. Každá IP kamera má svou vlastní IP adresu a jsou připojeny na NVR, což je síťový videorekordér.

Následující tabulka shrnuje zásadní výhody a nevýhody obou technologií:

Tab. 1: Vlastnosti analogových a IP kamer [7]

Vlastnost	Analogové kamery	IP (digitální) kamery
Rozlišení	0,4 MPix	Standardně 1,3 až 2 MPix
Citlivost	Vyšší	Nižší
Snímková frekvence	25 FPS	6 až 60 FPS
Detekce pohybu v obraze	Ano (s použitím DVR)	Ano
Inteligentní analýza	Ne	Ano
Sledování přes internet	Většinou ano (s DVR)	Ano
Nároky na diskovou kapacitu	Nižší (nižší rozlišení)	Vyšší (vyšší rozlišení a fps)
Kabeláž	Vyhrazená (ke každé kameře musí vést jeden a více kabelů)	Sdílená (lze využít i k dalším účelům). Více různých dat + PoE
Zabezpečení	Nižší	Vyšší
Standardizace	Vyšší	Nižší
Finanční nároky*	Nižší	Vyšší

*Finanční nároky na zřízení analogového systému jsou opravdu nižší, než zřízení IP systému, ale je zde vhodné uvažovat o využití počítačové sítě a vyšším rozlišení IP kamer, které mohou nahradit více analogových. Díky možnostem a vývoji technologií u IP kamer, je dle mého názoru nakonec poměr cena/výkon srovnatelný pro obě technologie.

4.3.3 Systémy kontroly vstupů – ACS

Přístupový systém neboli systém kontroly vstupu (SKV) lze chápat jako soubor opatření k zajištění řízení a evidence přístupu do zabezpečovaných prostor. Je zde nutné rozlišovat systémy přístupové a docházkové. U obou je nutné prokázání identity uživatele, ale u docházkových systémů je hlavním cílem navíc monitorování času a důvodu průchodu. [8]

Subjekt se může identifikovat jednoznačně třemi základními způsoby:

- heslo, kód, kontrolní otázka,
- identifikační karta, přívěšek, RF ovladač, apod.
- biometrie.

Přístupové systémy podle jejich rozsahu lze rozdělit na autonomní a modulární.

- Autonomní systém je tvořen maximálně dvěma snímacími zařízeními a využívá se především pro instalace s nízkým požadavkem na bezpečnost. Příkladem zde může být autonomní dveřní zámek s integrovanou čtečkou.
- Modulární systém využívá logicky větší počet přístupových míst, více řídicích jednotek a společné řídicí pracoviště.

Systémy kontroly vstupu je možné integrovat spolu s dalšími systémy. V praxi nejpoužívanější integrace je s těmito systémy:

- docházkový systém,
- stravovací systém,
- PZTS, EPS, CCTV,
- IT systémy,
- regulace a měření. [8]

4.3.4 Elektrická požární signalizace

Elektrická požární signalizace (EPS) je ucelený systém sloužící ke zvýšení požární bezpečnosti objektu. Za předpokladu správné instalace EPS a následného včasného zásahu se dá velmi účinně jednat v případě vzniku požáru a lze tak snížit rizika s ohledem na ochranu osob, majetku a také vliv na životní prostředí.

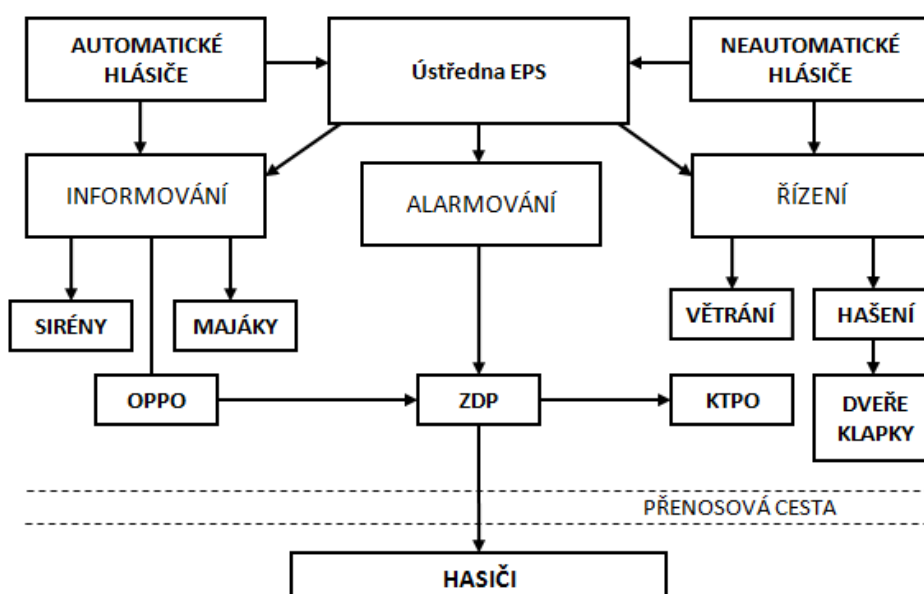
Hlavní úkoly systému EPS z funkčního hlediska spočívá zejména ve včasném rozpoznání prvotních příznaků požáru, ohlášení události obsluze systému, upozornění osob na vzniklé nebezpečí a aktivaci požárně bezpečnostních zařízení, která brání šíření požáru, usnadňují

její likvidaci nebo tuto likvidaci provádějí samočinně. Mezi požárně bezpečnostní zařízení řadíme stabilní hasicí zařízení a samočinné odvětrávací zařízení. [9]

Komplexně řešený systém EPS umožňuje:

- rychlé a spolehlivé určení místa požáru,
- vyhlášení požárního poplachu,
- aktivaci ostatních zařízení požární ochrany – stabilní hasicí zařízení a zařízení pro odvod kouře a tepla, samočinné odvětrávací zařízení,
- aktivaci a řízení evakuačního systému v dané oblasti,
- ovládání a signalizaci stavu dalších požárně bezpečnostních zařízení,
- automatickou komunikaci s hasičským záchranným sborem (HZS). [10]

Na ústřednu, která je centrální částí celé EPS, jsou připojeny automatické nebo manuální požární hlásiče. Aktuální hlásiče detekují požár na základě fyzikálních nebo chemických změn ve střeženém prostoru. Manuální hlásiče se ovládají ručně a jsou umístěny na strategických místech, kde je možné při vzniku požáru včasné reagovat. Ústředna sbírá informace od detektorů a hlásičů a ty dále vyhodnocuje. V případě požáru musí zajistit signalizaci (optickou nebo akustickou), provést sérii dalších postupů, např. odblokování únikových cest, odpojení výrobních technologií a připravit objekt pro zásah HZS. Součástí EPS je i klíčový trezor požární ochrany (KTPO) a obslužné pole požární ochrany (OPPO), které slouží HZS pro rychlejší přístup do budovy. V neposlední řadě je zde také zařízení pro dálkový přenos (ZDP), které slouží k odesílání poplachových zpráv.



Obr. 2: Blokové schéma funkce ústředny EPS [10]

Hlásiče používané v EPS můžeme rozdělit podle principu jejich fungování na hlásiče:

- tepelné,
- optické,
- ionizační,
- vyzařování plamene.

Z hlediska funkce ústředny je důležitý postup při vyhlášení požárního poplachu. V normálním režimu rozlišujeme dva základní stavy. Stav DEN a stav NOC. Pokud v režimu DEN vyhlásí automatický hlásič poplach, ústředna vyhlásí a zobrazí na indikačním tablu poplach úseku. Začne se odpočítávat čas T1, který slouží k přijetí hlášení o poplachu obsluhou. Pokud se tak nestane, je vyhlášen všeobecný poplach s následným předáním zprávy na pult HZS. Pokud obsluha přijme hlášení o poplachu zmáčknutím tlačítka, odstartuje se čas T2, ve kterém může obsluha dojít na místo požáru a vyhodnotit jeho stav. Pokud se jedná o planý poplach, může obsluha v čase T2 zrušit vyhlášení všeobecného poplachu. Pokud dojde k závěru, že požár neuhasí, zmáčknutím nejbližšího tlačítka manuálního hlásiče vyvolá všeobecný poplach s cílem přivolat hasiče. Stejně tak se stane, pokud by doběhl čas T2 a obsluha nezrušila poplach úseku. V případě režimu NOC – bez obsluhy ústředna dle naprogramování přechází k vyhlášení všeobecného poplachu a přivolání hasičů dle jejího naprogramování. [10]

4.3.5 Elektronická ochrana zboží

Jedná se o speciální problematiku předmětové ochrany a patří zcela mimo klasicky známá zabezpečení. Dle typu nabízeného zboží dochází ze strany zákazníků nejčastěji ke krádežím atraktivního zboží, které lze snadno odcizit a skrýt například pod bundu, jako například různé druhy spotřební elektroniky, knih, oblečení, potravin, alkoholu apod.

Ochranu lze provést několika způsoby, přičemž neoptimálnější je jejich vzájemná kombinace a provázanost. Nejefektivnější je elektronická ochrana zboží (EAS – Electronic Article Surveillance). Způsoby, jakým lze zboží chránit jsou např.:

- zabezpečení etiketami radiofrekvenčního nebo magnetického systému,
- použití pasivních prvků ochrany – zrcadla,
- sledování prostoru kamerovým systémem,
- dohled sjednanou soukromou bezpečnostní službou,
- vlastní detektivové pohybující se mezi zákazníky v civilním oblečení,
- režimová opatření (upozornění, že prostor je pod neustálým dohledem). [1]

EAS je ochrana hlídající prostor v místě vstupu nebo výstupu prodejny, kde pomocí anténního systému detekujeme změny elektromagnetického pole. Tato změna je dosažena přítomností etiket, kde etiketou může být laděný obvod, magnetická páska, nebo dvojice magnetických kmitajících pásků. Systémy EAS dělíme tedy na elektromagnetické, akustomagnetické a radiofrekvenční zařízení (popř. RFID systémy). [11]

1) Elektromagnetické zařízení (EM)

Pro svou činnost využívá změnu elektromagnetického pole, vyvolána etiketou, mezi základními prvky systému, dvěma anténami - vysílačem (transmitter) a přijímačem (receiver). Etiketa zde představuje magnetický proužek přichycený na zboží. Když se aktivní etiketa nachází v proměnlivém magnetickém poli mezi vysílačem a přijímačem, etiketa mění svojí magnetizací toto pole. Přijímač detekuje způsobenou změnu signálu, a jestliže se shoduje s jedinečným frekvenčním signálem etikety, spustí alarm. Deaktivace probíhá pomocí skeneru využívající magnetické pole o vysoké intenzitě.

Tyto etikety mají své výhody, kterými jsou především malé rozměry, dají se tedy ukrýt například i do knih, dále se vyznačují vysokou detekční schopností systému a možností je znovu aktivovat. Nevýhodou tohoto zařízení je především fakt, že jsou nejdražším systémem ze všech EAS.

2) Akustomagnetické zařízení (AM)

Tyto systém jsou založeny na principu rezonance. Ochranný prvek se skládá z jednoho nebo více magnetických pásku z různých kovů, z nichž se jeden může pohybovat. Kovový pásek se v elektromagnetickém poli rozkmitá a ochranný prvek vyše tón v podobě signálu. Podle druhů kovů a geometrických rozměrů se odvíjí rezonanční frekvence, na jejímž základě dochází k identifikaci ochranného prvku. Deaktivace probíhá pomocí demagnetizace pevného pásku, který má vlastnosti magneticky tvrdých kovů. Demagnetizací dochází k rozladění tónu, tj. ke změně frekvence. [11]

Používají se především v obchodech s textilem, sportovními potřebami a v obchodech s většími vstupy, kde se uplatní jejich výhoda většího dosahu, který je až 2,7 metru. Dalšími výhodami jsou malé rozměry, vysoká odolnost proti rušení a především se jedná o nejspolehlivější detekci ze všech zmiňovaných systémů. I tyto systémy mají své nevýhody, mezi které patří větší tloušťka samolepících etiket a také vyšší pořizovací cena.

3) Radiofrekvenční zařízení (RF)

Systém se skládá z malých etiket, vysílací antény a přijímací antény. Vzdálenost mezi těmito anténami může být do 2 metrů. RF technologie patří ve světě k nejrozšířenějším zařízením. Mohou být ve formě pevných nebo samolepících papírových etiket. Pevné etikety se připevňují na zboží nekovového charakteru, např. oblečení, a při zaplacení jsou ze zboží sejmuty. Papírové etikety se při zaplacení deaktivují.

Etikety se skládají z kondenzátoru a cívky, kde tyto prvky tvoří laditelný LC obvod (u RFID se v etiketě nachází navíc sloužící k identifikaci). Při průchodu s aktivní etiketou mezi anténami reaguje etiketa na přesně danou frekvenci vysílanou vysílačem. Odezva etikety je přijata přijímačem a vyhodnocena, shoduje-li se odezva s definovanou frekvencí, spustí se alarm. Deaktivace papírových etiket je způsobena přerušením malého kovového pásku LC obvodu vlivem vysokofrekvenčního výboje. [11]

Nejčastější je použití v prodejnách oděvů, sportovních potřeb, obuvi, hraček apod. Výhodami tohoto systému je nízká pořizovací cena, vysoká detekční schopnost systému, relativně jednoduchá elektronika, nastavení a deaktivace, dostupnost a různorodost etiket (papírové, pevné etikety na láhve, etikety na kabely apod.). Na druhé straně se mezi nevýhody řadí nebezpečí vzniku planého poplachu (např. stočený drát simulující etiketu), citlivost na rušení jinými RF systémy, nepoužitelnost na zboží z kovu a hlavně snadné zabránění šíření poplachového signálu stíněním (např. stačí i vlhká ruka). [11]

4) RFID systémy

RFID (Radio Frequency Identification) - identifikace na radiové frekvenci. Jde o moderní radiofrekvenční systém identifikace objektů. Nasazuje se tam, kde je kladen důraz na co nejrychlejší a přesné zpracování informací a okamžitý přenos těchto dat k dalšímu zpracování. Technologie RFID je dnes považována za přímého nástupce čárových kódů, z hlediska budoucího vývoje se však nepředpokládá úplné nahrazení čárových kódů. Dnes se používají kombinace RFID s natisknutým čárovým kódem. [12]

RFID etiketa obsahuje obvod, který reaguje na vysokofrekvenční vysílání vysílače – přijímače, kterému následně předává zpět informace. Etiketa obsahuje celkem tedy anténu s laděným obvodem a křemíkový čip, které vysílaný signál přijmou a zpět vrátí jednoznačnou informaci o každém jednotlivém kusu zboží. Touto metodou je možné číst více etiket současně. [11]

Využití RFID ve spojitosti s ochranou zboží se nachází zejména při sledování stavu zásob ve skladech a pultech, kde je možné zjištění aktuálního stavu bez potřeby manipulace. Výhodami RFID je především zrychlení procesu příjmu, výdeje, přesunu apod., odstranění chyb lidského faktoru, minimalizace nákladů spojené se značením a manipulací, opakovaný zápis údajů zboží do čipu, přesná evidence jednotlivých kusů, palet apod., velká odolnost vůči teplotě, vlhkosti, není nutnost přímé viditelnosti označených jednotek. Nevýhodami mohou být kolize čteček nebo čipů při práci více čteček současně, nebo při načítání všech čipů, které se mohou vzájemně rušit. V dnešní době mají výrobci možnosti tyto problémy eliminovat až úplně odstranit. [11]



Obr. 3: Zleva EM, AM a RF samolepící etikety [11]

4.4 Kombinovaná ochrana

Tato ochrana je kombinací mechanických zábranných systémů a elektronické ochrany, případně i dalších prvků bezpečnostní ochrany.

Integrované bezpečnostní systémy využívají nejčastěji kombinaci a provázanost různých systémů elektronické ochrany majetku a osob. Integrované bezpečnostní systémy dnes mohou z jednoho řídicího centra řídit a koordinovat PZTS, EPS, CCTV, ACCES, průmyslovou havarijní signalizaci a zdravotní a nouzovou signalizaci. Pokud všechny takto integrované systémy vyhoví platným zákonným normám. Kombinovaná ochrana se používá zejména ve velkých nebo důležitých podnicích a městech, zejména při realizaci integrovaného záchranného systému (IZS).

