# Bezpečnostní systémy pro finanční instituce

Security systems for financial institutions

Tomáš Macháč

Bakalářská práce
2011



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Tomáš MACHÁČ** |
| Osobní číslo: | **A07491** |
| Studijní program: | **B 3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Téma práce: | **Bezpečnostní systémy pro finanční instituce** |

Zásady pro vypracování:

1. **Proveďte analýzu bezpečnostních rizik v zabezpečení finančních institucí.**
2. **Zpracujte normativní úpravy platné v ČR.**
3. **Vytvořte vlastní projekt pro danou finanční instituci.**
4. **Zhodnoťte projekt z ekonomického hlediska.**
5. **Vyhodnoťte přínosy nového řešení.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:


1. **JUDr. František Brabec – Ochrana bezpečnosti podniku. Eurounion Praha 1996. ISBN 80-85858-29-0**
2. **JUDr. Laucký Vladimír – Technologie komerční bezpečnosti I. Zlín: UTB ve Zlíně 2004. ISBN 978-80-7318-889-4**
3. **JUDr. Laucký Vladimír – Technologie komerční bezpečnosti II. Zlín: UTB ve Zlíně 2007. ISBN 978-80-7318-631-9**
4. **Kindl Jiří – Projektování bezpečnostních systémů I. Zlín: UTB ve Zlíně 2007. ISBN 978-80-7318-554-1**
5. **KŘEČEK, STANISLAV A KOL. – Příručka zabezpečovací techniky. Cricetus (BEN), Blatná 2002, 3. aktualizované vydání, ISBN 80-902938-2-4**


Vedoucí bakalářské práce: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
*děkan*

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

## ABSTRAKT

Tato práce řeší bezpečnostní rizika zabezpečení finančních institucí. Cílem práce je demonstrovat současný stav bezpečnostních systému v této oblasti. V teoretické části se zabývám analýzou rizik možného napadení finančních institucí a hodnocení rizik pachateli před bankovní loupeží. V praktické části se zabývám kriterii návrhu bezpečnostního systému pro banku. Zhodnotím cenovou nabídku dvou systému dostupných na našem trhu. Dále se zabývám, jakým směrem se budou orientovat bankovní loupeže a bezpečnostní vybaveni finančních institucí.


Klíčová slova: PZTS, EPS, CCTV, finanční instituce, bezpečnostní technologie.


## ABSTRACT

This work solves safety security risks of financial institutions. The objective of the work is demonstrate current status security systems in this area. In the theoretical parts I solve analysis risk possible attack and rating risk attackers before bank robbery. In the practical part I solve the design criteria of security systems for banks. I validate the quote two systems available on the market. I'm also concerned, what direction will steer the bank robbery and financial institution security equipment.


Keywords: I&HAS, Fire Alarm Systém, CCTV, financial institutions, security technology.

Rád bych touto cestou poděkoval svému vedoucímu bakalářské práce Ing. Rudolfovi Drgovi, za odborné vedení, rady a věcné připomínky, které mi poskytoval během zpracování práce.

Za odbornou pomoc bych chtěl poděkovat především svému kolegovi z práce, panu Petrovi Sedlaříkovi – technik v bezpečnostní firmě.

V poslední řadě bych chtěl poděkovat i své nejbližší rodině a mé přítelkyní za morální i finanční podporu. při studiu na Fakultě aplikované informatiky UTB ve Zlíně.

**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

Veškeré finanční instituce demonstrují svou sílu bezpečnosti instalovaným zabezpečovacím systémem nejvyšší kvality.

Při vstupu na pobočku si klient může všimnout nálepky, že objekt je monitorován kamerovým systémem a střežen elektronickou zabezpečovací signalizací. Finančním institucím jde především o to, aby se klient cítil dobře a nic neohrožovalo jeho zdraví.

Ale i nejkvalitnější zabezpečení nás neochrání před krizovou situací, při které se klient a zaměstnanci ocitnou tváří v tvář velkému nebezpečí. Krizová situace při loupežném přepadení je z pohledu ohroženého vždy nečekaná a náhlá. Přepadený se cítí být zaskočený, ruce se mu třesou, nohy mu ztěžknou, jeho pohyby jsou nekoordinované v důsledku prvého úleku. Nejspíše ani kvalitní psychologická příprava tyto přirozené reakce neodstraní. Efektivnost psychologické přípravy spočívá v tom, jak po přežití prvého úleku dále rozumně chovat, aby se nezvyšovala rizika přepadení. Důležitým úkolem přepadeného je zmapovat a zapamatovat identifikační znaky pachatele.

V dnešní době je objasněno každé druhé přepadení banky. Počet loupežných přepadení narůstá a zvyšuje se agresivita pachatelů. Proto kombinace kvalitního kamerového záznamů a výpovědí obětí loupežného přepadení použijeme k snadnější identifikaci pachatele.

Výsledkem práce je projekt elektronické zabezpečovací signalizace, kamerového systému a požární ochrany objektu.

# I. TEORETICKÁ ČÁST

# 1 BEZPEČNOSTNÍ MANAGEMENT ORGANIZACE

V dnešní době pachatelé (hackeři, bankovní lupiči) dokážou konkurovat moderní technologii. Proto ochrana bezpečnosti managementu finančních institucí nesporně vyžaduje integrovaný a komplexní postup řídících kroků. Půjde o organizační a řídící akty, normy, pravidla, pokyny, nařízení. Cílem je maximálně ochránit organizaci proti vloupání, přepadení, rozkrádání, krádeži, ale i jiným nekriminálním jevům ohrožující stabilní a bezproblémový provoz organizace jako jsou požáry, havárie, výpadky provozu, chyby v technologii, nedbalost a nepozornost zaměstnanců. Z hlediska řízení organizace sem patří informace o ohrožení podniku, stanovení bezpečnostních, odborných, provozních a obchodních rizik. Koncepce a návrhy k ochraně organizace řeší technické, technologické, organizační, personální a informační problémy. Vytvořením koncepce bezpečnosti politiky organizace je jedním důležitým dokumentem a je dílčí částí řídících dokumentů managementu. [3]

## 1.1 Bezpečnostní audity

Kombinace speciálních metod zkoumá a identifikuje skutečný aktuální stav procesů a opatření v určených oblastech bezpečnosti. Přezkoumání bezpečnostní situace v organizaci provádí specializovaná firma nebo jednotlivec pracující v průmyslu komerční bezpečnosti. Cílem bezpečnostních auditů je porovnat a posoudit míru dosažené shody aktuálního stavu s požadovaným kriterii. Zdokumentovat nalezené nedostatky a rozdíly, navrhnout doporučení a upozornit na potenciální rizika. Zpravidla se závěr bezpečnostního auditu vyjadřuje ve třech rovinách konečného výsledku (vyhovuje bez výhrad, vyhovuje podmíněně, nevyhovuje). Bezpečnostní audity se provádí na základě určitého vzoru. Nejčastější použití je auditní osnova, auditní model nebo auditní matrice.

Nejjednodušším vzorem pro provádění auditu je auditní osnova. Obsahuje běžný seznam úkonů a úkolů, které mají být v auditu obsaženy, a je stanoven cíl, který říká, na co má audit odpovědět, respektive čeho má být auditem dosaženo. Pomocí této osnovy je pak zpracována auditní zpráva či zpráva o provedeném auditu. Vytvořením auditního modelu získáme reálný model situace, jevu, objektu. Také poslouží k získání modelu situace spadající do výsledku „vyhovuje bez výhrad“. Postupuje se podle modelu a hodnotí se stupeň přiblížení reálné (současné) situace tomuto modelu, zpravidla se podle nějaké

číselné stupnice, počty bodů se sčítají a je uvedeno, kolik bodů musí být dosaženo pro výsledky, vyhovuje bez výhrad, vyhovuje podmíněně a nevyhovuje. Podle získaných výsledků se pak zpracuje závěr. Auditní matrice je nejpřesnější stanovení úrovně bezpečnosti v určitém objektu, podniku, situaci, jevu a činnosti. Protože tyto konkrétní auditované veličiny je vypracována přesná matice, která nepřipouští žádné odchylky obdobně jako ve výrobě šablona, pokud na určitou auditovanou činnost průmyslu komerční bezpečnosti tato matrice nepasuje, je výsledek nevyhovující. Pokud po určitých úpravách, které lze rychle nejlépe okamžitě odstranit, je dosaženo výsledného stavu, že matrice pasuje a výsledek vyhovuje podmíněně. Pokud v matrice „pasuje“ výsledek je vyhovuje bez výhrad. Pojem „matrice pasuje“ chápeme tak, že je naprosto totožná se zjištěným stavem při auditu, a to okamžitě na místě a v tu hodinu, kdy je audit prováděn, nikoliv po opravách. Přípravě osnovy, modelu a matrice musíme věnovat maximální pozornost. Vcházíme ze souhrnu zjištěných faktů na auditovaném místě. Ke shromáždění faktů musíme provést 5 kroků (1. Zjištění skutečného stavu na místě 2. Zhodnocení bezpečnostních rizik 3. Provedení bezpečnostní analýzy 4. Provedení analytické syntézy 5. Zpracování osnovy, modelu a matrice).