5 DOHLEDOVÁ A POPLACHOVÁ PŘIJÍMACÍ CENTRA

Dohledová a poplachová přijímací centra (DPPC), jak již název napovídá, slouží k přijímání informací ze střeženého objektu pomocí PZST. Jedná se o centra zahrnující výpočetní techniku se speciálními programy, které vyhodnocují a dále zpracovávají přicházející informace a na základě vyhodnocení dávají jasnou představu o aktuálním stavu střeženého objektu.

V případě vzniku nebezpečí je dispečink upozorněn signalizací na DPPC. Dispečer informuje kontaktní osobu a jsou provedeny kroky potřebné k zabránění vzniku škod, např. vysláním zásahových jednotek (ZJ), které se k objektu dostaví a provedou fyzickou obhlídku a zjistí skutečný stav a informují dispečera, se kterým přijmou opatření. Jedná-li se o poplach způsobený příčinou nevýznamného charakteru, jako je například nezavřená ventilačka nebo pohyb zvířete, popř. špatnou obsluhou, dojde k informování majitele a k napravení stavu (přivření okna apod.). Dojde-li ke zjištění, že došlo k narušení pláště budovy nebo je uvnitř znatelný pohyb nežádoucí osoby, ZJ kontaktuje a vyčká příjezdu PČR a majitele objektu. Následuje společná obhlídka objektu. V případě přistižení pachatele, platí zde následující: zadržení pachatele provádí výhradně PČR, jsou-li rizika ohrožení zdraví pro sebe a okolí vyhodnocena jako minimální, může pachatele zadržet i ZJ, ale pouze v objektu, nebo jeho bezprostřední blízkosti. Pomocí pracovníka SBS se zajistí dostřežení objektu do doby opravy poškozených částí pláště budovy, PZTS apod.

Dohledová a poplachová přijímací centra jsou prováděna jako:

- pracoviště policie ČR, kde jsou soustředěny informace z technických bezpečnostních systémů,
- pracoviště obecní policie, která slouží ke stejným účelům,
- pracoviště HZS, kde jsou soustředěny informace o vzniklém požárním nebezpečí získané z technických prostředků EPS,
- pracoviště integrovaného záchranného systému (IZS) kraje (okresu, oblasti), kde jsou soustředěny informace z různých technických zařízení sloužících pro řízení IZS (pulty PZTS, EPS, CCTV apod.),
- pracoviště firem podnikajících v PKB, kde jsou soustředěny informace z různých bezpečnostních systémů a současně je zde organizován represivní zásah a následný informační tok k zákazníkovi a součinnostním složkám (PČR, obecní policii, hasičům, IZS apod.). [2]

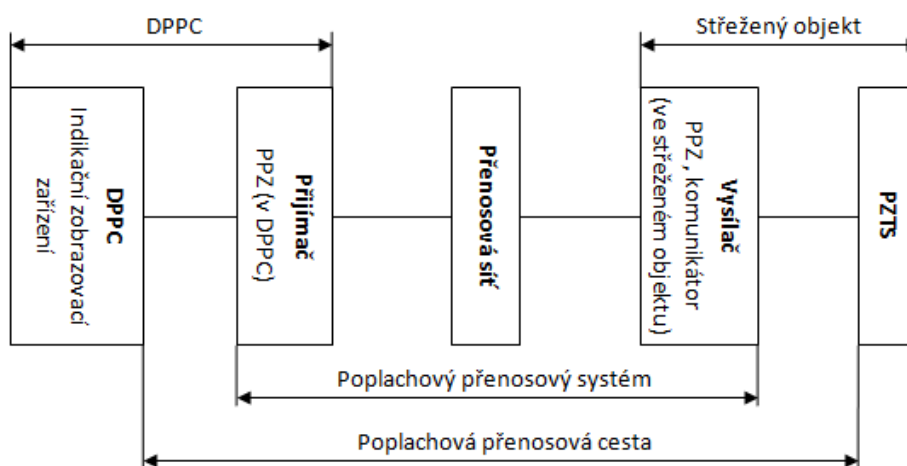
5.1 Poplachový přenosový systém

Informace získaná PZTS pokračuje na vysílač, ve střeženém objektu a pomocí přenosové sítě je přeneseno k přijímači v DPPC, odkud je předána do samotného systému DPPC, který přichází informaci vyhodnotí a zobrazí ve srozumitelném znění obsluze.

Obecný průběh přenosu zprávy pomocí JTS na DPPC je možné shrnout následovně:

- vznik události a vyhodnocení PZTS,
- komunikátor ústředny PZTS (vysílač) se připojí na telefonní linku,
- vytočí číslo na DPPC,
- DPPC vyšle Handshake (potvrzení spojení),
- ústředna vyšle data na DPPC,
- DPPC potvrdí příjem písknutím KissOff (potvrzení přijetí),
- na DPPC dojde k dekódování dat a informace se zobrazí na monitoru.

Přijímač a vysílač jsou tzv. poplachová přenosová zařízení (PPZ) a spolu s přenosovou sítí tvoří poplachový přenosový systém (PPS), viz následující obrázek. Vedení mezi vysílací a přijímací částí PPZ musí být trvale kontrolováno.



Obr. 4: Schéma poplachového přenosového systému

5.2 Typy přenosu

Základní a prioritní funkcí DPPC je přenos poplachových informací přes poplachovou přenosovou cestu, trasu. Tento přenos může být proveden několika způsoby, které se liší především náročností instalace, spolehlivostí a pořizovacími a provozními náklady. Mezi nejpoužívanější přenosové trasy patří telefonní, GSM, rádiová a internetová trasa. Každá samozřejmě vyžaduje jiné HW prostředky a má své výhody a nevýhody.

5.2.1 Jednotná telefonní síť – analogová (JTS/PSTN)

JTS (nebo PSTN - Public Switched Telephone Network) se stále hojně používá pro přenos zpráv na DPPC a je to způsobeno její dostupností a nízkou pořizovací cenou. Velké množství ústředen obsahuje již zabudované komunikátory telefonní linky, čímž odpadáji nutnosti dokupovat rozšiřující části ústředen nutné pro komunikaci jinými typy přenosů.

Nevýhodou je však nemožnost časté kontroly spojení přenosové cesty díky nákladům za spojení pomocí JTS. Proto se kontroluje spojením s DPPC 1x za 24hod. [13]

5.2.2 Digitální síť integrovaných služeb - ISDN

Stejně jako u linky JTS se u ISDN (Integrated Services Digital Network) používá datový hlasový přenos, výhodou je ovšem oproti klasické analogové JTS vyšší přenosová rychlost. Na jednom spojení může probíhat zároveň datový přenos i hlasový hovor. Nevýhodou je, že DPPC musí mít ISDN kartu. Jelikož byl ISDN přenos na svou dobu poměrně drahý a ústředny neměly v sobě integrovaný komunikátor s podporou formátu ISDN, byl v České Republice rovnou nahrazen mobilní sítí GSM. [13]

5.2.3 Globální systém pro mobilní komunikaci – GSM

V dřívějších dobách se jednalo o finančně náročný typ přenosu, ale v dnešní době je již situace mnohem lepší. Používání tohoto typu je nejčastěji v místech, kde není zavedena telefonní linka a nelze použít radiový přenos, např. chatové oblasti apod. GSM síť nám dává dále na výběr použití hovorových pásem, datového přenosu GPRS nebo SMS.

Hovorové pásma - stejně jako u předchozích typů se i zde používá hlasový přenos. Nutností je dokoupení GSM brány k ústředně, aby bylo možné informace přenášet.

Datový přenos GPRS – jde o velmi kvalitní pokrytí s nízkými provozními náklady na přenos zpráv na DPPC. Probíhá obousměrná komunikace mezi DPPC a PZTS s častým testováním přenosové trasy. Jedná se o nahrazení radiového přenosu, neboť radiová síť nelze použít všude, ale GPRS má téměř stoprocentní pokrytí území ČR.

Přenos pomocí SMS – používají se, pokud je DPPC postaveno na přijímání SMS zpráv. SMS zprávy se odesílají z objektu pomocí GSM brány, kdy lze nastavit hovor jako poplachovou nebo informační zprávu a mohou být zasílaný paralelně i majiteli objektu. Důležité je si uvědomit, že v případě přetížení sítě v dané lokalitě, se může doručení SMS výrazně zpozdít, ze zákona mají operátoři na doručení až 72 hodin. [13]

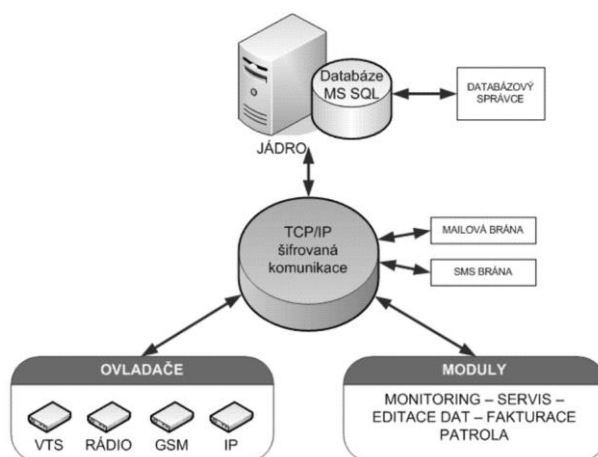
5.2.4 Radiový přenos na vyhrazených frekvencích

Hlavní a největší předností tohoto typu je zajisté to, že radiová přenosová trasa je jedinou trasou určenou výhradně pro účely přenosu dat z poplachových přenosových systémů. Dalšími nespornými výhodami jsou například: přenosová trasa je po registraci u Českého telekomunikačního úřadu (ČTÚ) zcela pod kontrolou provozovatele DPPC, jedná se o nejrychlejší způsob přenosu, je obtížně napadnutelná, zasílání zpráv není zpoplatněno. Nevýhodou mohou být ovšem poměrně vysoké finanční náklady na zřízení vlastního vysílače, v opačném případě může být vysílač ve vlastnictví DPPC a zákazníkovi jej pouze pronajímat za měsíční poplatek.

5.2.5 Internet – KRONOS

Využití internetové cesty je velmi efektivní, nevýhodou může být ovšem nedeklarovaná stabilita připojení a možnost napadení hackerem.

Zástupcem moderního přístupu za využití internetu je zcela jistě KRONOS NET 2.0 REVOLUTION od polského výrobce Next! s.c. KRONOS je plně síťové softwarové řešení pro monitorovací a dohledová centra. Slouží pro efektivní zpracování a správu přijímaných stavů z elektronických systémů. Poskytuje možnost vzdálené správy, report informací o chybách, dynamické přepínání na záložní centra, samostatnou práci jednotlivých složek systému, neudrzuje v paměti zbytečné informace a automaticky upozorňuje na důležité skutečnosti. Jeho funkce se dají shrnout slovy otevřenost a modularita, kdy na základě potřeb zákazníka je možné připojení a následný report přes mnoho různých přenosových tras. Na následujícím obrázku je pro názornost zobrazeno schéma systému KRONOS. [14]



Obr. 5: Blokové schéma systému KRONOS NET 2.0 REVOLUTION [15]

II. PRAKTICKÁ ČÁST

6 POPIS OBJEKTU

Popisovaný objekt se nachází blízko od centra města. Jedná se o budovu, která má fyzický podklad, ale pro návrh a vizualizaci v práci je vytvořen objekt fiktivní se stejnou lokací. Skutečná budova je k dispozici pro pronájem nebo prodej a je předurčena pro skladovací, obchodní nebo výrobní podmínky.

Půdorys celého objektu a jednotlivých místností uvnitř něj je podle mého návrhu, jak by měl objekt vypadat po odkoupení, rekonstrukci a před samotným započítáním instalace bezpečnostních zařízení. Jde tedy o rekonstrukci, při které lze rovnou provést zabezpečení objektu.

Pro vizualizaci 3D objektu jsem využíval volně dostupného programu Google SketchUp a pro tvorbu půdorysů a jednotlivých 2D výkresů pak studentskou verzi programu AutoCAD. Veškeré výkresy jsou elektronickou přílohou práce a také přílohami samotné bakalářské práce.

Adresa: Průmyslový areál Rybníky

760 01 Zlín

(budova č. 315)

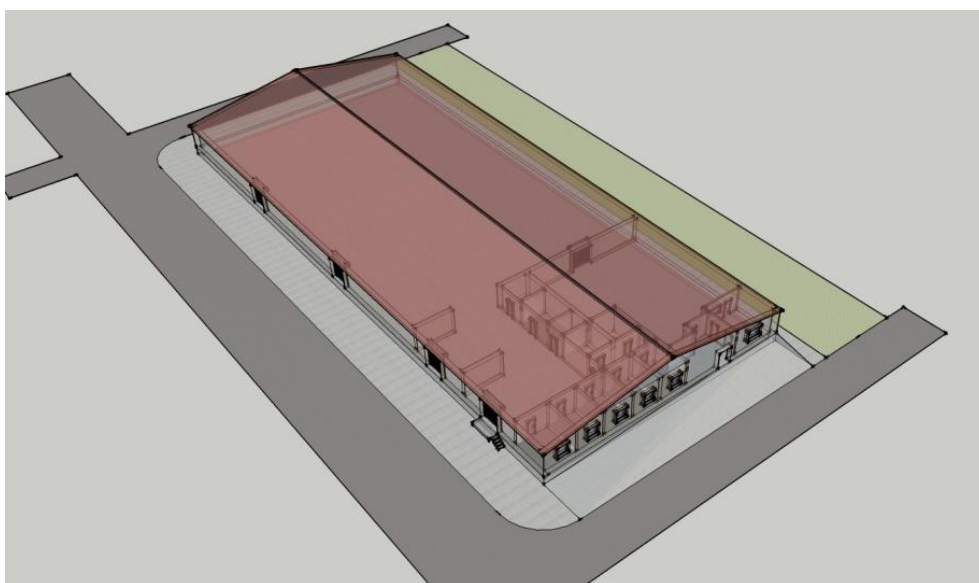
GPS: N 49°13.59930', E 17°39.98003'



Obr. 6: Umístění objektu [16]

Parametry objektu:

- Počet místností: 17
- Tloušťka stěn:
 - Obvodové zdi: 50 cm
 - Nosné zdi: 50 cm
 - Příčky: 30 cm
- Zastavěná plocha: 2100 m²
- Užitná plocha: cca 2000 m²
 - Sklad: cca 1400 m²
 - Prodejna: cca 270 m²
 - Expediční prostory: cca 170 m²
 - Užitkové místnosti: cca 160 m²
- Orientace hlavního vstupu: SZ
- Otvory:
 - Obvodová okna: 6
 - Obvodové dveře: 1
 - Vnější vrata: 4
 - Vnitřní okna: 1
 - Vnitřní dveře: 15
 - Vnitřní vrata: 1

*Obr. 7: Vizualizace objektu*

7 BEZPEČNOSTNÍ POSOUZENÍ

Bezpečnostní posouzení je prováděno vždy při návrzích poplachových systémů, přičemž se snažím analyzovat veškeré možné faktory, které tento návrh a samotný systém ovlivňují.

Cíle bezpečnostního posouzení:

- je odhalení v průběhu přípravy systémového návrhu faktory mající vliv na volby komponent a jejich umístění,
- stanovení požadovaného stupně zabezpečení. [17]

Bezpečnostní posouzení bere v úvahu čtyři základní oblasti, které by se měli posuzovat a jedná se o zabezpečované hodnoty, budovu, vnější a vnitřní vlivy.

Posouzení bezpečnosti ve spojitosti zabezpečovaných hodnot a budovy je součástí analýzy rizik, kde je cílem stanovení stupně zabezpečení podle ČSN EN 50131-1 ed.2.

Cílem posouzení vnitřních a vnějších vlivů (společně nazývány jako ostatní vlivy) je zhodnocení podmínek uvnitř a vně zabezpečovaných prostor a v závislosti na výsledcích pak správná volba a umístění komponent.

7.1 Analýza rizik

7.1.1 Zabezpečované hodnoty

a) Druh majetku

Největším podílem na aktivech společnosti se podílí samotné jednotky nápojů, ať už se jedná o drobné lahve, barely nebo sudy. Dále jsou součástí prodeje cigarety a pochutiny.

Nedílnou součástí je vozový park činící tři nákladní vozidla a výpočetní technika sloužící potřebám prodeje a vedení společnosti.

Lahve s alkoholem a cigarety jsou nejatraktivnější pro různé potulné pachatele, kteří představují pro objekt velké riziko. Atraktivní mohou být i jednotlivé části výpočetní techniky nebo vozidla, avšak jejich odcizení a následné zpeněžení není zcela snadné a výnosné.

b) Hodnota majetku

V následující tabulce je zobrazena maximální hodnota částí majetku, jedná se o kompletní cenu předpokládaného majetku a pro přesnost je zde uvedena i hodnota majetku, který lze při pokusech o napadení a krádež poškodit a následně je nutné jej opravit.

Tab. 2: Hodnota majetku

Majetek	Celková hodnota v Kč
Vozový park	4.000.000
Výpočetní technika a elektronika	200.000
Zboží – nápoje	25.000.000
Zboží - ostatní	1.000.000
Vybavení (nábytek, skladovací boxy, atd.)	400.000
Poškoditelný majetek (okna, dveře, atd.)	500.000

c) Množství nebo velikost

V objektu se nachází několik set druhů nápojů a dalšího zboží uskladněném ve skladu v bednách nebo samostatně v policích v prodejně. Jejich odcizení, následná manipulace, transport a další nakládání s tímto majetkem nepředstavuje pro pachatele příliš velké obtíže. Z toho důvodu je tento majetek považován pro pachatele za velmi atraktivní na rozdíl od dalšího vybavení objektu a vozového parku. Je zde nutné tedy zabezpečit tyto aktiva před samotným zcizením a to především zabráněním přístupu k nim, nebo včasným odhalením a dostižením pachatele.

d) Historie krádeží

Objekt se bude teprve zřizovat, tudíž na něj doposud nemohly být spáchány pokusy o vloupání a krádeže. Je zde možné vycházet z okolních průmyslových objektů a přilehlého skladu potravin. Do okolních objektů se pachatelé dostali, nebo se snažili dostat především pomocí rozbití oken nebo dveří s cílem odcizit drobný majetek, jako potraviny, alkohol, cigarety, výrobky, drobné elektrospotřebiče nebo ponechané peníze.

e) Nebezpečí

Nebezpečí pro objekt představují málo obývané prostranství v okolí objektu, množství stavebního materiálu a odpadu v okolí, který by mohl posloužit při snaze o vniknutí do chráněných prostor nebo poškození konstrukce budovy.

f) Poškození

V místech, kde se nachází zabezpečovaný objekt je možné riziko vandalizmu, neboť zde není příliš rušný provoz ve večerních a nočních hodinách. Poškození vandalizmem se vztahuje především na poškození vnějších částí budovy popř. poškození přistavených vozidel.

7.1.2 Budova

V bezpečnostním posouzení budovy se hodnotí faktory, které souvisejí se samotným objektem, ve kterém bude PZTS zřizován a nainstalován.

a) Konstrukce

Pro popis jednotlivých konstrukčních prvků budovy jsem zvolil formu tabulky s uvedeným prvkem a použitým materiálem.

Tab. 3: Konstrukce budovy

Konstrukční prvek	Použitý materiál
Obvodové stěny	Pálené cihly
Vnitřní stěny	Stavební bloky YTONG
Stropy vnitřních místností	Stropní keramické desky
Střecha	Plechové pláty
Podlaha	Železobeton

b) Otvory

Otvory pláště budovy tvoří okenní výplně, vstupní dveře a vrata od skladovacích prostor. Dalšími otvory není objekt vybaven. Použitý materiál a konstrukce je popsána v tabulce:

Tab. 4: Otvory pláště budovy

Otvor	Konstrukce
Okna	Dřevěné rámy
Vstupní dveře	Železné zárubně a dřevěné dveře
Vrata od skladu	Slitinové rolovací vrata

c) Režim provozu objektu

Objekt je využíván podle tabulky otevírací doby pro prodejní účely. Zaměstnanci společnosti vstupují a opouštějí budovu 30 minut před a po zahájení prodejní doby. Mimo pracovní dobu se v objektu nenachází žádní zaměstnanci kanceláří, s výjimkou závozníků a skladníků, kteří se mohou vrátit na firmu i po pracovní době v závislosti na zpoždění a možných zdržení při rozvozech, vše za přítomnosti a s vědomím vedoucího směny.

Vstup do objektu je zákazníkům umožněn jen v otevírací době, mimo tento čas pouze po domluvě s vedoucím. Prostory, do kterých může zákazník vstoupit, jsou striktně vymezeny v prostorách prodejny, vstupní haly a v případě potřeby také v chodbě ke kancelářím.

Tab. 5: Otevírací doba

Den	Otevírací doba
Pondělí - pátek	6:30 – 17:00
Sobota	7:00 – 12:00
Neděle a svátky	zavřeno

d) Držitelé klíčů

Klíče od hlavního vstupu má k dispozici ředitel, zástupce ředitele a vedoucí směny. Další klíče by měla mít k dispozici i firma zajišťující dohled a kontrolu. V místnosti vedoucích je skříňka s klíči, ke které mají přístup pouze vedoucí a při zahájení směny vydají potřebné klíče svým podřízeným, při ukončení směny se všechny klíče vrací vedoucím, kteří objekt opouštějí jako poslední.

e) Lokalita

Míra kriminality v okolí zabezpečovaných prostor je značná, jedná se především o vloupání a poškozování majetku. V okolí se nacházejí další budovy, které mohou představovat jak další možné zájmy, tak i možné ukrytí pachatelů.

Jedná se o lokalitu, která je sice součástí centra města, ale je odlehlou průmyslovou zónou, kde se nepohybují pěší osoby. Pohyb osob je zde především v rámci návštěvy některé z okolních firem. Odezva kolemjdoucích a nejbližších obytných budov na signalizaci PZTS vnější sirénou a majákem je tedy většinou velmi dlouhá a někdy nemusí být žádná. Proto je nutné tuto signalizaci o napadení přenést na dohledové centrum, ze kterého je veden zásah k objektu.

f) Stávající zabezpečení

Nynější zabezpečení obstarávají pouze základní prvky MZS, tj. starší dřevěná okna s obyčejnými skly, dřevěné dveře a dřevěné vrata. Elektronické zabezpečení zde ještě nebylo dříve zřizováno.

g) Historie krádeží, loupeží a hrozeb

V minulosti nebyl tento objekt vystaven krádežím a loupežím, ale v případě jeho zřízení na obchodní objekt toto riziko vzniká a může být velmi vysoké. Předpokládané hrozby v době mimo otevírací dobu spočívají především v průniky skrz okna, dveře a zcizení zboží nebo ponechané hotovosti. V době prodeje je zde možné počítat s krádežemi zboží přímo v prostorách prodejny, která je oddělené od skladovacích prostor.

7.2 Ostatní vlivy

7.2.1 Vnitřní vlivy

Na správnou funkci PZTS má vliv mnoho faktorů, které mají původ ve střežených prostorách. Většinou jsou tyto faktory ovlivnitelné a je možné je redukovat nebo zcela eliminovat v případě, kdy mají významný negativní vliv na PZTS. Dle vnitřních vlivů je vhodné zvolit správný výběr, umístění a nastavení komponentů. [17]

a) Vodovodní potrubí

Do místností jako jsou toalety, sprchy a úklidová místnost jsou přivedeny vodovodní rozvody za pomoci plastových potrubí, zde je nutné dbát na vliv pohybu vody v nich při nasazení mikrovlnných detektorů.

b) Vytápění, vzduchotechnické a klimatizační systémy

Vytápění je založeno na vlastním kotli a otopné panely jsou vyvedeny do všech místností a do skladovacích prostor na straně se vstupy zvenčí. Klimatizační systém je nainstalován do skladovacích prostor a také do samotných kanceláří a prodejny.

Turbulence vzduchu při aktivním vytápění nebo klimatizaci je potřeba brát v úvahu při nasazení ultrazvukových detektorů.

c) Vývěsní štítky nebo předměty

V prostorách skladu ani dalších místností se nenacházejí vývěsní štítky ani žádné podobné předměty, které by mohli mít vliv na funkci detektorů pohybu. Pouze nad prostory skladu a prodejny jsou zavěšeny lampy osvětlení, ale tyto by neměli mít možnost nevyžádaného pohybu. Reklamní tabule a štítky jsou uvnitř i vně objektu umístěny napevno.

d) Zdroje světla

Osvětlení objektu je založeno na LED panelech, které nemají vliv na použité technologie, ovšem je nutné brát v úvahu projíždějící vozidla, která by mohla osvětlovat skrze okna nainstalované PIR detektory, ty je nutné umístit tedy na vhodná místa.

e) Elektromagnetické rušení

V objektu může vznikat EM rušení od paletových vozidel, která jsou poháněna elektromotory, dále pak jsou elektromotory využity v čerpadle kotle, klimatizace, popř. v další elektronice, kde patří například lednice a mrazničky.

f) Divoká nebo domácí zvířata

V samotném objektu se žádná domácí ani divoká zvířata nevyskytují, ovšem v okolí objektu je vysoce pravděpodobný výskyt zatoulaných zvířat, jako jsou psi a kočky, které by mohli mít vliv na použité a nainstalované detektory pohybu a další.

g) Průvan

V prostorách skladu, prodejny i kanceláří je možný vznik průvanu, při ponechaných otevřených oknech a dveřích. V době střežení objektu jsou všechny otvory uzavřeny a není zde ponechána možnost na vznik průvanu, který by mohl mít vliv na bezpečnostní systém.

h) Uspořádání skladovaných předmětů

V prostorách prodejny i skladu jsou předměty a jednotlivé položky zboží umístěny v prodejních a skladovacích policích, jejich rozmístění je stálé a je tedy možné nastavit a rozmístit detektory na vhodná místa. Pozor je nutné si dát v případě odstavení paletových vozidel, které je nutné odstavit vždy na konci směny na k tomu určená místa.

i) Stavební konstrukce střežených objektů

Stavební konstrukce jsou popsány již v Tab. 3, v případě oken a dveří je zde brát v úvahu, že se jedná o nová okna, která nezpůsobují velké změny teplot ve střežených prostorách.

j) Riziko planých poplachů u tísňových systémů

V případě instalace tísňových hlásičů, je potřeba je umístit na vhodná místa, aby nedocházelo k neúmyslnému spuštění. Dalším krokem je vhodné obeznámit o jejich funkci zaměstnance.

7.2.2 Vnější vlivy

Na správnou funkci PZTS se podílí i vlivy, které pocházejí z okolí střežených prostorů. Tyto vlivy není možné nijak zásadně ovlivnit a je nutno je brát v úvahu při návrhu PZTS. Především se zde jedná o vhodnou volbu typu a umístění jednotlivých komponentů. [17]

a) Dlouhodobě působící faktory

V okolí se nacházejí silnice a cesty, po kterých se pohybují osobní i nákladní automobily, vedle budovy bude možnost pro odstavení firemních vozidel i vozidel pro zákazníky. Z toho je nutné zvolit vhodné umístění bezpečnostních komponentů, aby nedocházelo k negativnímu ovlivňování funkce systému nebo zastínění použitých detektorů.

b) Krátkodobě působící faktory

Mezi potřebné informace při návrhu nebo následném nastavení, či dočasném upravení systému je třeba zařadit a také počítat i s blízkými stavebními pracemi, které se zde mohou vyskytovat při rekonstrukcích okolních objektů.

c) Vysokofrekvenční rušení

V případě využití bezdrátových komponentů při instalaci bezpečnostních systémů musíme věnovat pozornost, zda se v blízkosti nevyskytují další bezdrátové systémy, výkonné vysílače, amatérské nebo profesionální radiostanice a další bezdrátové komunikační sítě.

V blízkosti posuzovaného objektu se nenacházejí žádné radiostanice ani výkonné vysílače, které by mohli mít negativní dopad na správnou funkci instalovaného systému.

d) Sousední objekty

Sousední objekty slouží jako výrobní a skladovací prostory, ve kterých mohou být využívány elektromotory a zařízení, způsobující elektromagnetické rušení.

Nejbližší objekt slouží pro skladování gumárenských výrobků a polotovarů, tudíž nemá vliv na instalované prvky PZTS. Výrobní objekty, které by mohli mít negativní vliv, se nacházejí ve vzdálenosti několika desítek až stovek metrů.

e) Vlivy klimatických podmínek

Objekt se nachází v mírném podnebném pásu, který se vyznačuje teplým létem, mírnou zimou a rovnoměrnými srážkami po celý rok. Z toho vyplývá, že komponenty nejsou vystaveny dlouhodobým negativním vlivům extrémního počasí. Ovšem i pro podmínky zdejšího klimatu je nutné vybírat detektory a komponenty, které jsou určeny pro stanovené teploty a vlhkost vzduchu. Tyto informace přímo souvisejí s třídami prostředí podle platné normy ČSN EN 50131-1.

f) Ostatní vlivy

Zde je považován za podstatný fakt možný výskyt pohybujících se osob, zvířat a vozidel z okolních objektů v blízkosti budovy, jelikož tato není oplocena ani chráněna jinými prostředky.

8 NÁVRH ZABEZPEČENÍ

Návrh systému PZTS je proces, při němž se stanovuje rozsah systému, stupeň zabezpečení, komponenty odpovídajícího stupně zabezpečení, volby protiopatření, třídy prostředí apod. Při tomto procesu dochází k výběru vhodné ústředny, způsobu provedení kabeláže, ke stanovení počtu a typu detektorů, typu ovládacích a indikačních zařízení a dalších doplňkových zařízení. Návrh systému PZTS většinou také slouží pro přibližný odhad ceny navrhovaného systému. [18]

Zjednodušený postup při návrhu PZTS je následující:

- posouzení zabezpečovaných hodnot,
- bezpečnostní posouzení objektu,
- klasifikace prostředí,
- stupeň zabezpečení,
- volba protiopatření.

Přičemž všechny výše zmíněné body představují právě samotný proces návrhu PZTS, jejichž výsledkem je dokument, tzv. systémový návrh.

Pro svou práci jsem zvolil postup, kde jsou jednotlivé kroky zpracovány jako samostatné kapitoly. Bezpečnostní posouzení a posouzení zabezpečovaných hodnot již bylo provedeno v předchozí kapitole.

8.1 Klasifikace prostředí

Při výběru je nutné zvážit prostředí, ve kterém budou jednotlivé komponenty systému EZS umístěny a ve kterém budou schopny správného a spolehlivého provozu. Toto rozdělení je znázorněno v následující tabulce vycházející z normy ČSN EN 50131-1:

Tab. 6: Klasifikace prostředí

Třída	Název	Popis	Teploty
I.	Vnitřní	Vytápěná obytná nebo obchodní místa	+5 až +40°C
II.	Vnitřní – všeobecné	Přerušovaně vytápěná/nevytápěná místa (chodby, schodiště, sklady)	-10 až +40°C
III.	Venkovní – chráněné	Komponenty nejsou trvale vystaveny vlivům počasí	-25 až +50°C
IV.	Venkovní - všeobecné	Komponenty jsou trvale vystaveny vlivům počasí	-25 až +60°C

Pro zabezpečovaný objekt jsou zvoleny následující třídy prostředí podle teplot, které jsou pro dané prostory nastaveny a udržovány pomocí vytápění a klimatizace:

- *I. Vnitřní:* kanceláře, toalety, umývárny, prodejna (+10 až +25°C)
- *II. Vnitřní všeobecné:* chodby, sklad (+2 až +20°C)
- *IV. Venkovní všeobecné:* vše vně objektu (komponenty nejsou kryty)

8.2 Stupeň zabezpečení

Rozdělení do jednotlivých stupňů zabezpečení vychází z normy ČSN EN 50131-1, která bere v úvahu především znalosti a vybavení útočníka, viz následující tabulka.