Bezpečnostní audit se dělá vždy, když otevíráme, přebíráme objekt po jiné organizaci v průmyslu komerční bezpečnosti. Při skončení činnosti u zákazníka na základě jeho nepříznivého hodnocení. Když bude spáchán trestný čin v objektu nebo u zákazníka, kde jsme v obchodním vztahu. Jestliže do objektu budeme instalovat technická opatření a došlo k pojistné události. Zda li zaměstnanec nebo zaměstnanci se dopustili protiprávního jednání. [3]

## 1.2 Problematika bezpečnostní analýzy

Bezpečnostní analýza je rozbor ucelených informací a poznatků o určitém objektu, jevu nebo situaci z bezpečnostního hlediska, který má nebo bude mít zásadní význam pro výkon činnosti podniku v komerční bezpečnosti. Je to proces, kde se podle informací zjišťují důležitá fakta a skutečnosti. Ta jsou tříděná a srovnávána s ostatními informacemi, a to tak aby bylo možno učinit logické závěry. Bezpečnostní analýzu zahajujeme stanovením bezpečnostních rizik. Poté setřídíme stávající informace z objektů, jevů nebo situace. [3]

Taková analýza by měla být zpracována vždy, kde realizace ochranných a obranných bezpečnostních opatření v organizaci neodpovídá potřebám nebo požadavkům na tuto činnost a zvláště i v případech, kdy se projeví nedostatky v zajišťování firemní bezpečnosti, a to včetně ochrany ekonomických zájmů. [1]

Všeobecné cíle ochrany majetku, osob a jiných bezpečnostních zájmů určují cíle, které jsou s ostrahou a ochranou spojené. Patří sem ochrana hmotného majetku (ochrana objektů a prostorů, ochrana materiálů, hotových výrobků nebo polotovarů a ochrana výrobních nebo jiných zařízení), ochrana nehmotného majetku (ochrana výzkumů a vynálezů, ochrana know – how, ochrana licenčních práv a personálních informací), ochrana osob (ochrana obchodních partnerů, zaměstnanců nebo návštěvníků podniků), ochrana veřejného pořádku a bezpečnosti v organizaci (pořádková služba uvnitř objektu), ochrana bezporuchovosti provozu podnikatelských aktivit organizace (elektronické sledování provozu, odhalování příčin a poruch firemními detektivy), protipožární ochrana objektu (protipožární hlídky, vybavení objektu protipožárními prvky), ochrana bezpečnosti a zdraví při práci (systém režimových opatřeni), ochrana proti narušování a poškozování životního prostředí (systém kontrolních mechanizmů ochrany životního prostředí a systém opatření při vzniku havárie).

Obecně zde nezapomínáme na základní kriminalistické otázky kdo, co, kdy, kde, jak, čím a proč. Analýza má i své vědecké stránky vychází vždy z logiky. Respektuje základní myšlenkový postup rozkládající vymezený celek na jeho jednotlivé prvky. Předmět v naší činnosti vysvětlujeme myšlenkovým či faktickým rozborem složek. Hlavními předměty analýzy jsou zpravidla: objekty, subjekty, procesy a technika. Cílem každé analýzy je dobrat se objektivní pravdy o stavu bezpečnostní situace v objektu o určité situaci nebo jevu. Bezpečnostní analýza musí mít stejně jako audit určitou strukturu. Po stanovení bezpečnostních rizik postupujeme dále k vyhodnocení minulého stavu. Zde zjistíme, zda v minulosti byla provedena nějaká analýza a ptáme se, z jakého důvodu událost nastala. Dále nás zajímá i současná situace mapujeme okamžitý stav. Důležité je také syntetizovat poznatky a prognózujeme budoucí stav. Vědecká bezpečností analýza může mít řadu druhů. Kvantitativní analýza, která zjišťuje možnosti ohrožení. Patří sem analýza rizik, analýza pomocí kontrolních záznamů a bezpečností audit. Kvalitativní zjišťuje možnost ohrožení v určitém úseku. Sem patří analýza příčin následku, analýza spolehlivosti lidských zdrojů a analýza stromem poruch.

**Postup analýzy:**

- Stanovení bezpečnostních rizik.
- Posouzení reálných hrozeb.
- Posouzení reálné zranitelnosti.
- Zbytkové rizikové faktory (odchylky).
- Obsahové nároky.
- Časové nároky.
- Finanční nároky.
- Návrh cílového stavu bezpečnosti daného systému.
- Návrh konkrétních bezpečnostních opatření.
- Návrh zásad bezpečnosti politiky.
- Doporučení dalšího postupu. [3]

## 1.3 Zásady pro optimální bezpečnost

Vyžaduje koncepty, které navzájem určují mechanická, technická, fyzická a režimová opatření. Je důležité, aby se nejdříve určila místa s vysokým rizikovým potenciálem. Zvláštní pozornost musíme věnovat všem existujícím otvorům v budově (okna, dveře, technologické prostupy). Dále je potřeba uskutečnění mechanických, technických a režimových opatření. Souhra všech těchto opatření, určených podle požadavků objektu, redukuje účinně riziko vloupání. Mechanická ochranná zařízení znemožňují vniknutí a pachatel je takto déle na místě činu. Je rozhodující, aby co nejdříve byl detekován pokus o vloupání a oznámení na pult centralizované ochrany se stálou obsluhou (policie ČR, popřípadě bezpečnostní agentura). Díky včasnému vyrozumění získají připravené zásahové síly čas, aby mohli zasáhnout a zabránit následným škodám. [2]

### 1.3.1 Opatření k ochraně objektu

- Hodnocení rizik, které odhalí zranitelné kritické oblasti.
- Příprava plánů před vznikem krizových situací.
- Zavedení vnější kontroly (monitorování míst v okolí objektu, která slouží jako nástupiště útočníků).
- Důsledná kontrola vstupujících osob a vozidel (to zajišťuje současně technika i lidé).
- Zvýšení mechanické odolnosti přístupů do chráněných přístupů. Tím se sníží přístup k potencionální krádeži či nežádoucí činnosti.
- Zapojení pracovníků ohrožené firmy do ochrany, jejich seznámení s ochranou pracovišť, školení a cvičení zaměřené na to, jak nepovolaným osobám znemožnit získání informací, uložení peněz nebo zboží a dokumentů.
- Koordinace všech bezpečnostních systémů v objektu.
- Dokumentace o všech vloupáních a jejich pokusech a jiných trestných činech. [2]

### 1.3.2 Předmět zkoumání

Předmětem zkoumání má být:

- okolí objektu (v širším i užším smyslu slova),
- vnější bezpečnost,
- ochrana perimetru a všech vstupů/vjezdů,
- způsob kontroly oprávněnosti všech vstupujících osob/vozidel,
- ochrana budov a vnitřních objektů i šech vstupů/vjezdů,
- bezpečnostní osvětlení,
- charakter vnitřních kontrol,
- zámky a klíčové režimy,
- bezpečnostní systémy (PZTS, EPS, CCTV, EKV),
- vstupy peněz, cenin, jiných důležitých komponentů a způsoby přebírání,