Tab. 7: Stupeň zabezpečení

Stupeň	Riziko	Prostory	Útočník
1	Nízké	Obytné objekty s méně cennými aktivy	Malá znalost PZTS, sortiment snadno dostupných nástrojů
2	Nízké až střední	Kancelářské, obytné, komerční prostory	Omezené znalosti PZTS, běžné nástroje a přístroje (např. multimetr)
3	Střední až vysoké	Banky	Obeznamení s PZTS, rozsáhlý sortiment zařízení a přístrojů
4	Vysoké	Tajné archivy, muniční sklady	Podrobný plán vniknutí, kompletní sortiment nástrojů a přístrojů.

PZTS musí být přiřazen stupeň zabezpečení, který určuje jeho provedení. Musí být zařazen do jednoho ze čtyř stupňů, kde nejnižší je stupeň 1 a nejvyšší stupeň 4. Stupeň zabezpečení celého PZTS odpovídá komponentu s nejnižším stupněm zabezpečení. [19]

Stupeň zabezpečení pro daný objekt je stanovena na stupeň 2.

Pro každý stupeň je charakteristická konkrétní volba protiopatření viz následující tabulka.

Tab. 8: Charakteristické volby protiopatření

Možné narušení	Stupeň 1.	Stupeň 2.	Stupeň 3.	Stupeň 4.
Obvodové dveře	O	O	OP	OP
Okna		O	OP	OP
Ostatní otvory		O	OP	OP
Stěny				P
Stropy a střechy				P
Podlahy				P
Místnosti	T	T	T	T
O – otevření; P – průnik; T - nástraha				

8.3 Komponenty PZTS

Pro zabezpečení objektu jsem se rozhodl využít výrobky českého výrobce a dodavatele zabezpečovací techniky, firmu Jablotron. Nová řada systému, Jablotron 100, obsahuje hybridní ústředny, které mají sběrníkové nebo bezdrátové připojení detektorů. Jedná se o zcela novou technologii této společnosti, která přináší výhody svých předchůdců. Jejich předností je moderní design, výhodná cena, dobrá dostupnost servisní a poradenské činnosti a také velmi rozsáhlý sortiment komponentů a rozsáhlé možnosti rozšíření.

Pro rekonstrukci a nové stavby je většinou výhodnější využít sběrníkové propojení, při kterém je možné značně ušetřit a nevzniká zde možnost rušení bezdrátového spojení. Zvolil jsem tedy přednostně sběrníkové prvky, které je pak možné kdykoliv doplnit o prvky bezdrátové.

Všechny prvky musí splňovat požadovaný stupeň zabezpečení a musí být vhodné pro zvolenou třídu prostředí. Vybrané komponenty systému PZTS, které jsem zvolil pro zabezpečení objektu, jsou popsány jednotlivě v následujícím textu. Pro přehlednost je přiložena i tabulka se seznamem použitých komponentů a potřebných prvků pro jejich instalaci.

Tab. 9: Seznam použitých komponentů

Položka	Označení
Sběrníková ústředna	JA-106KR
Modul ovládacího panelu	JA-192E
Akumulátor	SA214-7
PIR detektor pohybu	JA-110P
Magnetický kontakt	JA-111M
PIR detektor pohybu a rozbití skla	JA-120PB
Kombinovaný detektor kouře a teplot	JA110-ST
Přístupová klávesnice	JA-114E
Venkovní PIR detektor pohybu	JA-188P
Sířena – vnitřní	JA-110A
Sířena – venkovní	JA-111A
Univerzální instalační krabice	JA-190PL
Rozbočovač sběrnice	JA-110Z-B
Kabel – páteřní a vzdálené spoje	CC-01
Kabel	CC-02

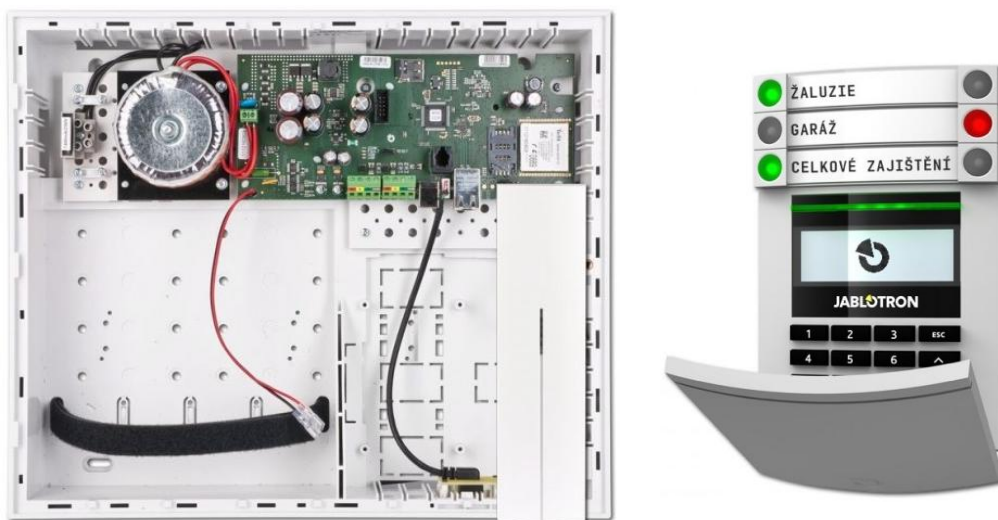
8.3.1 Ústředna JA-106KR

Ústředna JA-106 KR je určena k ochraně rozsáhlých objektů, kanceláří a firem. Nabízí také flexibilní řešení ochrany obytných komplexů, administrativních budov a firem, které potřebují systém o mnoha sekcích. Požadované nastavení a velikost systému se programují prostřednictvím softwaru F-link.

Jablotron ústředna JA-106KR nabízí:

- až 120 sběrnicevých nebo bezdrátových zón
- až 300 uživatelských kódů
- až 15 sekcí
- až 32 programovatelných výstupů
- 20 vzájemně nezávislých kalendářů
- SMS reporty ze systému až 30 uživatelům
- 5 uživatelů má možnost využívat kromě SMS i hlasové reporty
- 4 nastavitelné PCO
- 5 volitelných protokolů pro PCO
- 2 vzájemně nezávislé svorkovnice pro připojení sběrnice
- 1 konektor pro vestavěný radiový modul (JA-110R)
- 1 konektor pro komunikační modul PSTN (JA-190X)

Ústředna má vestavěný GSM/GPRS/LAN komunikátor, který umožňuje hlasovou, SMS nebo GPRS komunikaci s koncovými uživateli nebo středisky PCO. Je vybaven 1 GB paměťovou kartou pro uchování dat událostí, hlasových zpráv, ukládání snímků atd.



Obr. 8: Ústředna JA-106KR a ovládací modul JA-114E [19]

Technická specifikace ústředny JA-106KR:

Stupeň zabezpečení:	2 dle ČSN EN50131-1, ČSN EN 50131-3, ČSN EN 50131-6, ČSN EN 50131-5-3
Rádiové vyzařování:	ČSN ETSI EN 300220 (modul R), ČSN ETSI EN 301 419-1, EN 301 511
EMC:	ČSN EN 50130-4, ČSN EN 55022, ČSN ETSI EN 301 489-7
Bezpečnost:	ČSN EN 60950-1
Prostředí:	třída II. (-10 až +40°C), dle ČSN EN 50131-1
Napájení ústředny:	230 V / 50 Hz, max. 0,2 A, třída ochrany II
Napájecí zdroj:	typ A (ČSN EN 50131-6)
Identifikace volajícího:	ČSN ETSI EN 300 089
Max. trvalý odběr z ústředny:	1,2A
LAN komunikátor:	Ethernet rozhraní
GSM komunikátor QUAD-BAND:	850/900/1800/1900MHz
Pracovní frekvence (modul JA-110R):	868 MHz ISM pásmo

8.3.2 Sběrníkový přístupový modul JA-114E

Jablotron JA-114E je přístupový modul s LCD displejem, ovládacími klávesami a čtečkou RFID pro ovládání zabezpečovacího systému. Obsahuje jeden ovládací segment pro jednoduché ovládání, a pokud je potřeba, může být vybaven celkem 20 segmenty JA-192E.

Modul má dále funkci úspory energie během výpadku napájení a je adresovatelný.

Technické specifikace modulu JA-114E:

Podmínky provozování:	ČTÚ č. VO-R/10/09.2010-11
Napájení:	ze sběrnice ústředny (9...15 V)
Prostředí:	dle ČSN EN 50131-1 II. vnitřní všeobecné (-10 až +40 °C)
Frekvence:	125 kHz
Klasifikace:	stupeň 2 dle ČSN EN 50131-1, ČSN EN 50131-3
Dále splňuje:	ČSN ETSI EN 300330, ČSN EN 50130-4, ČSN EN 55022, EN 60950-1
Proudová spotřeba při záloze (klidová):	15 mA
Proudová spotřeba pro volbu kabelu:	50 mA
Každý další ovládací segment:	0,5mA

8.3.3 PIR detektor pohybu JA-110P

Jablotron JA-110P je sběrníkový detektor pohybu PIR určený pro ochranu interiéru. Charakteristiky detekce lze optimalizovat pomocí výměnných čoček.

Technické specifikace detektoru JA-110P:

Napájení:	ze sběrnice ústředny 12 V (9 ... 15 V)
Rozměry:	95 x 60 x 55 mm
Prostředí:	dle ČSN EN 50131-1 II. vnitřní všeobecné
Doporučená instalační výška:	2,5 m nad úrovní podlahy
Úhel detekce / délka záběru:	110° / 12 m (se základní čočkou)
Klasifikace:	stupeň 2 dle ČSN EN 50131-1, ČSN EN 50131-2-2
Dále splňuje:	ČSN EN 50130-4, ČSN EN 55022
Proudová spotřeba při záloze (klidová):	5 mA
Proudová spotřeba pro volbu kabelu:	5 mA
Rozsah pracovních teplot:	-10 až +40 °C



Obr. 9 Detektory JA-110P a JA-120PB

8.3.4 PIR detektor pohybu a rozbití skla JA-120PB

Slouží k prostorové detekci pohybu osob v interiéru budov a k detekci rozbití skleněných ploch tvořících plášť budov. Obsahuje dva nezávislé detektory.

K detekci pohybu osob využívá PIR senzor.

Rozbití skleněných ploch detekuje detektor tříštění skla GB na základě změn tlaku vzduchu a charakteristických zvuků rozbíjení skla.

Technické specifikace detektoru JA-120PB:

Napájení:	ze sběrnice ústředny 12 V (9 ... 15 V)
Rozměry:	60 x 95 x 55 mm
Splňuje:	ČSN EN 50130-4, ČSN EN 55022
Rozsah pracovních teplot:	-10 až +40 °C
Prostředí:	ČSN EN 50131-1 II. vnitřní všeobecné
Klasifikace	stupeň 2 dle ČSN EN 50131-1, ČSN EN 50131-2-2, ČSN CLC/TS 50131-2-7-1
Doporučená instalační výška:	2,5 m nad úrovní podlahy
Proudová spotřeba při záloze (klidová):	5 mA
Proudová spotřeba pro volbu kabelu:	5 mA
Úhel detekce / detekční pokrytí PIR:	110°/12 m (se základní čočkou)
Detekční vzdálenost rozbíjení skla:	9m (sklo min. 60x60 cm)

8.3.5 Venkovní PIR detektor pohybu JA-188P

Detektor JA-188P zajišťuje stabilní a přesnou detekci pohybu ve vnějším prostředí. Venkovní PIR detektor pohybu je založen na technologii dvouzónového detektoru pohybu společnosti OPTEX. Detekční rozsah lze nastavit od 1,4 do 12 m se zorným úhlem 85°.

Technické specifikace detektoru JA-188P:

Podmínky provozování:	ČTÚ VO-R/10/09.2010-11
Napájení:	3x Lithiová baterie typ LS(T)14500 (AA 3,6 V 2 Ah)
Stupeň zabezpečení:	stupeň 2 dle ČSN EN 50131-1, ČSN EN 50131-2-2
Splňuje:	ČSN ETSI EN 300220, ČSN EN 50130-4, ČSN EN 55022, ČSN EN 60950-1
Pracovní frekvence:	868,1 MHz, Jablotron JA-100
Třída zařízení:	IV dle ČSN EN 50131-1
Typická životnost baterie:	cca 3 roky (šetřicí režim 120 s)
Dosah - vzdálenost od ústředny:	až 300 m na přímou viditelnost
Krytí detektoru:	IP55
Rozsah pracovních teplot:	IV dle ČSN EN 50131-1
Detekční charakteristika:	12 m / 85° ; 94 segmentů
Montážní výška detektoru:	2,5 – 3,0 m

8.3.6 Magnetický detektor otevření JA-111M

Detekuje otevření dveří či oken. Má sabotážní ochranu krytu, která se aktivuje po otevření krytu. K aktivaci senzoru dochází po oddálení permanentního magnetu od senzoru.

Technické specifikace detektoru JA-111M:

Napájení	ze sběrnice ústředny 12 V (9 – 15 V)
Rozměry	26 x 55 x 16 mm, pasivního magnetu 16 x 55x 16 mm
Spotřeba	klidová 5 mA
Provozní teplota	-10 až 40 °C
Úroveň zabezpečení	stupeň 2, EN 50131-1

8.3.7 Kombinovaný detektor kouře a teploty JA-110ST

Sběrníkový detektor požáru Jablotron JA-110ST (optická a teplotní detekce) detekuje požár v obytných a komerčních budovách. Umožňuje nastavení detekce: optická a teplotní, optická nebo teplotní, pouze optická nebo pouze teplotní.

Technické specifikace detektoru JA-111M:

Napájení:	ze sběrnice ústředny 12 V (9...15 V)
Rozměry:	průměr 126 mm, výška 50 mm
Splňuje:	ČSN EN 54-5, ČSN EN 54-7, ČSN EN 50130-4, ČSN EN 55022
Poplachová teplota:	60°C až 70°C
Citlivost detektoru kouře:	$m = 0,11, 0,13$ dB/m dle ČSN EN 54-7
Detekce teplot:	třída A2 dle ČSN EN 54-5
Proudová spotřeba při záloze (klidová):	5 mA
Proudová spotřeba pro volbu kabelu:	10 mA
Rozsah pracovních teplot:	-10°C až +80°C



Obr. 10: Detektory JA-188P, JA-111M a JA-110ST

8.3.8 Vnitřní siréna JA-110A

Napájení:	ze sběrnice ústředny 12V (9...15 V)
Rozměry:	90 x 90 x 28 mm
Splňuje:	dále ČSN EN 50130-4, ČSN EN 55022, ČSN EN 60950-1
Prostředí:	dle ČSN EN 50131-1 II. vnitřní všeobecné
Siréna:	piezo elektrická, 90 dB/m
Klasifikace:	stupeň 2 dle ČSN EN 50131-1, ČSN EN 50131-4
Proudová spotřeba při záloze (klidová):	5 mA
Proudová spotřeba pro volbu kabelu:	30 mA
Rozsah pracovních teplot:	-10 až +40 °C

8.3.9 Venkovní siréna JA-111A

Napájení:	ze sběrnice ústředny 12 V (9...15 V)
Rozměry:	200 x 300 x 70 mm
Splňuje:	dále ČSN EN 50130-4, ČSN EN 55022, ČSN EN 60950-1
Stupeň krytí:	IP34D
Třída prostředí:	venkovní všeobecné -25 až +60°C
Záložní akumulátor:	NiCd pack 4,8 V / 1800 mAh životnost cca 3 roky
Klasifikace:	stupeň 2 dle ČSN EN 50131-1, ČSN EN 50131-4
Proudová spotřeba při záloze (klidová):	5 mA
Proudová spotřeba pro volbu kabelu:	50 mA
Siréna piezo elektrická:	110 dB/m (při plně dobitém akumulátoru)



Obr. 11: Vnitřní a vnější siréna JA-110A a JA-111A

8.4 Rozmístění komponentů

8.4.1 Zásady umístování komponentů

Pro volbu a instalaci jednotlivých typů komponentů je nutné vycházet z prostředí, v jakém mají být nainstalovány a dále pak pracovat. Dále jsou uvedeny příklady základních zásad pro komponenty, které mohou být v objektu použity.