- místa uložení peněz a procedury ukládání,
- ochrana důležitých vnitřních procesů a procedur,
- místa a způsob odbavování zásilek apod.,
- ochrana výpočetního centra, výpočetní sítě a jednotlivých zařízení,
- ochrana informací a dat,
- prucedůry ochrany proti vloupání, loupeži, podvodů a hospodářské kriminalitě,
- smluvní procedury,
- dostatečnost a účinnost vnitřní legislativy,
- ochrana proti sabotáži a terorismu,
- ochrana důležitých osob organizace. [2]

## 1.4 Plánování loupeží a hodnocení rizik pachateli

Loupežné přepadení finančních institucí je více či méně plánována a připravována. Před loupežným přepadením pobočky je místo často vytipováno a sledováno. Je zjišťována vzdálenost peněžního ústavu k policejní služebně, je ověřována situace v prostoru s peněžními přepážkami v různých dnech a různých časech, jsou zjištěny způsoby dotací, počet zaměstnanců a zákazníků. Dále je posuzována výše vyplacených a přijímaných obnosů, zjišťuje se viditelnost do objektu zvenčí. Někdy je i zjišťována úroveň zabezpečovací a monitorovací techniky. Pachatele dávají přednost peněžním ústavů na venkově nebo v malých městech, kde je možnost rychlého úniku z místa činu. Základní poznatky plánovaných bankovních loupeží jsou:

- Loupeže jsou plánovány krátkodobě a jednoduše.
- Pachatelé si obstarávají masky a zbraně a seznamují se s okolím banky a únikovou cestou.
- Profesionálové a amatéři se liší při výběru objektu přepadení.
- Amatéři volí banku k přepadení podle možnosti útěku (blízko dálnice, velikost banky a její poloha).

- Profesionální pachatelé volí banku podle možnosti úkrytu v blízkosti banky. V některých případech berou tito pachatelé v úvahu vzdálenost policejního útvaru, charakteristika vnitřního zařízení, a bezpečnostní zařízení banky.
- Průběh činů bývá částečně plánován (až 75% pachatelů).
- Bezpečnostní zařízení v bance hraje velkou roly.

Bezpečnostní zařízení v bankách jsou pro pachatele, kteří plánují loupežné přepadení přirozenou součástí průběhu typickému přepadení. Tato zařízení jsou předpokládaná v různých variantách, které jsou pro provedení přepadení bezvýznamná. Pachatelé velmi často před přepadení banku neobhlíží, neboť to zvyšuje riziko, že budou po přepadení snadněji identifikováni. Pachatelé amatéři často ignorují vývěsní tabule s nápisem „máme časové zabezpečení trezoru“. Z toho vyplývá, že amatéři jsou mnohem nebezpečnější, když jim personál banky pod výhružkami nevydá peníze, jelikož to z technických důvodů není možné. Každý pachatel posuzuje svou kalkulaci, když od své kořisti odečte riziko. Proto pachatelům vyhovuje, když mohou očekávat velkou kořist při nepatrném riziku a vysoké bezpečnosti realizaci činu, včetně chování bankovních zaměstnanců. V České republice je pro některé pachatele typické to, že svůj čin plánují. Velmi často sem patří: výběr objektu a času přepadení, zjištění zabezpečení objektu, počet zaměstnanců a fyzické ochrany, získání spolupachatelů, zbraně, masky, ale také dopravního prostředku. Řada pachatelů se připravuje i na svůj herecký výstup v napadeném prostoru. Nacvičují si postup, postoje se zbraní, komunikace s personálem, ale i klienty. A to proto, aby zapůsobil na své okolí v co nejkratším čase a docílil vydání finanční hotovosti. [2]

# 2 ZPŮSOBY OCHRANY FINANČNÍCH INSTITUCÍ

Z pohledu zabezpečení objektu a stanovení rizika napadení je potřeba objekt rozdělit do jednotlivých bezpečnostních zón, ve kterých se stanovuje stupeň mechanické, elektronické a fyzické ochrany a rozsah možného pohybu osob. Bezpečností zóny:

- Zóna A – je přísně střeženou zónou, kam mají vstup pouze oprávnění zaměstnanci banky za nejpřísnějších podmínek. Tato zóna musí tvořit dispozičně uzavřený celek, kde všechny stavební otvory jsou zabezpečeny na určité úrovni balistické odolnosti. Požadovaná úroveň pro obvodové zdi, a také všechny výplně stavebních otvorů je stanovena stejně.
- Zóna B – vyznačuje prostory, které podléhají zvláštnímu bezpečnostnímu režimu, a to včetně vstupu. Tyto prostory jsou určeny k tomu, aby do nich vstupovali klienti za předpokladu, že jsou splněna určena bezpečnostní opatření. Klienti banky mohou vstoupit s doprovodem oprávněného zaměstnance nebo bankovní policii. Mohou také vstoupit s platnou vstupní kartou vydanou bankou. Do těchto prostor mohou vstoupit i oprávnění zaměstnanci banky.
- Zóna C – vymezuje prostory, které jsou za normálního provozu přístupné pouze zaměstnancům banky. Uvnitř této zóny jsou provozy, které jsou řešeny na různých bezpečnostních úrovních. Režim vstupu může být oprávněn individuálně do výše rizika. Pro klienty a ostatní návštěvy platí zásady při vstupu jako u zóny B.
- Zóna D – je zónou volnou a vstup do prostor těchto budov není řízen oprávněnými zaměstnanci banky ani bankovní bezpečností. Těchto prostor by mělo být v bance minimum. Jsou obvykle omezeny a to jak prostorově, tak i časově. Důležitá je také kontrola prostoru po skončení návštěvních hodin. Zde mohou být odkládány nežádoucí předměty, případně výbušniny. [2]

## 2.1 Ochrana fyzická

Fyzickou bezpečností rozumíme ochranu, zajišťovanou fyzickou přítomností osob přímo v chráněném prostředí finanční instituce. Ostrahou může být vlastní zaměstnanec organizace pověřeným výkonem toho druhu zabezpečení. Nebo dodavatelé soukromých bezpečnostních firem, kteří tyto funkce zajišťují prostřednictvím vlastních pracovníků.

Fyzickou ochranu můžeme rozdělit z hlediska času na přetržitou, vázanou na pracovní dobu finanční instituce nebo nárazovou (po dobu mimořádné události). Formy fyzické ochrany jsou kontrola vstupu, strážní služba, bezpečnostní dohled, ochranný doprovod, zásahová činnost v rámci fyzické bezpečnosti.

**Fyzická bezpečnost z hlediska rozsahu a účelu:**

- Propustková a informační - Zabraňují vstupu neoprávněných osob, případně vjezdu vozidel a neoprávněnému vnášení a vynášení předmětů. Kontrolovat a evidovat osoby, pohybující se v režimových prostorech, vjíždějící a vyjíždějící vozidla. Poskytovat informace návštěvníkům a zajišťovat dodržení stanoveného řádu návštěv. Zajišťovat uzamykání vchodů do objektu a dveří v objektu podle stanoveného řádu. Plnit úlohu ohlašování požáru, havárii a jiných mimořádných událostí.
- Ochrana perimetru - (obchůzka kolem objekt nebo na strážních místech).
- Celoplošná (dohledová) – Dohled nad dodržováním oprávněnosti pohybu nebo činnosti osob v chráněném objektu. Dohled nad dodržováním stanoveného vnitřního provozního režimu. Doprovod určených osob. Dozor nad prácemi, prováděnými zpravidla externími pracovníky v objektu. Kontrola uzavření stanovených prostor a objektů.
- Doprovodná – Doprovod při přepravě nebo při definovaných úkolech. Při přepravě jsou cennosti a peníze nejzranitelnější.
- Dozorčí a operátorská – (PZTS, EPS, EKV, CCTV)
- Zásahová

**Pracovníci fyzické ochrany z hlediska výzbroje a výstroje:**

- Ozbrojeni - (prostředky osobní ochrany – ochranné spreje, elektrické šokové prostředky, střelné zbraně použít v nutné obraně § 29 trest. zákoníku).
- Neozbrojeni – (Na operačních a dispečerských stanovištích, informátoři u vstupu nebo ve veřejných prostorách banky).
- Veřejná ochrana – ve stejnokroji s viditelným označením.
- Skrytá fyzická ochrana – při podezření z krádeží.

## 2.2 Ochrana technická

### 2.2.1 MZS – Mechanické zábranné systémy

Mechanické ochrany jsou navrhovány v rámci stavby nebo úprav objektu. Jsou kompromisem mezi odolností a komplexností, a také mezi estetikou prostoru a vizuálního působení na klienty. Systémem MZS je důsledné a bezpečné oddělení klientských prostor od prostorů zázemí a další mechanicky odolné oddělení prostor IT technologií a prostor úschovy hotovosti nebo sejfů. Doba překonání mechanické ochrany by měla být minimálně stejná jako doba příjezdu zásahové skupiny. Veškeré mechanické prostředky zabraňují vstupu do chráněných prostorů, budov a manipulací s chráněnými předměty. [7]

**Vnější mechanická odolnost objektu spočívá s v instalaci těchto zařízení:**

- Ploty (bezpečnostní plot s ostnatým drátem, betonový plot, plot s válcového plechu) zde hraje důležitou roli znesnadnění překonání průniku, ale také estetické hledisko.
- Závory (hydraulické, mechanické a elektromechanické).
- Zdi (z různých stavebních materiálů). Zde hraje důležitou úlohu estetika, cena a snaha zakrýt pohled na vnitřní část pozemku.
- Brány (pojezdové, sklápěcí, elektromechanické a mechanické).
- Turnikety většinou celokovové umožňují průchod pouze jedné osobě, popřípadě umožňuje vedení kola.
- Bariéry proti nájezdu vozidel (betonové překážky, výsuvné kůly, ocelová zábradlí).

**Vnitřní mechanické zabezpečení stavebních částí budov:**

- Dveře (hlavní, vedlejší nebo balkónové) - měly by být mechanicky odolné a to zvláště na plášti budovy, kde je předpokládaný útok pachatele. Ty mohou být doplněné zámkovými systémy s bezpečnostním kováním.
- Okna (střešní, etážová) – na plášti budovy, kde je předpokládaný útok pachatele. Měly by být bezpečnostně vrstvená, popřípadě doplněna bezpečnostní fólii.
- Stěny, podlahy a stropy, které jsou vybaveny tak, aby je nebylo možno jednoduše překonat.

- Střechy by se měly chránit proti přelezení, ohni, proražení (válcovaný plech, kovové sítě)
- Turnikety (poloprofilové, plnoprofilové, karuselové, válcovité) umožňují průchod pouze jedné osobě. Pro průchod většího počtu osob se zřizují branky.
- Pásmové propusti jsou to dvojice, popřípadě více dveří ve vzájemné vazbě na otevření. Zde je umožňován průchod pouze jedním směrem.
- Mříže (z válcované oceli)
- Stálé žebříky, okapové trubky a bleskosvody by měly být chráněny bezpečnostními řetězy nebo ostnatým drátem.
- Přepážky mají za účel oddělovat bezpečnostně klienta a zaměstnance. Měly by být mechanicky odolné.
- Peněžní přepážky SITEC, balisticky odolné, umožňují příjem a výdej peněžní hotovosti v kontejnerech.
- Uzamykající systémy (časové zámky, kombinační zámky, bezpečnostní vložky). Je to zásada, kdy jakýkoliv zámek by měl mít minimální počet klíčů. Klíče by neměly opouštět objekt, měly by být uloženy na bezpečném místě.
- Bezpečnostní rámy.
- Bezpečnostní rentgen.

**Úschovná místa a trezorové místnosti:**

- Pancéřované peněžní sejfy.
- Komorové trezory.
- Vestavěné komorové trezory.
- Bankomaty.
- Noční trezory.
- Ocelové schránky (skříně).
- Pancéřové schránky různého bezpečnostního stupně.

- Trezorové místnosti (zděné s ocelovými deskami, armaturované betonové stěny). Dnes se nabízejí dvě možnosti: a) Velmi silné stěny z armaturovaného betonu o šířce 80 – 100 cm a nebo dvě stěny s kontrolní chodbou (vnější stěna o minimální šířce 30 cm a vnitřní 60 cm, meziprostor maximálně 60 cm, odolné proti diamantovým vrtákům a pilám i proti trhavinám, b) Stěny o malé šířce, 40 – 50 cm silné, z různých materiálů, vnitřní stěny jsou obloženy několika vrstvami pancéřových desek (je to „dům v domě“).
- Technika k ochraně dat (schránka k ochraně dat, místnost pro zabezpečení dat nebo archivní místnost). [2]

**Normativní úprava MZS**

- Skříňové trezory mobilní, ale také trezory určené k zazdění jsou certifikovány dle normy ČSN EN 1143-1+A1:2009. Tato norma je členěná na bezpečnostní třídy, a to od třídy 0 až po třídu X.
- Depozitní systémy jsou certifikovány dle normy ČSN EN 1143-2:2003, bezpečnostní třídy D.
- Trezory se základní bezpečnostní jsou certifikovány dle normy ČSN 91 6012:2001, tato norma je dělena na tři bezpečnostní třídy od Z1 do Z3.
- Úschovné objekty (bezpečnostní trezorové schránky) jsou certifikovány dle normy ČSN EN 14450:2005, je rozdělena na dva stupně (LEVEL 1 a LEVEL2).
- Time trezory jsou certifikovány dle normy ČSN EN 1143-1:2006.
- Ocelové schránky jsou certifikovány dle normy ČSN EN 91 6012:2001.
- Konstrukce trezorových stěn jsou certifikovány dle normy ČSN EN 1143-1:2006. Tato norma je členěná na bezpečnostní třídy, a to od třídy 0 až po třídu XIII.
- Trezorové dveře jsou certifikovány dle normy ČSN EN 1143-1:2006. Tato norma je členěná na bezpečnostní třídy, a to od třídy 0 až po třídu XIII.
- Zámky s vysokou bezpečnostní jsou certifikovány dle normy ČSN EN 1300:2005, tato norma je dělena na čtyři bezpečnostní třídy A, B, C, D.

- Okna, dveře, vrata, dveřní kování, uzamykající systémy a jejich komponenty jsou certifikovány dle normy ČSN P ENV 1627:2000. Tato norma je členěná na bezpečnostní třídy, a to od třídy 1 až po třídu 6.
- Mříže a žaluzie jsou certifikovány dle normy ČSN P ENV 1627:2000. Tato norma je členěná na bezpečnostní třídy, a to od třídy 1 až po třídu 4.
- Zámky a střelkové zámky jsou klasifikovány podle normy ČSN EN 12209:2004

  čl. 4.2 tab. 2. Tato norma je členěná na bezpečnostní třídy, a to od třídy 1 až po třídu 7.
- Elektromechanicky ovládané zámky klasifikováno dle normy ČSN EN 14846:2008.
- Visací zámky a příslušenství visacích zámků je certifikováno dle normy ČSN EN 12320:2002. Tato norma je členěná na bezpečnostní třídy, a to od třídy 1 až po třídu 6.
- Cylindrické vložky pro zámky – třída bezpečnosti související s klíčem. Jsou certifikovány dle normy ČSN EN 1303:2005. Tato norma je členěná na bezpečnostní třídy, a to od třídy 1 až po třídu 6.
- Nouzové dveřní uzávěry – únikové cesty jsou certifikovány dle normy ČSN EN 179:2008.
- Dveřní kování, dveřní kliky, štítky a knoflíky jsou certifikovány dle normy ČSN EN 1906:2003. Tato norma je členěná na bezpečnostní třídy, a to od třídy 1 až po třídu 4.
- Panikové dveřní uzávěry jsou certifikovány dle normy ČSN EN 1125:2008. [5]

### 2.2.2 PZTS – Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy PZTS slouží k tomu, aby vždy spolehlivě a včas odhalily pachatele a rychle předaly zprávu o narušení střeženého prostoru. Jsou to elektronická zařízení, která chrání osoby i majetek, který se nachází v zabezpečené oblasti. Při narušení střežené oblasti dojde pomocí detektorů k vyhlášení poplachu, který je poté přenášen pomocí komunikátoru na hlídací strážní službu nebo zodpovědnou osobu.

Elektronickým zabezpečovacím zařízením se dají pokrýt v podstatě všechny typy prostor a objektů od rodinných domů, kancelářských prostor až po průmyslové objekty.