PIR detektory se mají instalovat podle následujících zásad:

- pohyb pachatele kolmý na myšlený průmět detekční charakteristiky detektoru,
- umístění na pevném podkladu bez vibrací,
- možnost překrytí detekčních zón,
- vyvarovat se umístění v prostorech s předměty prudce měnící svou teplotu a dbát zvýšené pozornosti na možné turbulence vzduchu (ventilace a topení),
- nesmí být nasměrovány na okna, dveře a další otvory (možnost oslnění).

Detektor rozbití skla:

- uvnitř střežených prostor na rovnou stěnu nebo do rohu,
- žádné překážky pohlcující zvuky (silné textilní záclony apod.),
- mimo mechanizmy a zařízení vydávající výrazné zvuky či vibrace,
- dbát na možné okolní vlivy (otevření dveří – změna tlaku a řinčení klíčů)

Ústředna:

- uvnitř střeženého prostoru,
- umístění do prostoru s nejvyšším stupněm zabezpečení,
- zamezení sledování obsluhy ústředny,
- vyloučit přístup veřejnosti.

Klávesnice:

- uvnitř střežených prostor,
- umístěna tak, aby nemohly nepovolané osoby sledovat ovládání klávesnice,
- nutné zajistit potřebnou signalizaci pro účely identifikace poruch nebo poplachu.

Siréna:

- např. na průčelí objektu do výšky nedostupné bez použití žebříku nebo štaflí.

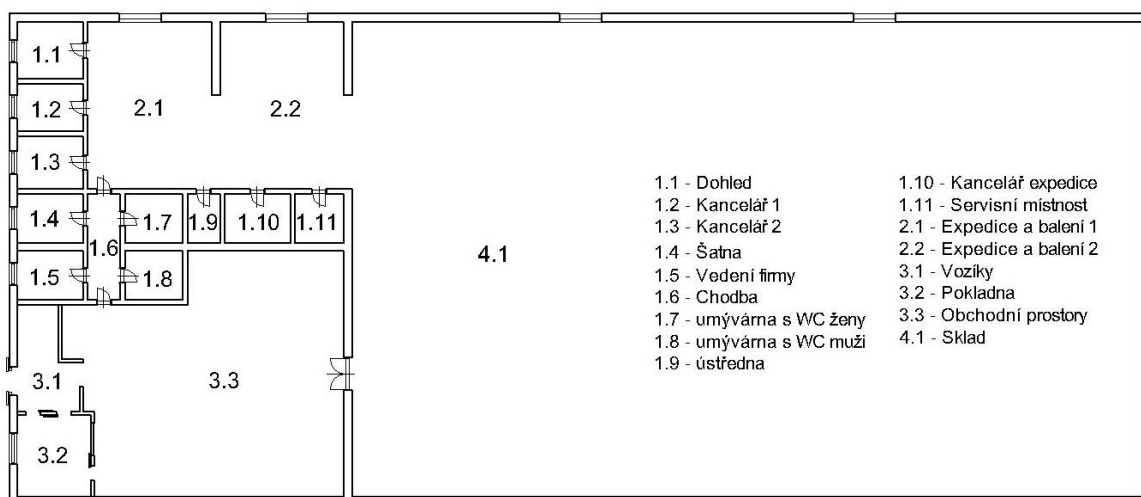
Mikrovlnné a ultrazvukové detektory nejsou pro popisovaný objekt vhodné, jelikož je zde množství kovových konstrukcí a vodovodních plastových potrubí ovlivňující činnost MW detektorů a měnící se uspořádání uložení zboží, které negativně ovlivňuje UZ detektory.

8.4.2 Rozmístění

Pro lepší přehlednost jsou v následujícím textu vloženy výřezy jednotlivých částí objektu. Celková výkresová dokumentace obsahující půdorys (P I), legendu (P II) a rozmístění komponent (P III) je pak součástí příloh práce.

Objekt je rozdělen podle následujícího obrázku na čtyři pracovní bloky:

- Blok 1: kanceláře, toalety, šatny, chodba a další užitkové místnosti (1.1 až 1.11),
- Blok 2: expediční prostory (2.1 a 2.2),
- Blok 3: prodejní prostory, pokladna a vstupní hala (3.1 až 3.3) a
- Blok 4: sklad (4.1)



Obr. 12: Pracovní rozdělení objektu

- Blok 1 a blok 2

V kancelářích, chodbě a v servisní místnosti (1.9), ve které je nainstalována ústředna, jsou použity pro zajištění okenních výplní detektory otevření oken, které jsou doplněny ve všech výše uvedených místnostech PIR detektory pohybu. Pro všechny místnosti platí umístění detektorů v horních rozích ve výšce cca 2,5 m podle výkresové dokumentace s ohledem na následné rozmístění nábytku.

Další jsou expediční prostory, v nichž je nutné zabezpečit dvoje vrata, která jsou proto vybavena detektory otevření a prostorovou ochranu zde zajišťují PIR detektory pohybu.

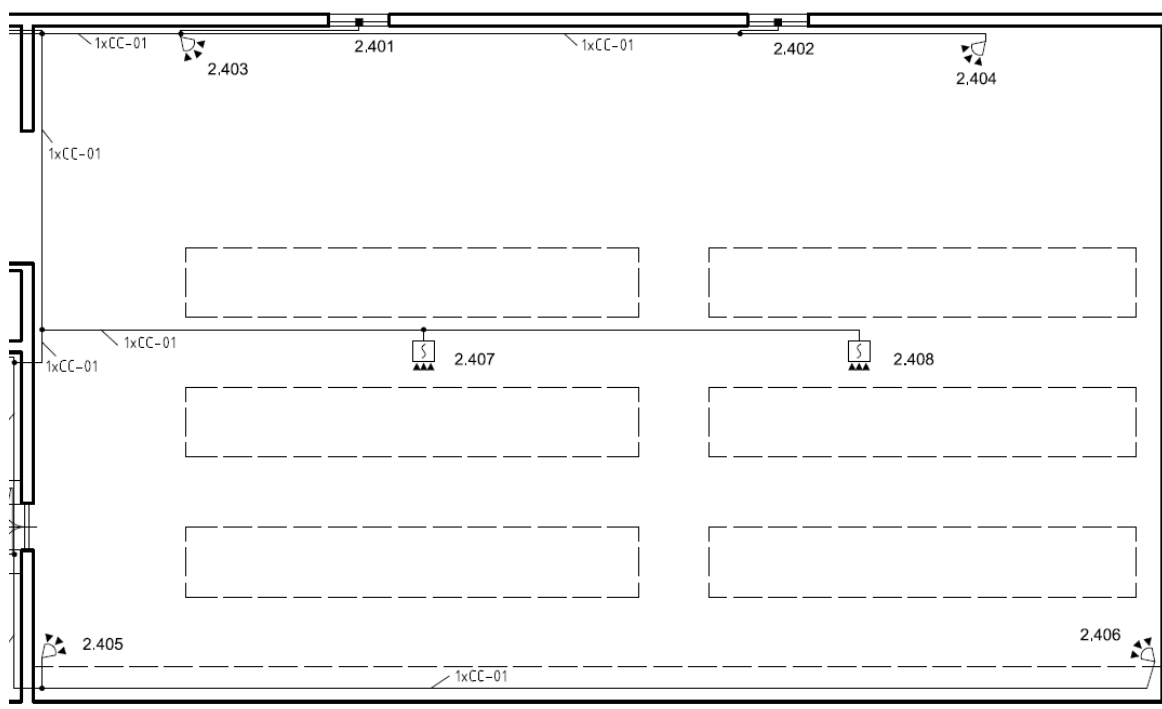
V ostatních místnostech pracovních bloků 1 a 2 není nutné použít další detektory pohybu, jelikož při snaze dostat se do těchto prostor by narušitel musel projít některou z okolních místností, které jsou střeženy. Posledním prvkem je venkovní PIR detektor umístěn vedle levých vrat.

c) Blok 4

Poslední pracovní blok je sklad, u kterého nejsou žádná okna, ale nacházejí se zde dvojce vrata, stejně jako v předchozím bloku, jsou i zde vybavena magnetickými detektory otevření.

Oblast kolem vstupních vrat je střežen detektory pohybu, které mají se základní čočkou detekční dosah cca 12 metrů, proto budou umístěny ve vzdálenosti cca 5 metrů od bližší hrany vrat. Prostorová ochrana je zde dále doplněna o detektory v rozích protější stěny, kde levý PIR detektor slouží pro detekci pohybu v oblasti průchodu z prodejních prostor a pravý detektor je zde zvolen pro zvýšení střeženého prostoru.

Stejně jako v prodejních prostorech je i zde jako doplnění PZTS o detektory požáru, které budou umístěny u stropu, hřebene střechy.



Obr. 15: Rozmístění detektorů v bloku 4

8.5 Konfigurace systému

V následujících informacích je uvedena konfigurace systému, která vychází z funkcí jednotlivých místností a rozmístění komponent. Mezi základní informace zde budou patřit údaje vztahující se k rozdělení místností do sekcí, zapojení komponentů, nastavení jednotlivých částí systému a možnosti jeho střežení.

8.5.1 Rozdělení do sekcí a možnosti střežení

Ústředny řady JA-100 umožňují nastavení několika sekcí, které lze střežit nezávisle, nebo v případě nastavení i závisle na ostatních, a je možné pro každou z nich mít vlastní ovládací a signalizační modul, který je volitelnou součástí a doplňkem ovládací klávesnice. Pro daný objekt jsou zvoleny celkem 3 sekce, kterými jsou:

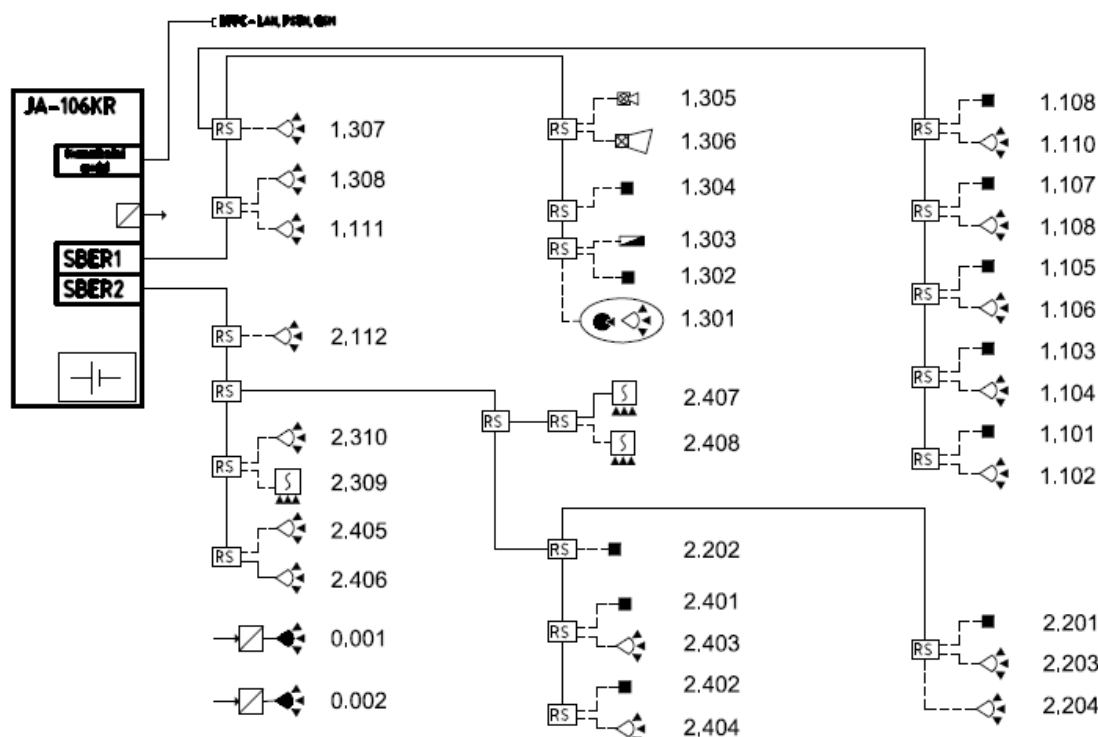
- 1 – „obchod a vedení“, (místnosti: 1.4, 1.5, 1.6, 3.1, 3.2 a 3.3)
- 2 – „expedice a sklad“ a (místnosti: 1.1, 1.2, 1.3, 1.9, 2.1, 2.2 a 4.1)
- 3 – „vnější prostory“.

Pro jednotlivé sekce platí následující pravidla:

- sekci „expedice a sklad“ lze zastřežit samostatně
- při zastřežení sekce „obchod a vedení“ se zastřeží i sekce „expedice a sklad“,
- při zastřežení sekce „vnější prostory“ se zastřeží celý objekt

8.5.2 Zapojení komponent

Následující blokové schéma zobrazuje strukturu zapojení jednotlivých komponent PZTS k ústředně pomocí sběrnice. Kompletní výkres zapojení je součástí příloh práce (P IV).



Obr. 16: Zapojení komponent k ústředně JA-106KR

Každý komponent použitý v systému má svou jedinečnou adresu, která je zde brána s ohledem na číslo sběrnice, místnosti instalace a pořadí komponentu.

Adresy a veškeré informace jednotlivých komponentů, místností a sekcí jsou uvedeny v příloze práce (P V).

8.6 Výpočet náhradního zdroje napájení

Napájecí zdroje musí splňovat požadavky normy ČSN EN 50131-6 odpovídající stupni zabezpečení a třídě prostředí. Rozlišují se zde tři typy napájení, přičemž ústředna JA-106KR je vybavena typem A, který obsahuje základní napájecí zdroj, např. síťový zdroj, a náhradní napájecí zdroj dobíjený PZTS, např. akumulátor dobíjený PZTS.

Pro napájecí zdroj typu A pro 2. stupeň zabezpečení dle ČSN EN 50131-1 platí:

- minimální doba napájení náhradním napájecím zdrojem: 12 hodin a
- maximální doba nabíjení náhradního napájecího zdroje na 80% maximální kapacity: 72 hodin.

Následující tabulka obsahuje seznam a počty jednotlivým komponentů, které mají nenulový proudový odběr, kde I_k je klidový proud a I_p proudový odběr při poplachu. Konstanta 1,2 ve vzorci pro výpočet kapacity náhradního zdroje (K_{NZ}) představuje snižování kapacity z důvodu stárnutí baterie.

Tab. 10: Proudové odběry

Položka	Označení	ks	I_k [mA]	I_p [mA]	I_{kc} [mA]	I_{pc} [mA]
Ústředna	JA-106KR	1	25	25	25	25
Modul ovl.	JA-192E	3	10	10	30	30
PIR	JA-110P	16	5	5	80	80
magnet	JA-111M	11	5	5	55	55
PIR+GB	JA-120PB	1	5	5	5	5
požární	JA-110ST	3	5	10	15	30
klávesnice	JA-114E	1	15	50	15	50
Siréna IN	JA-110A	1	5	30	5	30
Siréna OUT	JA-111A/AO	1	5	50	5	50
Celkem					235	355

$$K_{NZ} = ((12 - 0,25) \cdot I_k + 0,25 \cdot I_p) \cdot 1,2 \text{ Ah}$$

$$K_{NZ} = ((12 - 0,25) \cdot 0,24 + 0,25 \cdot 0,36) \cdot 1,2 = 3,42 \text{ Ah}$$

Jelikož kapacita náhradního zdroje musí být alespoň 3,42 Ah, je možné využít nejlevnější akumulátor s kapacitou 7 Ah s označením SA214-7.

8.7 Připojení na DPPC

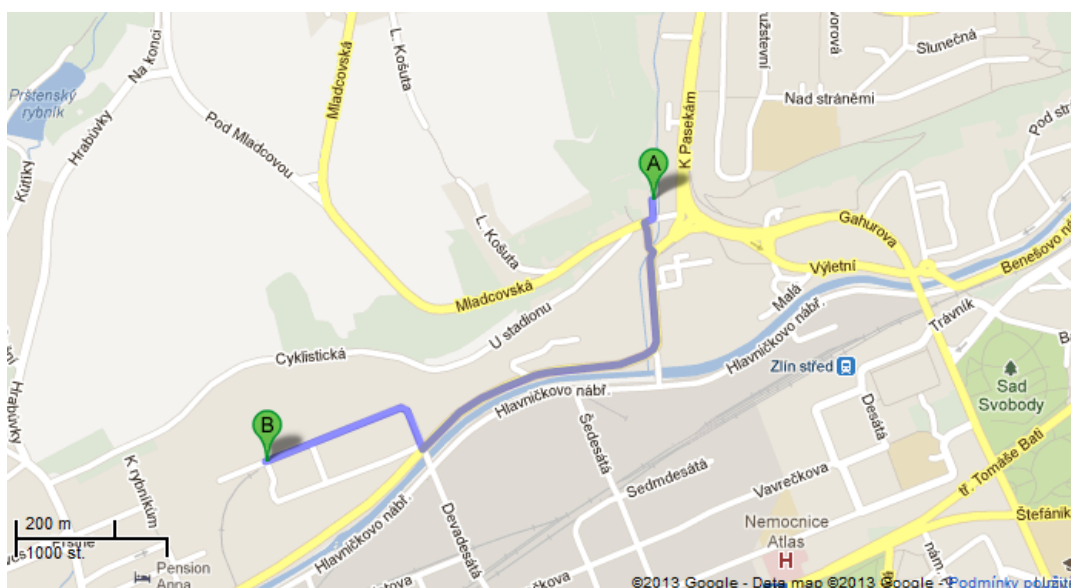
Jak již bylo v popisu komponent uvedeno, ústředna disponuje vestavěným GSM/GPRS/LAN popř. PSTN komunikátorem, který umožňuje hlasovou, SMS nebo GPRS komunikaci s koncovými uživateli nebo středisky DPPC.

Pro přenos zpráv je zvolen primárně radiový komunikátor, který je jištěný LAN komunikátorem. Radiový přenos představuje systém, u kterého je přenos zpráv zdarma, nejvyšší bezpečnost komunikace s DPPC, ale na druhé straně je pak vyšší pořizovací cena zařízení. Pro LAN komunikátor je výhodou nízká cena zařízení, nejnižší poplatky za provoz, ale nevýhodou pak nutnost internetového připojení v objektu a také nelze ovlivnit výpadky internetu od poskytovatele. Pomocí LAN je ovšem možné přenášet libovolná data a je možné mít zprovozněn i dálkový přístup k jednotlivým systémům.

Firmu pro zabezpečení jsem zvolil firmu SYSTEM plus Zlín, s.r.o, která je ve Zlínském kraji velmi známá, nabízí množství služeb a pro zabezpečovaný objekt má značnou výhodu v její vzdálenosti. Společnost zajišťuje především provoz DPPC s vlastním výjezdem a s garancí dojezdu s možností se připojit pomocí vlastní rádiové sítě NAM Global, telefonem, GSM/GPRS sítí, provoz pultu požární ochrany a připojení EPS na HZS Zlínského kraje, projekce, montáž, revize, servis a další kontroly a připojení PZTS na Městskou policii.

Adresa provozovny Zlín: Pod Babou 4260, Zlín, 760 01

Vzdálenost od objektu: cca 1,2 km s dojezdem do 5 minut



Obr. 17: Dojezd mezi objektem a DPPC [16]

8.8 Zásah

V případě aktivace poplachu PZTS některým z vnějších detektorů je zkontrolován záznam z kamerového systému (je-li nainstalován) pro ověření a potvrzení poplachu nebo označení jej za falešný poplach. Dojde-li k aktivaci alarmu z vnitřních prostor (nebo prostor, které nejsou pod dohledem CCTV), je k objektu vyslána zásahová jednotka příslušného DPPC, která provede obhlídku objektu a v případě zjištění nevýznamného důvodu se pokusí tento problém odstranit. Je-li zjištěn průnik skrz plášť budovy, je přivolána policie a majitel objektu, společně dojde k zajištění a prohlídce prostor, je povolána fyzická ochrana, která zajistí objekt na nezbytně nutnou dobu potřebnou k opravě a uvedení objektu a systému do bezpečného stavu. Během všech fází a možností spolupracuje dispečer DPPC a zásahové jednotky na informování a aktuálním stavu.

8.9 Údržba a servis

Doporučení pro pravidelnou údržbu a kontrolu PZTS a celého systému je četnost alespoň jednou za 12 měsíců. U bezdrátové verze je nutné si dávat pozor na životnost baterií.

Pravidelná kontrola – Provádí správce PZTS nebo servisní organizace a zahrnují především vizuální kontrolu komponent systému a popř. i funkční zkoušku (např. požární hlásiče zapojené v PZTS). Výsledky kontroly se zapisují do provozní knihy.

Pravidelná údržba – Obsahuje prohlídku a funkční zkoušku. Jednotlivé činnosti jsou doporučené a je vhodné je stanovit v souladu s technickým provedením systému a doporučením výrobce. O každé funkční zkoušce se provede záznam v provozní knize.

Pravidelná údržba má obsahovat:

- kontrola detekce sabotáže,
- nastavení do střežení a klidu,
- příchodové a odchodové procedury,
- kontrola napájecích zdrojů,
- funkčnost detektorů,
- funkčnost tísňových komponent,
- funkčnost výstražných zařízení a
- funkčnost přenosového zařízení.

Pravidelné revize – Revize je povinen zabezpečit vlastník (uživatel) PZTS v souladu s lhůtami odpovídajícími danému prostředí instalace.

Servis PZTS – Vlastník resp. uživatel může uzavřít s kompetentní organizací Servisní smlouvu (Dohoda o periodické kontrole zařízení).

V případě zásahu (opravy) jiným subjektem než smluvené servisní organizace je nutno provést záznam do provozní knihy.

8.10 Doplnění o mechanické zábranné systémy

Jelikož elektronické zabezpečení se vztahuje na detekci a signalizaci vzniklého nebezpečí, je nutné doplnit bezpečnostní systém o mechanické zábranné prvky. Jejich úroveň a určení je dáno také podmínkami jednotlivých pojišťoven.

Doporučení, které by se mělo aplikovat v daném objektu je zajistit plášťovou, popř. i částečnou prostorovou ochranu. Výhradně se bude jednat o vstupní a výstupní otvory. Především je zde možné využít bezpečnostní zámky, dveře, rolety, mříže, apod. nebo v případě další potřeby je možné zajistit i okenní výplně bezpečnostními fóliemi. Pro návrh je dále zvoleno rozdělení na dveře, okna, vrata skladu a expedice a další:

a) Hlavní vstup a vnitřní dveře

Vnitřní dveře od jednotlivých kanceláří a místnosti s ústřednou je vhodné doplnit a zajistit alespoň obyčejnými dveřmi, které jsou vybaveny zadlabávacím zámkem s cylindrickou vložkou. Zde se může uplatnit obyčejná vložka řady FAB 100 firmy Assa Abloy.

Pro hlavní vstup je možné použít plánované francouzské dveře s cylindrickou vložkou řady FAB 2000 a vícebodovým zámkem, které by bylo vhodné doplnit rolovací mříží.

b) Okenní otvory

Okenní otvory lze zabezpečit bezpečnostní fólií, nebo pevnou mříží. Na zabezpečovaném objektu není nutnost využít tohoto zabezpečení, ale je dle mého názoru vhodné použít mříže. Ty mohou pachatele odradit nutností využít vyšší úsilí k jejich překonání.

c) Vstupní a výstupní otvory skladu a expedice

Vstupní a výstupní otvory od skladovacích prostor a míst expedice budou provedeny pomocí průmyslových rolovacích vrat firmy Lomax ze slitin hliníku, které jsou již od výrobce dodávány na míru se zámkem a pojistkami proti zdvihu. Není zde proto nutné další vybavení mechanickými zábrannými prvky.

d) Další

Mezi další mechanické zábranné prvky by se mohlo řadit doporučení o koupi trezoru na dočasné uskladňování hotovosti z prodeje a dalších cenin.

8.11 Ochrana zboží

Ochrana zboží je pro začátek plánována za pomoci dnes klasických etiket s čárovými kódy. Každý zákazník musí projít skrz pokladnu, kde je ve vozíku pomocí mobilního čtecího zařízení započítáno nakoupené zboží. Kapsářství se zde bohužel jako ve všech obchodech nelze stoprocentně vyhnout, výhodou je zde fakt, že skleněné a plastové lahve se těžce skrývají. Čárové kódy jsou již mnohdy od dodavatelů výrobků vytištěné na obalech jednotlivých výrobků, nebo je lze vytisknout na speciálních tiskárnách v ceně použitého tiskového materiálu. Pořizovací a provozní cena je tedy velmi nízká, jelikož je nutné zakoupit pouze čtecí a vyhodnocovací zařízení, popř. tiskárnu etiket.

Do budoucna je možnost rozšířit čárové kódy o RFID systém, který je především velmi rychlý a přesný, jeho pořizovací a provozní náklady jsou ovšem vyšší a je tedy nutné zvážit přínos této technologie pro menší a střední podniky.

8.12 Rozšíření o CCTV

Kamerový systém v objektu je určitě vhodným doplňkem, kdy je možné mít jednotlivé kamerové výstupy vyvedeny do dohledové místnosti a mít rychlý přehled nad děním v objektu během pracovní doby. Mimo pracovní dobu by byl systém nastaven tak, kdy při aktivaci PZTS dojde i k aktivaci kamerového systému se současným záznamem a možností vizuální kontroly objektu na DPPC.

Kamerový systém je navrhnout za pomoci IP kamer, které jsou vybaveny funkcí PoE, což představuje napájení přímo z datového vedení a také lze mít aktivní dálkový přístup, kdy si majitel může po zadání potřebných údajů prohlížet snímky z kamer kdekoliv, kde má přístup na internet.

V celém objektu jsou navrženy celkem čtyři kamery, z toho dvě vnitřní a dvě venkovní. Jedna vnitřní kamera snímá pokladní prostory a další slouží pro kontrolu expedičních prostor. Vnějšími snímanými prostory jsou prostory před hlavním vstupem a severní prostory před skladem a expedicí, kde se nacházejí parkovací místa. Přesné umístění je uvedeno ve výkresové dokumentaci v příloze práce (P III).

8.12.1 Vivotek IP8332

VIVOTEK IP8332 je venkovní All-In-One IP kamera, která nabízí kvalitní denní sledování a rovněž i noční režim díky integrovanému IR přísvitu.

- Snímací čip: 1/4" CMOS, uzávěrka 1/5 až 1/25000 s
- Citlivost (ČB s IR): 0 lx (integrovaný IR přísvit – 12x IR LED, 15 m)
- Objektiv: 3,6 mm/F1,8; horizontální úhel záběru: 56°
- Video: H-264, MPEG-4 a MJPEG; 1280x800 px s 25 fps
- Rozhraní: 10/100 Mbit/s Ethernet (RJ-45)
- Vstupy: slot paměťových karet, 1x digitální vstup, 1x alarmový vstup
- Krytí: IP66
- Pracovní teplota: -20° až + 50°C
- Napájení: 12V adaptérem nebo PoE dle IEEE 802.3af; 4W

8.12.2 Vivotek IP7161

Vnitřní 2MPx IP kamera, podpora objektivů s automaticky řízenou clonou, podpora IR přísvitů, přenos zvuku, PoE, Ethernet, možnost externího mikrofonu a reproduktoru, reléový výstup, živé sledování pomocí mobilních telefonů 2,5 a 3G, paměťový slot.

- Snímací čip: 1/3.2" CMOS, uzávěrka 1/5 až 1/40000 s
- Citlivost (barevně): 0,8 lx (podpora den/noc)
- Objektiv: 4,5 až 10 mm/F1,8; horizontální úhel záběru: 37,1° až 77,6°
- Video: MPEG-4 a MJPEG; 1600x1200 px s 15 fps
- Rozhraní: 10/100 Mbit/s Ethernet (RJ-45)
- Vstupy: slot paměťových karet, 1x digitální vstup, 1x alarmový vstup
- Pracovní teplota: 0° až + 50°C
- Napájení: 12V adaptérem nebo PoE dle IEEE 802.3af; 8W

8.12.3 Netgear GS108P

ProSafe 8portový 10/100/1000 gigabitový přepínač s 4 porty PoE.

- Porty: 4 porty 10/100/1000Mbps s PoE a 4 porty klasické 10/100/1000Mbps
- Protokoly a standardy IEEE: 802.3i 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3x flow kontrol, 802.3af DTE power via MDI
- Spotřeba zařízení: 60 W (max. včetně 4 portů s PoE)
- Provozní teplota: 0 to 40° C



Obr. 18: Vnitřní a vnější kamera Vivotek IP8332 a IP7161



Obr. 19: PoE Switch Netgear GS108P

8.12.4 IPCorder KNR-1004

Unikátní záznamové zařízení pro IP kamery, umožňující jednoduchou instalaci, řízení routeru pro vzdálený přístup a streamování zaznamenaného videa.

- Počet kanálů: až 4 IP kamery / enkodéry (videoservery)
- Komprese: H.264, MPEG-4, JPEG
- Možnosti záznamu: stálý, při detekci pohybu, při změně na digitálním vstupu
- Max. datový tok: 16Mbps
- Úložný prostor: 1HDD s max 3TB
- Přístup: z internetu, z mobilního telefonu z tabletů
- Síťové rozhraní: 1x RJ-45, 1000/100/10Mbps
- Provozní teplota: 0°C až 40°C
- Schválení a normy: CE, FCC, RoHS
- Napájení: 12V DC / 19W



Obr. 20: Záznamové zařízení IPCorder a záložní zdroj CyberPower

8.12.5 CyberPower Value800ELCD-FR

Pro zajištění bezpečnosti i při výpadcích dodávky elektrické energie je systém vybaven záložním zdrojem typu UPS firmy CyberPower, který má následující vlastnosti:

- záložní napájecí zdroj UPS 230V AC
- max. výstupní výkon 480W/800VA
- kapacita baterie 9Ah
- multifunkční LCD displej nepřetržitě zobrazuje stav UPS:
- zásuvky AC 230V (typ E/FR odpovídající ČSN) s funkcí záložního zdroje
- ochrana před přepětím
- vstupní napájecí EURO zásuvka AC 230V (IEC320C14)
- technologie Line-Interactive
- automatická regulace výstupního napětí AVR
- plně digitální řízení postavené na mikroprocesoru
- filtry pro elektromagnetické (EMI), vysokofrekvenční rušení (RFI), ochrana proti proudovým rázům a úderu blesku
- PC rozhraní USB/RS232
- součástí dodávky software Power Panel pro PC

8.13 Fyzická ochrana

Elektronické zabezpečení nezabrání průniku pachatele do střeženého objektu, nebo vzniku dalších nebezpečných situací, pouze jej detekuje a o jejich vzniku dále informuje. Toto zabezpečení lze zvýšit kombinací s mechanickými zábrannými systémy a fyzickou ochranou.

Pro zabezpečovaný objekt je ideálním řešením v době otevírací a provozní doby fyzická ochrana zajištěna z řad vlastních zaměstnanců. Podle finančních prostředků je možno mít jednoho nebo dva zaměstnance, kteří mají své stanoviště v místnosti dohledu. Plní funkci kontrolně dohledovou, kdy se v průběhu pracovní doby pohybuje pracovních po objektu a v případě instalace CCTV má na starosti jeho obsluhu a celkově dohlíží na bezpečnost v objektu a dále plní úkoly, které jsou stanoveny v pracovní smlouvě.

Mimo pracovní dobu, kdy se v objektu nikdo nenachází, je možné využít pouze fyzickou ochranu v rámci výjezdu zásahové jednotky příslušného DPPC při vyhlášení poplachu.

9 CENOVÉ ZHODNOCENÍ

Následující kapitola je věnována cenovému přehledu za jednotlivé navrhované systémy. PZTS je zde bráno jako primární volba s doplněním o MZS, CCTV a fyzickou ochranu.

Důležité je si uvědomit, že se nejedná o přesné částky, které bude nutné při realizaci zaplatit, ale jde pouze o rozpočtový návrh, ve kterém jsou zohledněny pouze výrobky, nikoliv montážní a instalační práce. I cena jednotlivých komponent se velmi rychle mění a proto může být výsledná cena o něco vyšší, ale i samozřejmě nižší.