Podstatný vliv na kvalitu a spolehlivost systému PZTS mají snímací prvky - detektory, které vysílají signál o narušení střeženého prostoru. Jejich správná volba je zásadní pro spolehlivou funkčnost celého systému. Bezpečnostní detektory se volí jak podle způsobu použití, tak podle prostředí instalace.

Nejčastěji používané detektory v systémech PZTS do venkovního prostředí jsou infrazávory, mikrovlnné bariéry, venkovní pohybové detektory a detekční plotové systémy.

Pro systémy elektronického zabezpečení vnitřních prostor jsou pak nejpoužívanější pohybové infradetektory, detektory tříštění skla, magnetické kontakty, kombinované pohybové detektory s detektory tříštění skla, požární detektory kouřové, tepelné nebo kombinované.

Pro ovládání poplachového zabezpečovacího a tísňového systému PZTS slouží obvykle klávesnice. S její pomocí je možno systém PZTS zejména zapnout nebo vypnout ze střežení, zjistit stav systému, pořizovat uživatelské kódy, zjišťovat místa poplachů a ovládat mnoho dalších funkcí systému.

Zabezpečovací systémy je možné ovládat i pomocí bezdrátových ovladačů, případně dálkově pomocí SMS, nebo z počítače po internetu

V mnoha případech bývá důležitá také vzájemná návaznost poplachových zabezpečovacích a tísňových systémů PZTS na ostatní systémy v objektu, např. přístupový systém, kamerový systém, datovou síť, internet, vytápění, elektroinstalaci atd. Tuto spolupráci nazýváme systémová integrace.

Na správném návrhu a provedení poplachových zabezpečovacích a tísňových systémů přímo závisí bezpečnost jak objektů, tak v mnoha případech i osob. Proto je nutné, aby projekt a instalaci poplachových zabezpečovacích a tísňových systémů PZTS zajistila odborná firma, která provede profesionální zhodnocení všech aspektů na místě a navrhne optimální způsob řešení instalace zabezpečovacího zařízení. [6]

**Ústředny PZTS**

Ústředny PZTS tvoří jádro zabezpečení. Zpracovávají informace od detektorů a systémových prvků a komunikují s přenosovými systémy jejich prostřednictvím s pulty centralizované ochrany.

Pro potřeby finančních ústavů s náročnými požadavky na podskupiny, úrovně hesel, vazby mezi prvky PZTS i na jiné systémy jsou obvykle navrhovány sběrnicové systémy. Detektory jsou připojovány do koncentrátorů rozmístěných po objektu. Koncentrátory komunikují s vlastní ústřednou po datovém vedení. Tím se redukují kabelové trasy v objektu a současně je možnost modulárního rozšiřování systému o další koncentrátory. Současně je v ústředně vestavěn zálohovaný zdroj pro koncentrátory a čidla. U větších aplikací je nutné rozdělit napájení do více větví a tím i na více samostatně zálohovaných zdrojů. [7]

**Detektory pro vnitřní použití:**

- Infračervený PIR detektor - je nejčastěji používaným pohybovým detekčním prvkem v poplachových zabezpečovacích a tísňových systémů PZTS. Jeho funkce je založena na zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Je schopen zachytit pohyb těles, která mají jinou teplotu, než teplotu okolí.
- Mikrovlnný detektor - patří mezi pohybové detektory a funguje na principu aktivního vysílání mikrovlnného záření, které vyhodnocuje změnu své fáze mikrovln po odrazu od pohybující se osoby.
- Detektor tříštění skla - patří do skupiny akustických detektorů a jeho princip je založen na snímání zvukové charakteristiky tříštění skla a tlakové vlny vzniklé nárazem na skleněné plochy.
- Magnetický kontakt - kontaktní detektor, který slouží k plášťové ochraně objektů a používá se nejčastěji k hlídání otevření dveří, oken, vrat, rolet. Funkce magnetického kontaktu je založena na principu jazýčkového relé spínaného magnetickým polem permanentního magnetu.

- Kombinovaný pohybový detektor s detektorem tříštění skla – skládá se ze dvou detektorů v jednom krytu. Detektor pohybu a detektor tříštění skla. Oba detektory mohou vyhodnocovat poplachové události společně, nebo nezávisle na sobě.
- Kombinovaný pohybový detektor PIR s mikrovlnným detektorem - funkce duálního pohybového detektoru je založena na kombinaci dvou principů detekce. V tomto případě je to detekce infrapasivní a mikrovlnná. K vyhlášení poplachu dojde pouze v případě, že obě detekční části vyhlásí poplachový signál současně, tím zvyšuje spolehlivost detekce a snižuje náchylnost k planým poplachům.
- Otřesový detektor - je určen k ochraně pevných ploch nebo trezorů před probouráním, prořezáním a vhodným způsobem doplňuje plášťovou ochranu.
- Tísňové detektory - Magnetické kontakty či mikrospínače zapouzdřené do podoby vhodně tvarovaného tlačítka či nožní spínací lišty. Slouží zaměstnancům k nepozorovanému vyvolání tísňového hlášení v případě přímého ohrožení.
- Speciální detektory - slouží k detekci doplňkových veličin, například indikují výšku hladiny nebo zaplavení střeženého prostoru vodou, detekují různé druhy plynů.

**Detektory pro vnější použití:**

- Infrazávory - infrazávora je složena z vysílače a přijímače. Mezi nimi prochází dva nebo více infračervených paprsků. V případě přerušení těchto paprsků dochází k vyhodnocení tohoto stavu přijímačem a následnému vyhlášení poplachového signálu.
- Mikrovlnná bariéra - Zařízení se skládá z vysílače a přijímače. Narušení je detekováno na základě změny energie mikrovlnného pole mezi vysílačem a přijímačem.
- Venkovní pohybový detektor - jedná se v principu o standardní pohybový detektor v obalu s vyšším krytím a s clonou proti slunečnímu záření. Detektory bývají ještě vybaveny detekčním algoritmem, který vyhodnocuje okolní teplotu nebo intenzitu osvětlení. Ve velké míře jsou řešeny jako kombinované PIR+MW.
- Detekční plotové systémy - venkovní plotový systém pracující na principu detekčních kabelů montovaných na oplocení střeženého objektu. Speciální kabel registruje vibrace vznikající při přelézání, stříhání nebo jiné manipulaci s tělesem

plotu. Řídící modul vyhodnocuje signál z detekčních zón a pomocí speciálních algoritmů rozlišuje pokus o překonání plotu a běžné vibrace vznikající vlivem okolního prostředí.

- Bezdrátový detekční systém - je perimetrický systém umožňující střežení plotu pomocí speciálních bezdrátových akceleračních RFID tagů připevněných na pletivu a vratech. Tagy snímají časové a dynamické změny v poloze pletiva, které jsou typické pro přelézání plotu narušitelem.[6]

**Dohledová a poplachová přijímací centra**

Dohledová a poplachová přijímací centra (pulty centralizované ochrany) jsou poslední částí zabezpečovacího systému. Zajišťuje přenos poplachových událostí z objektu banky do centra bezpečnostní služby nebo police ČR. Na základě takto přenesených informací je prováděn fyzický zásah na objektu.

Na objektu je tzv. objektový díl přenosového zařízení, který informace z ústředny vysílá na vlastní pult centrální ochrany. Finanční ústavy jsou připojovány na PCO bez výjimek. Obsluha PCO může přímo na plánech daného objektu sledovat čidla v poplachovém stavu, časovou posloupnost událostí a koordinovat činnost zásahové jednotky. [7]

**Normativní úprava PZTS**

**Norma ČSN EN 50131** „*na rozdíl od předchozího vydání rozlišuje poplachové systémy pro detekci vniknutí a poplachové systémy pro detekci přepadení. V souvislosti s tím jsou některé body této normy formulovány odděleně pro tyto dva druhy zabezpečení. V originále této normy se kromě jediné zkratky, IAS (Intruder Alarm System - poplachový systém pro detekci vniknutí), použité v předchozím vydání normy, objevuje zkratka I&HAS (Intruder and Hold-up Alarm System - poplachový systém pro detekci vniknutí a přepadení). Na několika místech normy jsou použity zkratky HAS (Hold-up Alarm System - poplachový systém pro detekci přepadení) tam, kde systém postrádá funkci detekce vniknutí, a IAS tam, kde systém postrádá funkci detekce přepadení. Proto jsou nyní v českém překladu normy místo dosud používané zkratky EZS používány zkratky z originálu - I&HAS "poplachové zabezpečovací a tísňové systémy", IAS pro "poplachové zabezpečovací systémy" a pro HAS*

*"poplachové tísňové systémy" V českých textech lze uvedené zkratky z originálu nahradit následujícím způsobem: I&HAS=PZTS, IAS=PZS, HAS=PTS.“[11]*

**Norma ČSN EN 50518-1** stanovuje požadavky na umístění dohledových poplachových center (pultů centralizované ochrany) a na ohodnocení rizik. Dále jsou v normě uvedeny stavební požadavky na dohledová centra z hlediska odolnosti proti napadení a proti požáru.