Tab. 11: Rozpočet PZTS

Položka	Označení	ks	Montážní firma Kč/ks bez DPH	Doporučená cena Kč/ks s DPH	Montážní firma celkem bez DPH	Doporučená cena celkem s DPH
Ústředna	JA-106KR	1	5414	11944	5414	11944
Modul ovl.	JA-192E	3	60	99	180	297
baterie	SA214-7	1	338	338	338	338
PIR	JA-110P	16	348	571	5568	9136
magnet	JA-111M	11	223	367	2453	4037
PIR+GB	JA-120PB	1	781	1250	781	1250
požární	JA110-ST	3	587	963	1761	2889
klávesnice	JA-114E	1	1275	2093	1275	2093
PIR out	JA-188P	2	4269	7007	8538	14014
Sířena IN	JA-110A	1	342	561	342	561
Sířena OUT	JA-111A	1	1046	1716	1046	1716
Krabičky	JA-190PL	20	43	70	860	1400
Rozbočovač	JA-110Z-B	20	64	105	1280	2100
Kabel	CC-01	250	5	8	1250	2000
Kabel	CC-02	50	3,5	5,5	175	275
Celkem					31261	54050

Tab. 12: Rozpočet CCTV

Prvek	Označení	Počet	Cena Kč/ks s DPH	Cena celkem s DPH
Venkovní kamera	Vivotek IP8332	2	6521	13042
Vnitřní kamera	Vivotek IP7161	2	7950	15900
PoE Switch	Netgear GS108P	1	1949	1949
Záznamové zařízení	IPCorder KNR-1004	1	5939	5939
Pevný disk	WD Red 2TB	1	2453	2453
UPS	APC BK650EI	1	2850	2850
Kabel	Cat 5e	70	9	630
Celkem				42763

Rozpočet MZS zahrnuje pouze prvky, které nejsou součástí samotné rekonstrukce (např. průmyslová vrata, interiérové a vstupní dveře). Základem MZS jsou zadlabávací zámky a cylindrické vložky, doplnit je lze později mřížemi do oken a na vstupní dveře.

Tab. 13: Rozpočet MZS

Prvek	Typ	Počet	Cena Kč/ks s DPH	Cena celkem s DPH
Zadlabávací zámek (interiér)	FAB 05140	13	129	1677
Vícebodový zámek	HOBES K125	1	1341	1341
Cylindrická vložka (interiér)	FAB 100	13	211	2743
Cylindrická vložka (vstup)	FAB 2000	1	1298	1298
Celkem				7059
Doplňkové				
Okenní mříže	/	6	2500	15000
Rolovací mříže	Lomax	1	20000	20000
Celkem				35000

Pro připojení na DPPC je vycházeno z ceníků různých firem zajišťující tuto službu, proto by mohla být konečná cena rozdílná. Cena střežení komerčního objektu se pohybuje kolem 900 až 1300 Kč za měsíc, s rozdílnými podmínkami platby za výjezdy. V rámci zajištění bezpečnosti a možnosti vzniku planého poplachu pohybujícími se lidmi, zvířaty a vozidly v okolí objektu je vhodné využít vyšší úrovně dohledu, u které bývají jednotlivé výjezdy zdarma. V případě instalace kamerového systému je možné tyto možnosti zkombinovat, popř. dále smluvně stanovit pro individuální přístup, kdy je možné vnější detektory (nejvíce náchylné na falešné poplachy) kontrolovat pomocí tohoto kamerového systému bez nutnosti výjezdu zásahové jednotky.

10 VÝVOJ BEZPEČNOSTNÍCH SYSTÉMŮ

Touto poslední kapitolou bych se rád věnoval vlastnímu názoru na další vývoj bezpečnostních systémů a na základě vypracované práce také získaným poznatkům při návrhu zabezpečení komerčních i nekomerčních objektů.

V minulosti, přítomnost a zajisté i v budoucnosti bude vždy v naší společnosti nebezpečí působící na naše zájmy, ať už se jedná o vlastní život a zdraví, tak i majetek. Z toho důvodu bude vždy potřeba zajišťovat potřebnou bezpečnost. V případě ochrany objektů je nejvýhodnějším řešením začít u základních prvků mechanické ochrany a dále pak pokračovat na poplachové systémy, které ve svém základním provedení nepředstavují příliš vysoké nároky na finance.

Dnešní moderní systémy podporují ve velké míře i bezdrátové varianty, které jsou dnes velmi oblíbené, protože není nutno zasahovat do stávající stavby a jejich instalace je tak velmi snadná. V dalších krocích zabezpečení lze přistoupit k integrovaným systémům, kde spolupracuje PZTS s dalšími systémy, jako např. CCTV, ACS, EPS apod. mimo tyto bezpečnostní systémy lze využít jeden systém i pro ovládání domácích spotřebičů a vytvořit tak inteligentní domácnost s jednoduchou obsluhou.

V budoucnosti bude mnoho systémů směřovat dle mého názoru k bezdrátovým technologiím, které jsou snadné pro instalaci, a jejich cena neustále klesá, přičemž kvalita se zvyšuje. Mimo bezdrátové technologie je žádanou volbou i možnost vzdáleného přístupu a ovládání pomocí internetového připojení, což už dnes mnoho systémů také umožňuje. Je ovšem nutné zajistit bezpečnost přenosu těchto dat. Samozřejmě drátové systémy budou stále velmi využívány, neboť jejich nasazení je levnější a v mnohých případech jednoznačně výhodnější.

Pozornost bych chtěl věnovat i určení stupně zabezpečení, u kterého se podle platných norem věnujeme zkušenostem a vybavení možného pachatele. Podle mého názoru se zde může jednat o nejednoznačnou informaci. Přesnější by bylo zde rozlišovat typy objektů a případně i objem majetku.

Dalším negativním poznatkem je i neustálá změna názvosloví a zkratk, kdy podle platných norem mnohdy platí nové značení, ale obrovské množství firem je nesprávně používá, zde bych uvedl jako hlavní příklad nového značení DPPC, kdy při vyhledávání firem zajišťující tuto službu, je nutné vyhledávat staré značení PCO.

ZÁVĚR

Cílem práce bylo provést komplexní zabezpečení daného objektu fyzickými a technickými prostředky. Forma práce byla zvolena jako popis jednotlivých typů ochran, mezi které se řadí podle základního rozdělení fyzická ochrana a technická ochrana, technická ochrana v sobě dále obsahuje mechanické zábranné systémy a systémy elektronické.

Teoretická část tedy obsahovala popis výše zmíněných typů ochrany do dostatečné hloubky, která je potřebná pro další postupy v práci. V závěru teoretické části bylo poté uvedeno možné napojení na dohledové a poplachové přijímací centrum.

Praktická část práce byla založena na projektovém návrhu zabezpečení objektu. Objekt, který byl cílem práce, je fyzicky skutečná budova vhodná k prodeji či pronájmu. Projektový návrh uvažuje s verzí odkoupení objektu, jeho rekonstrukce dle představ kupce s následným uvedením do provozu jakožto velkoobchod s nápoji.

Prvním bodem, který je nutno vždy zpracovat je podání informací o objektu, kde se jedná především o jeho polohu, rozměry apod. Poté bylo provedeno bezpečnostní posouzení, které mělo za cíl zjistit veškeré vlivy, které mají na objekt vliv a které je nutné brát v úvahu při návrhu systému, výběru jednotlivých komponent a také pro volbu způsobu fyzické ochrany.

Bezpečnostní posouzení tedy tvořilo základ pro další postupy práce. Prvním bodem, který je nutno vyřešit, je klasifikace prostředí a také určení stupně zabezpečení dle platných technických norem. Následující částí práce bylo seznámení s použitými prvky systému PZTS, jejich rozmístění a zapojení. Nechybí ani volba přenosu signálu na DPPC.

Jelikož je objekt brán jako rekonstrukce, je vhodné již při návrhu komplexního zabezpečení navrhnout vhodné prvky mechanické ochrany. Bezpečnost je také zvýšena doporučením o doplnění o kamerový systém, který má v obchodních prostorách velký význam.

Veškeré návrhy jsou zpracovány v práci v podobě výkresů a tabulek a jejich cenové ohodnocení je také podstatnou součástí práce. Práce je provedena tak, aby bylo možné ji v případě realizace bez větších problémů využít v praxi.

Jak bylo v poslední kapitole s vlastním názorem zmíněno, některé informace používané v bezpečnostních systémech nejsou dle mého názoru zcela ideální, ale jejich úpravu a vývoj ukáže jako vždy až čas a praktické zkušenosti.

ZÁVĚR V ANGLIČTINĚ

The objective of the study was to make a comprehensive security physical and technical means. Form work was chosen as a description of the type of protection, among which is according to the basic division of physical protection and technical protection, technical protection within itself also contains a mechanical barrier systems and electronic systems.

Theoretical part thus includes a description of the aforementioned types of protection to a sufficient depth, which is required for further steps of work. At the end of the theoretical part was then stated the possible connection to the monitoring and alarm receiving center.

The practical part was based on the project proposal of security. The building, which was the aim of this work, is the real actual building suitable for sale or rent. Project proposal considering the purchase object its reconstruction according to the wishes buyers with subsequent commissioning as a wholesale drinks.

The first point that must always handle is submission of information on the property where it is especially the location, dimensions, etc. Then it was a safety assessment, which was aimed at identify any factors that have influence on the object which is necessary to take account when designing the system, the selection of individual components and also for selection of physical protection.

Safety assessment thus formed the basis for further work. The first point that needs to be solved is classification of the environment and also to determine the level of security according to the applicable technical standards. The following part of this work was to study the elements used in PZTS, their deployment and integration. There is also a choice of signal transmission to the ARC.

Because the object is taken as the reconstruction, it is appropriate to already the design of a comprehensive security suggest features mechanical protection. Security is also enhanced recommendation on the addition of a CCTV that is in the business great importance.

All proposals are processed at work in the form of drawings and tables and their valuation price is also a major part of the work. The work is carried out so that it can be used in practice without any problems.

In the last chapter with an attitude mentioned, some of the information used in security systems are not, in my view, entirely perfect, but their adaptation and evolution always proves to time and practical experience.

SEZNAM POUŽITÉ LITERATURY

- [1] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.
- [2] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.
- [3] LAUCKÝ, Vladimír. *Řízení technologických procesů v průmyslu komerční bezpečnosti*. Vyd. 2. Ve Zlíně: Univerzita Tomáše Bati, 2006, 101 s. ISBN 80-731-8432-X.
- [4] HANZENOVÁ, Monika. *Objektová bezpečnost a režimové opatření*. Zlín, 2011. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce JUDr. Vladimír Laucký.
- [5] IVANKA, Ján. *Mechanické zábranné systémy*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 151 s. ISBN 978-80-7318-910-5.
- [6] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I*. 3. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 123 s. ISBN 9788073188504.
- [7] IP vs. analog kamery a základní pojmy | Stasanet.cz. *Kamery a zabezpečovací systémy*. [online]. 2012 [cit. 2013-04-20]. Dostupné z: <http://www.stasanet.cz/IP-vs-analog-kamery-a-zakladni-pojmy/>
- [8] VÍTEK, Tomáš, Miroslav HUSÁK a Tomáš TEPLÝ. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.: Přístupové systémy a jejich aplikace*. 1. vyd. Zlín: VeRBuM, 2011, s. 123-137. ISBN 978-80-87500-05-7.
- [9] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.
- [10] DRGA, Rudolf. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.: Dohledová a poplachová přijímací centra a jejich další vývoj*. 1. vyd. Zlín: VeRBuM, 2011, s. 148-155. ISBN 978-80-87500-05-7.
- [11] SOVA, Antonín. *Moderní metody ochrany zboží proti zcizení*. Zlín, 2007. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce doc. Ing. Luděk Lukáš, CSc.
- [12] RFID portál. *RFID portál* [online]. [cit. 2012-11-26]. Dostupné z: http://www.rfidportal.cz/index.php?page=rfid_obecne

- [13] HOLÍK, Radek. *Logistické zabezpečení dohledových a poplachových přijímacích center*. Zlín, 2012. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce JUDr. Vladimír Laucký.
- [14] DRGA, Rudolf a Michal ŠMIRAUS. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.: Dohledová a poplachová přijímací centra a jejich další vývoj*. 1. vyd. Zlín: VeRBuM, 2011, s. 139-144. ISBN 978-80-87500-05-7.
- [15] JabloNET. *JabloNET* [online]. 2010 [cit. 2012-11-21]. Dostupné z: http://www.jablonet.cz/download/prezentace/100415_otradovice_kronos.ppt
- [16] Mapy Google. *Google* [online]. 2013 [cit. 2013-4-26]. Dostupné z: <https://maps.google.com/maps?hl=cs>
- [17] VALOUCH, Jan. FAKULTA APLIKOVANÉ INFORMATIKY. *Projektování bezpečnostních systémů*. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-5.
- [18] VYMAZAL, Michal. Návrh EZS. Softwarová podpora návrhu elektronického zabezpečovacího systému EZS [online]. 2010 [cit. 2013-04-20]. Dostupné z: <http://ezs.labskalouka.cz/?q=node/16>
- [19] ČSN EN 50131-1 ed.2. Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky. Český normalizační institut, 2011.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Systém kontroly vstupu
CCTV	Uzavřené kamerové systémy
EAS	Elektronická ochrana zboží
EPS	Elektrická požární signalizace
GSM	Globální systém pro mobilní komunikaci
HZS	Hasičský záchranný sbor
IP	Internet protocol
IZS	Integrovaný záchranný systém
JTS	Jednotná telefonní síť
MW	Mikrovlny
PIR	Passive infrared
PKB	Průmysl komerční bezpečnosti
PoE	Power over Ethernet
PSTN	Public switched telephone network
PZTS	Poplachové zabezpečovací a tísňové systémy
SBS	Soukromé bezpečnostní služby
SHZ	Stabilní hasicí zařízení
SOZ	Samočinné odvětrávací zařízení
UZ	Ultrazvuk
ZJ	Zásahová jednotka

SEZNAM OBRÁZKŮ

<i>Obr. 1: Blokové schéma ústředny PZTS.....</i>	<i>23</i>
<i>Obr. 2: Blokové schéma funkce ústředny EPS.....</i>	<i>26</i>
<i>Obr. 3: Zleva EM, AM a RF samolepící etikety.....</i>	<i>30</i>
<i>Obr. 4: Schéma poplachového přenosového systému</i>	<i>32</i>
<i>Obr. 5: Blokové schéma systému KRONOS NET 2.0 REVOLUTION</i>	<i>34</i>
<i>Obr. 6: Umístění objektu</i>	<i>36</i>
<i>Obr. 7: Vizualizace objektu</i>	<i>37</i>
<i>Obr. 8: Ústředna JA-106KR a ovládací modul JA-114E</i>	<i>48</i>
<i>Obr. 9 Detektory JA-110P a JA-120PB</i>	<i>50</i>
<i>Obr. 10: Detektory JA-188P, JA-111M a JA-11ST.....</i>	<i>52</i>
<i>Obr. 11: Vnitřní a vnější siréna JA-110A a JA-111A</i>	<i>53</i>
<i>Obr. 12: Pracovní rozdělení objektu.....</i>	<i>55</i>
<i>Obr. 13: Rozmístění detektorů v blocích 1 a 2.....</i>	<i>56</i>
<i>Obr. 14: Rozmístění detektorů bloku 3.....</i>	<i>56</i>
<i>Obr. 15: Rozmístění detektorů v bloku 4</i>	<i>57</i>
<i>Obr. 16: Zapojení komponent k ústředně JA-106KR.....</i>	<i>58</i>
<i>Obr. 17: Dojezd mezi objektem a DPPC.....</i>	<i>60</i>
<i>Obr. 18: Vnitřní a vnější kamera Vivotek IP8332 a IP7161</i>	<i>65</i>
<i>Obr. 19: PoE Switch Netgear GS108P.....</i>	<i>65</i>
<i>Obr. 20: Záznamové zařízení IPCorder a záložní zdroj CyberPower</i>	<i>65</i>