### 2.2.3 CCTV – Uzavřeny kamerový okruh

Kamerové systémy jsou dnes neodmyslitelnou součástí zabezpečení finančních ústavů. Slouží pro zvýšení bezpečností banky i jejích klientů.

Kamerový systém je tvořen vlastními kamerami, záznamovým zařízením, monitory a pomocnými prvky.

Zvýšený důraz je kladen na sledování hotovostních pracovišť, vstupy do trezorů a technických místností a cestu dotační. Zde jsou nasazovány kamery s vyšším rozlišením i citlivostí a nastavením umožňujícím identifikaci jednotlivé osoby. Obvykle bývají doplněny ještě kamerou příchodovou a odchodovou.

Další kamery slouží jako přehledové na komunikačních cestách a bankovních halách. Systém bývá podle potřeby doplněn například vnější kamerou u vjezdu do dotačního boxu.

Provedení kamer je podle účelu a umístění různé. Od klasických vnitřních kamer na stojánku, přes kamery ukryté pod omítkou až po kamery vnější v klasickém temperovaném krytu nebo krytu polokulovém.

Specifickými jsou velké počítárny hotovostí a pracoviště přípravy dotací. Zde bývá obvykle kompletní samostatný systém s kamerami „megapixlovými", samostatným záznamem a zvýšeným snímkováním.

Vzhledem k tomu, že ve finančních ústavech se jedná o bezpečnostní aplikaci, jsou navrhovány kamerové systémy s přenosem analogového videosignálu a digitálním zpracováním a ukládáním snímků. Napájení je zálohováno na několik desítek minut provozu bez síťového napájení.

Doba záznamu je zde běžně měsíc i více a tomu odpovídá skladba záznamových zařízení. Běžné je propojení PZTS a CCTV s tím, že podle typu poplachu z PZTS jsou nahrávány se zvýšeným snímkováním přesně definované kamery. [7]

Základní kritéria, kterými by se měl výběr kamery řídit, a který určuje samotnou použitelnost bezpečnostní kamery, je rozlišení kamery, použitý snímací čip a světelná citlivost kamery. Dalším důležitým prvkem ovlivňujícím kvalitu snímaného obrazu je volba správného objektivu kamery. Nesprávně zvolený objektiv může výrazně negativně ovlivnit výsledný obraz i při použití velice kvalitní kamery. Naopak kvalitní a dobře navržený objektiv umožní zachování dobré kvality obrazu i při použití levnější kamery. Kamery dělíme na dva základní druhy podle toho, do jakého prostředí je kamera určena. Jsou to kamery do venkovního prostředí a kamery do vnitřního prostředí.

**Bezpečnostní kamery pro vnitřní použití:**

Vzhledem k využití těchto kamer ve vnitřních prostorech, tedy v interiérech objektů, jsou tyto kamery konstruovány tak, aby jejich velikost byla co nejmenší a tím pokud možno co nejméně zasahovaly do vzhledu samotného interiéru. I vzhledem k poměrně malým rozměrům, jsou tyto kamery schopny snímat a přenášet obraz v kvalitním a velice vysokém rozlišení. Pro snímání obrazu v noci nebo za zhoršených světelných podmínek bývají používány kamery s automatickým přepínáním na noční režim (zvýšení citlivosti změnou režimu snímání z barevného na černobílý), nebo kamery doplněné infra přísvitem, který umožní kameře sledovat zájmový prostor i za nulového osvětlení. Pouhým okem však toto přisvícení není zaznamenatelné.

**Bezpečnostní kamery pro venkovní použití:**

Kamery do venkovního prostředí jsou velice podobné kamerám vnitřním a fungují na stejném principu. Jediný rozdíl mezi nimi je v konstrukčním provedení. Kamery do venkovního prostředí jsou obklopeny krytem, který je schopen odolat nepříznivým vlivům venkovního prostředí. Kamery mají vlastní vytápění a ventilaci a jsou ošetřeny proti vlhkosti. Stejně jako u vnitřních kamer, tak i u kamer venkovních lze pomocí infra přísvitu sledovat zájmový prostor i za nulového osvětlení. Venkovní kamery se vyrábějí s infra přísvitem, který osvítí prostor až do vzdálenosti 80m. Při požadavku na větší pokrytí se pak volí instalace přídavných infra reflektorů.

**Hlavní parametry kamery**

Prvním předpokladem je určení typu kamer, zda bude použita pro vnitřní nebo venkovní prostředí. Dále je nutné určit, mají-li být kamery skryté, nenápadné (malé rozměry) nebo naopak výrazné (odstrašující efekt). Důležitým faktorem jsou světelné podmínky ve kterých budou kamery pracovat - běžné světelné podmínky, kdy lze použít kamery se standardní citlivostí, při špatném osvětlení se používají kamery ultracitlivé nebo den/noc popřípadě úplná tma, kdy se použijí kamery s IR přisvícením nebo přídavné osvětlení. Dalším faktorem je určení rozlišení kamery (čipu).

Pro výběr vhodného objektivu je důležitý údaj o sledovaném prostoru (vzdálenost snímaného objektu od kamery a požadovaná šířka záběru), případně nutnost použití proměnného ohniska - zoomu.

**Parametry:**

- Snímací čip - CCD,CMOS
- Rozlišení – CIF, 2 CIF, 4 CIF, 1,3 MPix,2 MPix až
- 5MPix a více.
- Typ snímání – černobílá, barevná, den/noc
- Typ výstupního signálů – analogový, digitální (kroucený pár, IP)
- Napájení – 12V DC,24V AC,230V AC
- Uchycení objektivu – C, CS
- Typ montáže – pevná, otočná, kompaktní
- Speciální funkce – VMD, BLC,AGC, gama korekce [10]

**Přenos záznamového obrazu**

Přenos obrazu lze řešit analogově, pomocí koaxiálního kabelu, použitím strukturované kabeláže (přenos po krouceném páru), použitím optického kabelu nebo bezdrátovým přenosem. Zvolení druhu přenosu závisí na mnoha činitelích: počtu kamer, vzdáleností jednotlivých komponentů kamerového systému, náročnosti prostředí.

- **Koaxiální kabel** - přenos po koaxiálním vedení bývá nejběžnějším způsobem přenosu analogového video signálu po metalickém vedení. Je používán 75Ω

koaxiální kabel. Zde však je omezená vzdálenost přenosu vlivem úbytku signálu ve vedení a náchylností k rušení okolním prostředím. Zpravidla je technicky možné po tomto vedení přenést videosignál bez použití dalších komponentů na vzdálenost maximálně několika set metrů.

- **Datový kroucený kabel - strukturovaná kabeláž -** Pro tento způsob bývá nejčastěji používán datový UTP nebo STP kabel. Jedná se opět o přenos analogového videosignálu. Při této metodě se používají převodníky video signálu na twist (kroucený pár), které jsou osazeny na oba konce trasy. Tímto způsobem lze přenést videosignál na podstatně větší vzdálenost, než u koaxiálního vedení – řádově stovky až tisíce metrů. Velkou výhodou je také možnost přenosu více videosignálů po jednom kabelu – pro každý video signál je potom využíván jeden kroucený pár.

- **Optická kabeláž** - obdobným způsobem funguje i přenos videosignálu po optické kabeláži. Jsou zde použité převodníky pro přenos videosignálu po optickém vláknu, které jsou osazeny na obou koncích přenosové trasy. Při tomto způsobu přenosu lze videosignál distribuovat až na vzdálenost několika kilometrů.

- **Digitální IP kamerové systémy** - u IP kamerových systémů se používá digitální přenos videosignálu pomocí počítačové sítě LAN - strukturované kabeláže. Samotný přenos digitálního videosignálu z IP kamery po kabelu počítačové sítě je omezen vzdáleností 90-100m k nejbližšímu aktivnímu prvku počítačové sítě. Za použití aktivních a bezdrátových prvků lze však vytvořit rozsáhlou počítačovou síť, po které lze obraz z IP kamer přenést na prakticky jakoukoli vzdálenost. Pomocí internetu lze videosignál z kamer přenášet po celém světě.

  Je ale potřeba věnovat pozornost při připojování IP kamer do datové sítě sloužící zároveň pro běžnou počítačovou komunikaci. Digitální přenos videosignálu z IP kamer může vytvářet velice objemné datové toky, které by mohly způsobovat brzdění ostatní datové komunikace v síti a v některých případech může způsobit i zhroucení počítačové sítě. Proto je důležité, aby byl IP kamerový systém řešen buď samostatnou oddělenou počítačovou sítí, nebo byly použity aktivní prvky, které umožňují nastavit prioritu určitého druhu provozu.

- **Bezdrátový přenos obrazu CCTV** - tento přenos lze za použití k tomu určené technologie použít jak pro analogové, tak pro digitální IP bezpečnostní kamery. Tento přenos se používá v případech, kdy nelze provést kabelové rozvody videosignálu. Nejčastěji používané frekvence pro přenos videosignálu jsou 2,4 GHz a 5,8GHz. Podmínkou pro spolehlivou funkci přenosu v tomto pásmu je vždy přímá viditelnost mezi vysílací a přijímací anténou a čistý éter s volnými kanály. Pomocí tohoto přenosu lze videosignál distribuovat na vzdálenost až 1 kilometrů. [11]

**Záznam a zpracování obrazu**

Dnes se používají dva základní druhy moderních záznamových zařízení **DVR** (digitální záznamová zařízení) a **NVR** (síťová záznamová zařízení).

Na trhu jsou dále k dispozici různé záznamové karty do PC, jejich použití, funkce a spolehlivost je omezena druhem použitého PC a jeho konfigurací a dle našich zkušeností tento způsob řešení není vhodný pro profesionální aplikace bezpečnostního kamerového systému CCTV. Často cena takto sestaveného PC se záznamovou kartou překračuje i profesionální záznamové zařízení, které je pro tyto účely vyrobeny a konfigurovány. [11]

**DVR rekordéry**

Digitální videorekordéry DVR se používají k záznamu analogového obrazu pořizovaného CCTV kamerami. Tento typ záznamového zařízení je nejvíce rozšířený. V poslední době se stále více používají takzvané hybridní rekordéry. Tyto rekordéry umí uchovávat záznam z analogových, tak i digitálních IP kamer, což přináší nesporné výhody při modernizaci stávajících kamerových systémů možností postupného přechodu z analogového na modernější digitální systém. Digitální videorekordéry DVR používají jako záznamové médium klasický počítačový pevný disk, na který je uložen záznam. Do většiny rekordérů je možné doplnit i více disků. Tím lze dosáhnout vyšší kapacity a tím i delší doby záznamu. Doba uchovávání záznamu z CCTV kamer závisí jednak na technických možnostech rekordéru, ale také na legislativě dle prostoru, účelu a způsobu využití záznamů z kamer (využívání kamerového systému z pohledu zákona). [11]

DVR záznamová zařízení zaznamenávají obraz z více kamer najednou (multiplexní režim). V základním provedení bývají záznamová zařízení určeny pro 4, 8, 16, 32 kamer.

Digitální videorekordéry DVR se neomezují pouze na záznam obrazu z CCTV kamer, ale disponují i velikým množstvím přídavných funkcí. Při ukládávání záznamu na pevný disk je záznam opatřen časovou stopou. Díky tomu je možné rychle záznam vyhledat, přehrávat, přetáčet popřípadě exportovat. Další velice oblíbenou funkcí DVR je záznam pomocí detekce pohybu. Díky této funkci je pořizován záznam až ve chvíli, kdy se v zájmové oblasti něco děje. Pevný disk tak není zaplňován nepotřebnými záznamy. DVR také disponuje funkcí časového plánu. Zde lze nastavit, po jakou část dne má probíhat stálý záznam, popřípadě v jaké kvalitě a kdy je třeba zaznamenávat pomocí detekce pohybu či nezaznamenávat vůbec. V dnešní době internetových technologií je základním požadavkem připojení DVR k síti. Většina rekordéru je proto opatřena síťovou kartou a umožňuje připojení k lokální počítačové síti s přístupem k internetu a tím i dosažitelnost záznamů v podstatě odkudkoli po světě například pomocí běžného webového prohlížeče.

Co se týče ostatních funkcí, které DVR umožňují, je důležité zmínit možnost záznamu zvuku, použití ovládacích vstupů a výstupů, ovládání otočných PTZ kamer, zasílání varovných emailů, zálohování záznamu na externí datové úložiště a další. [11]

**NVR rekordéry**

Síťová záznamová zařízení zaznamenávají digitální obraz z IP kamerových systémů. Záznam obrazu je jako u DVR ukládán na pevný disk. NVR jsou většinou umístěny samostatně mimo místo monitoringu. Tam jsou připojeny na počítačovou síť. Slouží tak prakticky jako datové úložiště. S kamerami komunikují pomocí TCP/IP adres. Monitoring systému může být prováděn prakticky z jakéhokoli PC připojeného do počítačové sítě. NVR jsou dodávány ve standardních konfiguracích pro 4, 8, 16, 24, 32, 48 a 64 IP kamer. Funkce, kterými rekordéry NVR disponují, jsou obdobné jako u DVR. [11]

**Normativní úprava CCTV a zákon o ochraně osobních údajů**

Provozování kamerového systému je považováno za zpracování osobních údajů,

pokud je vedle kamerového sledování prováděn záznam pořizovaných záběrů, nebo jsou

v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů,

případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s

určitým jednáním.

Samotné kamerové sledování fyzických osob není zpracováním osobních údajů podle zákona č. 101/2000 Sb., protože postrádá úroveň podmínek pro zpracování údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. To však nevylučuje aplikaci jiných právních předpisů, zejména ustanovení občanského zákoníku upravujícího podmínky ochrany osobnosti.

**ČSN EN 50 132 –7** Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích, Část 7: Pokyny pro aplikaci z roku 1999. Norma se skládá z těchto částí:

- Část 1: Systémové požadavky
- Část 2-1: Černobílé kamery
- Část 2-2: Barevné kamery
- Část 2-3: Objektivy
- Část 2-4: Příslušenství
- Část 3: Lokální a hlavní řídící jednotka
- Část 4-1: Černobílé monitory
- Část 4-2: Barevné monitory
- Část 4-3: Záznamová zařízení
- Část 4-4: Zařízení pro okamžitý výtisk obrazu
- Část 4-5: Videodetektor pohybu
- Část 5: Přenos videosignálu
- Část 7: Pokyny pro aplikaci ČSN EN 50132-2-1 [13]

### 2.2.4 EKV – Elektronická kontrola vstupu

*„Přístupový systém doplňuje předchozí tři základní zabezpečovací systémy. Nejblíže má k MZS a PZTS, s nimiž je konstrukčně spojen. V podstatě je to systém umožňující organizovat přístup určitých skupin osob do určených prostor a v určených časech. Stejného účinku by bylo možno dosáhnout pomocí svazku klíčů pro každého zaměstnance (klíče k těm dveřím, do kterých může), ale právě pro nepraktičnost a problémy při ztrátě klíčů vznikly elektronické přístupové systémy.*

*Systém je výběrový a bývá instalován jen v některých objektech finančních ústavů. Zpravidla se jedná o větší pobočky a odděluje obvykle veřejné prostory od zázemí a běžné prostory zázemí od režimových prostor s omezeným přístupem i pro zaměstnance.*

*U menších objektů je možno instalovat „off line" čtečky, které mají veškeré údaje ve své paměti a s řídícím PC si vyměňují data jen občas nebo na ruční příkaz. U větších aplikací bývají instalovány „on line" čtečky, které s řídícím PC komunikují neustále a v případě poruchy přejdou do autonomního režimu s využitím vlastní zálohy dat.*