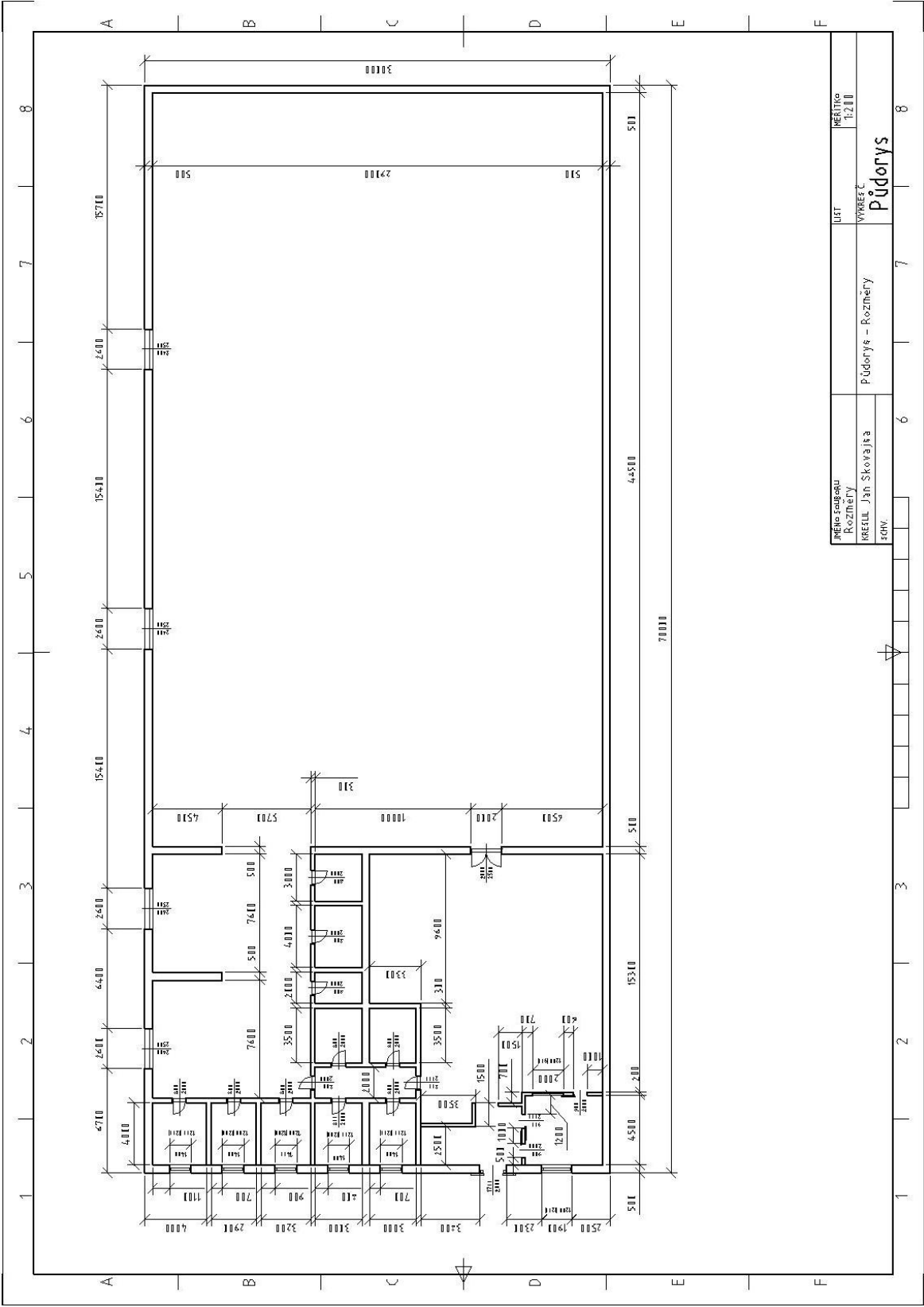
SEZNAM TABULEK

<i>Tab. 1: Vlastnosti analogových a IP kamer</i>	<i>24</i>
<i>Tab. 2: Hodnota majetku</i>	<i>39</i>
<i>Tab. 3: Konstrukce budovy</i>	<i>40</i>
<i>Tab. 4: Otvory pláště budovy.....</i>	<i>40</i>
<i>Tab. 5: Otevírací doba</i>	<i>41</i>
<i>Tab. 6: Klasifikace prostředí</i>	<i>45</i>
<i>Tab. 7: Stupeň zabezpečení.....</i>	<i>46</i>
<i>Tab. 8: Charakteristické volby protiopatření</i>	<i>46</i>
<i>Tab. 9: Seznam použitých komponentů</i>	<i>47</i>
<i>Tab. 10: Proudové odběry</i>	<i>59</i>
<i>Tab. 11: Rozpočet PZTS.....</i>	<i>67</i>
<i>Tab. 12: Rozpočet CCTV</i>	<i>67</i>
<i>Tab. 13: Rozpočet MZS</i>	<i>68</i>

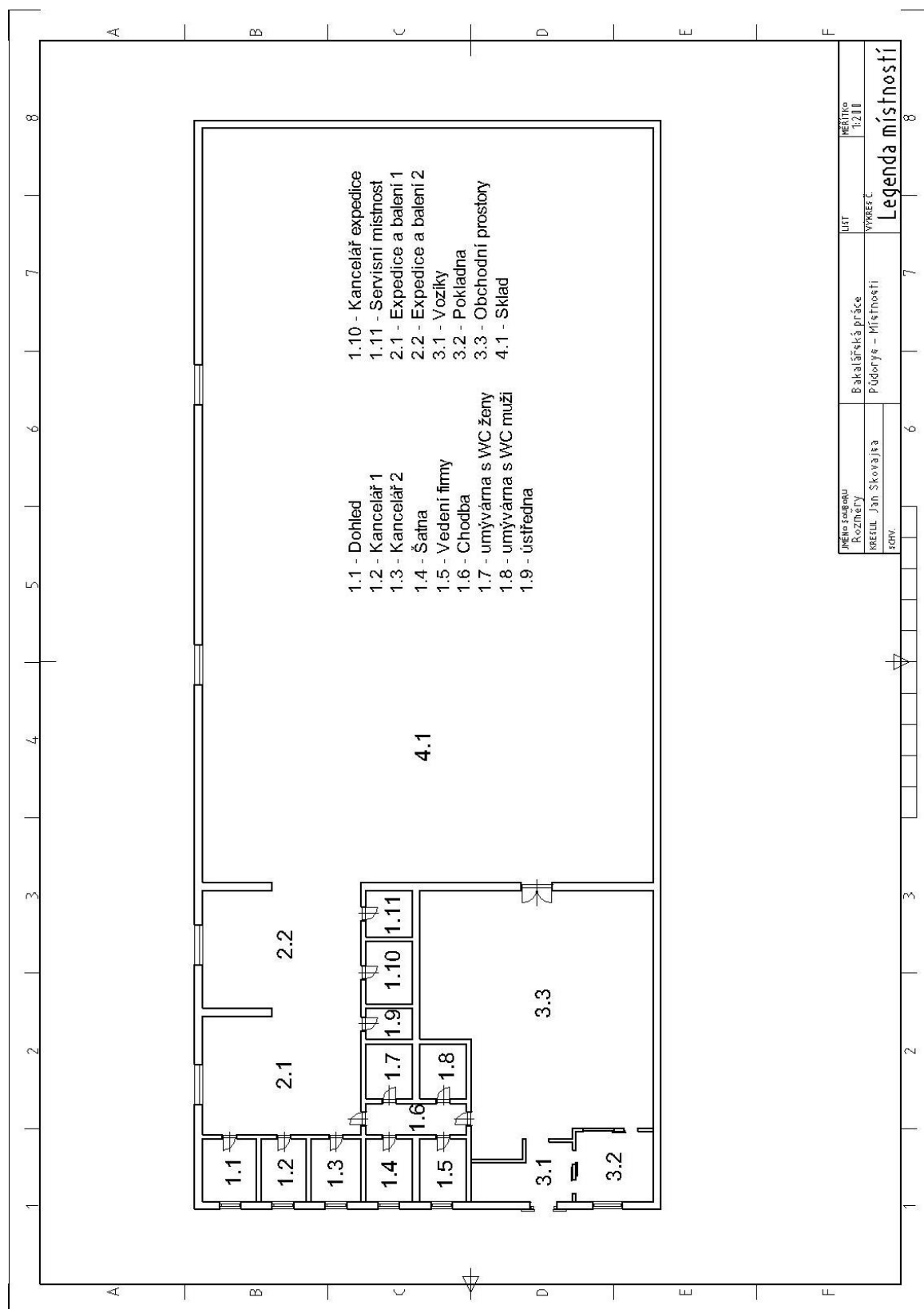
SEZNAM PŘÍLOH

PŘÍLOHA P I:	Půdorys	
PŘÍLOHA P II:	Legenda místností	
PŘÍLOHA P III:	Rozmístění	
PŘÍLOHA P IV:	Zapojení PZTS	
PŘÍLOHA P V:	Vlastnosti komponentů	
PŘÍLOHA P VI:	Vizualizace	(pouze elektronicky)
PŘÍLOHA P VII:	Ceníky a spotřeba	(pouze elektronicky)

PŘÍLOHA P I: PŮDORYS



PŘÍLOHA P II: LEGENDA MÍSTNOSTÍ



Legenda PZTS

Značka	Popis
	Ústředna
	PIR detektor pohybu
	PIR + dB
	Magnetický kontakt
	Sířena vnitřní
	Sířena venkovní
	Požární hlásič (pro PZTS)

Poznámky:

- nevyznačené kabely jsou provedeny typem CC-02 (4x0,5 mm)
- vyznačené páteřní vedení a vzdálené detektory CC-01 (2x0,8 + 2x0,5 mm)
- rozbočovací modul sběrnice JA-110Z-B

Značení detektorů : #S.#B#PP

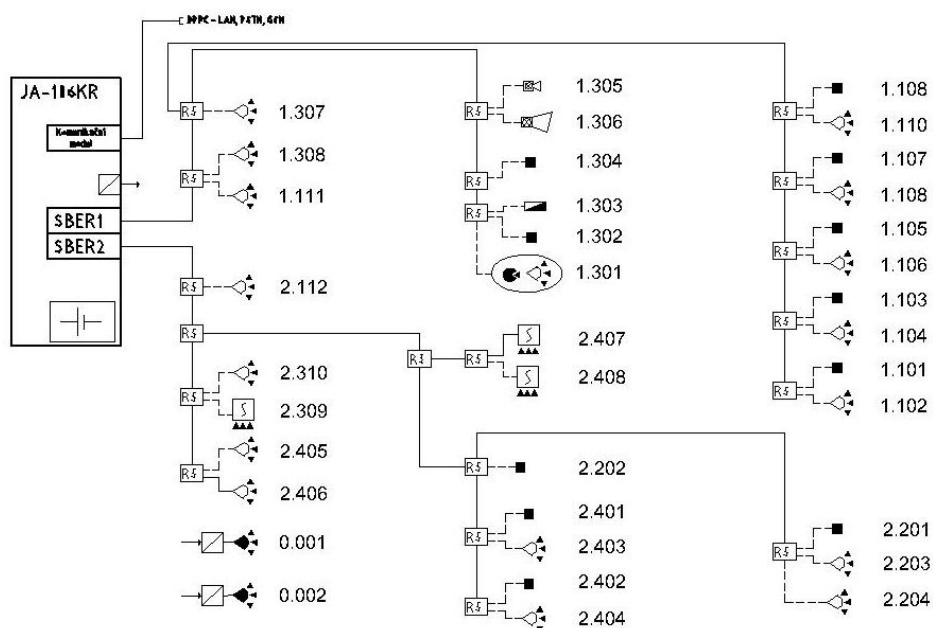
- S - Sběrnice
- B - pracovní blok (rozdělení objektu)
- PP - číslo komponentu

Skladovací police a nábytek

Titulní blok:

PRŮJEDNA	LET	1:200
Rozmístění PZTS	Bakalářská práce	
KREJČIL Jan Skovajsa	Půdorys - Rozmístění	
ZOHV.	Rozmístění	

PŘÍLOHA P IV: ZAPOJENÍ PZTS



Legenda PZTS	
Značka	Popis
PS	Zdroj (power supply)
	PIR detektor pohybu
	PIR venkovní
	PIR + GB
■	Magnetický kontakt
	Siréna vnitřní
	Siréna venkovní
	Požární hlásič (pro PZTS)
	Záložní AKU
	Vysílač
	Přijímač
	Rozbočovač sběrnice

Poznámka :

Značení detektorů: #S.#B#PP
 S - Sběrnice
 B - pracovní blok (rozdělení objektu)
 PP - číslo komponentu

Poznámka - kabeláž:

----- CC-02 (4x0,5 mm)
 ————— CC-01 (2x0,8 + 2x0,5 mm)

JMÉNO SOUBORU Zapojení PZTS	Bakalářská práce	LIST	MÉRITKO
KRESLIL Jan Skovajsa	Zapojení PZTS	VÝKRES Č.	Zapojení PZTS
SCHV.			

PŘÍLOHA P V: VLASTNOSTI KOMPONENTŮ

n	Komponent	Označení	Místnost	Sběrnice	Adresa	Sekce	Režim
1	Magnet	JA-111M	1.1	1	1.101	2	Okamžitý
2	PIR	JA-110P		1	1.102		Okamžitý
3	Magnet	JA-111M	1.2	1	1.103		Okamžitý
4	PIR	JA-110P		1	1.104		Okamžitý
5	Magnet	JA-111M	1.3	1	1.105		Okamžitý
6	PIR	JA-110P		1	1.106		Okamžitý
7	Magnet	JA-111M	1.4	1	1.107	1	Okamžitý
8	PIR	JA-110P		1	1.108		Okamžitý
9	Magnet	JA-111M	1.5	1	1.109		Okamžitý
10	PIR	JA-110P		1	1.110		Okamžitý
11	PIR	JA-110P	1.6	1	1.111		Okamžitý
12	PIR	JA-110P	1.9	2	2.112	2	Okamžitý
13	Magnet	JA-111M	2.1	2	2.201		Okamžitý
14	Magnet	JA-111M	2.2	2	2.202		Okamžitý
15	PIR	JA-110P	2.1	2	2.203		Okamžitý
16	PIR	JA-110P	2.2	2	2.204		Okamžitý
17	PIR+GB	JA-120PB	3.2	1	1.301	1	Zpožděný
18	Magnet	JA-111M		1	1.302		Okamžitý
19	Klávesnice	JA-114E		1	1.303		Tamper
20	Magnet	JA-111M	3.1	1	1.304		Okamžitý
21	Siréna IN	JA-110A		1	1.305		Tamper
22	Siréna OUT	JA-111A/AO		1	1.306		Tamper
23	PIR	JA-110P		1	1.307		Zpožděný
24	PIR	JA-110P	3.3	1	1.308		Okamžitý
25	Požární	JA-110ST		2	2.309		Okamžitý
26	PIR	JA-110P		2	2.310		Okamžitý
27	Magnet	JA-111M	4.1	2	2.401	2	Okamžitý
28	Magnet	JA-111M		2	2.402		Okamžitý
29	PIR	JA-110P		2	2.403		Okamžitý
30	PIR	JA-110P		2	2.404		Okamžitý
31	PIR	JA-110P		2	2.405		Okamžitý
32	PIR	JA-110P		2	2.406		Okamžitý
33	Požární	JA-110ST		2	2.407		24 hodin
34	Požární	JA-110ST		2	2.408		24 hodin
35	PIR	JA-110P	Out	/	0.001	3	žádný*
36	PIR	JA-110P		/	0.002		žádný*

*Při instalaci CCTV slouží k aktivaci alarmového vstupu

Poznámky k sekcím	
Sekce 1	Ize zastřežit samostatně
Sekce 2	Při střežení sekce 2 se automaticky zastřeží i sekce 1
Sekce 3	Při střežení sekce 3 se automaticky zastřeží i sekce 1 a 2
	Sekce 3 je vhodná spíše jako doplňková (např. s kombinací CCTV)