*Napájení je řešeno vlastním zdrojem se záložním akumulátorem, který zajistí funkci systému i při výpadku síťového napájení.*

*Ovládání dveří se tak neprovádí klíčem, ale přiložením karty. Čtečka vyhodnotí oprávnění karty a sepne (nebo nesepne) elektrický zámek, který je součástí dveří. Při ztrátě karty nebo změně oprávnění se provede změna v databázi v řídícím PC a z něj se přenese do všech čteček.*

*Odlišná je situace v přístupu do samoobslužných zón bank (uzavřené zádveří s nočním trezorem a bankomatem). Zde bývá venkovní čtečka magnetických klientských karet příslušného finančního ústavu, přes kterou klient po pracovní době otevře vstupní dveře (pokud není uvnitř jiný klient). Odchází se přes odchodové tlačítko nebo pohybový otvírač dveří.“ [7]*

**Normativní úprava**

*„Výrobky elektrické kontroly vstupu (EKV) jsou řešeny harmonizovanými evropskými normami ČSN EN řady 50 133, popřípadě i Národním bezpečnostním úřadem dle Zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti a vyhlášky NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.“ [14]*

### 2.2.5 EPS – Elektronická požární signalizace

Systém požární elektronické signalizace je soubor prvku k vyhodnocování vzniku požáru v objektu. Slouží k včasné detekci požáru a tím následně k ochraně osob a majetku před požárem. Včasná detekce mnohdy zabrání mnohomiliónovým škodám a ochránit spoustu lidských životů, které mohou být způsobeny požárem.

Hlavní funkce EPS jsou:

- detekce požáru a vyhlášení požárního signálu
- předání informace o požáru na vzdálené místo (ohlašovna požáru)
- ovládání zařízení, která slouží k šíření požáru, usnadňují, případně přímo provádí protipožární zákrok
- vydání signálu, které ovládají další důležité zařízení (vypnutí elektrického proudu, odvod tepla a kouře, evakuační rozhlas, výtahy)

Z hlediska principu lze EPS rozdělit na konvenční a adresné systémy.

Funkce **konvenčních systémů** elektrické požární signalizace je založena na detekci pomocí vyhodnocení proudových změn na smyčce, na které jsou osazené požární hlásiče. V případě vzniku požáru, změní aktivní požární hlásič celkový odpor smyčky. Tyto změny jsou následně vyhodnoceny požární ústřednou a poté je vyhlášen požární poplach. Vedení jednotlivých smyček požární signalizace je provedeno paprskově z požární ústředny EPS a zakončeno vyvažovacími odpory.

Výhodou těchto požárních systémů je nízká cena. Naopak nevýhodou těchto systémů požární signalizace je velmi omezená nebo žádná možnost přesného umístění požárního hlásiče, který detekuje poplach. Dále nelze zjišťovat stavy jednotlivých detekčních prvků v rámci linky. Rovněž obsluha konvenční požární signalizace je omezena pouze na ovládání celých linek a nikoli jednotlivých požárních hlásičů.
Dále je velmi problematické provádění různých změn v požární signalizaci z hlediska ovládání či přiřazování jednotlivých požárních hlásičů do skupin (zpravidla 1 linka = 1skupina hlásičů).

**Adresné systémy** požární signalizace pracují na principu datové komunikace s jednotlivými prvky, umístěnými na tzv. dialogové lince. Každý prvek požární signalizace na datové lince má svoji přesnou identifikaci a sám komunikuje s požární ústřednou. Jednotlivé prvky systému požární signalizace jsou seřazeny v software požární ústředny do skupin a funkčních celků a jejich přiřazení, adresace a funkce jsou volně nastavitelné, a to samostatně pro každý prvek požárního systému.

Programování a nastavení požární signalizace se provádí pomocí počítače propojeného s konfiguračním programem. Velkou výhodou adresných požárních signalizačních systémů je přesná identifikace každého požárního prvku v systému a tím i možnost přesné a rychlé lokalizace místa požáru. Každý prvek je opatřen přesným popisem, který je zobrazen na displeji požární ústředny nebo ovládacího panelu. Další výhodou je i jednoduchá kabeláž požárních linek a jejich velká kapacita osazení jednotlivými detekčními prvky. Na lince mohou být připojeny jak prvky detekční (požární hlásiče) tak i ovládací (reléové prvky).

Na jedné adresné lince mohou být stovky prvků v závislosti na jejich odběru a použitém systému požární signalizace EPS. Linky jsou řešeny jako kruhové, což znamená zvýšení spolehlivosti funkce požární signalizace EPS v případě poruchy kabeláže (zkrat, přerušení). Do každé požární ústředny může být svedeno několik linek.

U moderních adresných systémů elektrické požární signalizace je možné jednotlivé požární ústředny spojovat do společné sítě a tím získat kompaktní a moderní systém elektrické požární signalizace i u velmi rozsáhlých objektů a areálů.
Tyto vlastnosti zajišťují také velice snadné změny konfigurace a nastavení požární signalizace, popřípadě její rozšiřování. Údržba a pravidelné zkoušky jsou z důvodu přesnějších informací a možností nastavení jednotlivých detekčních prvků podstatně flexibilnější a jednodušší. [6]

**Každou EPS lze rozdělit na tři části:**

- řídící a vyhodnocovací jednotka (požární ústředna)
- detekční část (požární hlásiče)
- ovládací a signalizační část (požární sirény, dálkový přenos signálu)

### Ústředny EPS

Požární ústředna zabezpečuje kompletní funkce celého systému EPS. Jedná se zejména o napájení a vyhodnocování stavu požárních hlásičů, ovládání požární signalizace a aktivace ovládacích prvků návazných zařízení a v neposlední řadě také o kontrolu stavu a provozuschopnosti celého zařízení EPS nebo i ostatních připojených zařízení. Napájení každé požární ústředny musí být zálohováno a to proti výpadku napájecí sítě akumulátory. Každé zařízení elektrické požární signalizace musí být schopno provozu na náhradní zdroj po dobu minimálně 24 hodin, z toho 15min ve stavu signalizace požáru.
V dnešní době moderní požární ústředny mají široké možnosti programování jejich funkcí a tím i optimalizaci celého systému EPS v daných objektech nebo areálech. Výhodnou funkcí moderních systémů EPS je možnost síťování ústředen, a tím vytvoření jednoho kompaktního systému požární signalizace a to i ve velkých areálech či aglomeracích. Systémy EPS je možné ovládat nebo monitorovat přímo na místě, ale také na dálku pomocí internetu, GPRS přenosů. [6]

### Hlásiče požáru

Požární hlásiče slouží ke identifikaci požáru a zaslání informace do požární ústředny. Hlásiče požáru jsou tlačítkové nebo automatické. Tlačítkové hlásiče slouží k ručnímu vyvolání požárního poplachu osobami, které se nachází při zjištění požáru nebo kritické situace.
Automatické hlásiče požáru reagují na výskyt nebo změnu fyzikálních parametrů prostředí bez nutnosti zásahu lidského činitele. Dle principu detekce je určen i způsob jejich použití v různých prostředích. Jejich vhodným výběrem je zajištěna včasná detekce vznikajícího požáru a spolehlivost funkce bez zbytečných planých poplachů.

Hlásiče požáru můžeme rozdělit:

- opticko-kouřové požární hlásiče
- teplotní hlásiče požáru
- lineární teplotní kabely
- lineární kouřové hlásiče požáru
- hlásiče vyzařování plamene

- kombinované hlásiče požáru
- kouřový nasávací systém
- ionizační hlásiče požáru [6]

**Normativní úprava EPS**

- Zákon č. 133/1985 Sb. „O požární ochraně“
- VYHLÁŠKA 23 ze dne 29. Ledna 2008 „O technických podmínkách požární ochrany staveb“
- VYHLÁŠKA 246/2001 Sb. ze dne 29. června 2001 „O stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)“
- V dubnu 2011 bylo vydáno nové znění ČSN 73 0875 Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení. Při projektování nových stavebních objektů a při projektování změn stávajících objektů a technologických souborů a to zejména v návaznosti na požárně bezpečnostní řešení podle příslušného právního předpisu (§ 41 vyhlášky č. 246/2001 Sb.).

- Konkrétní návrh a dokumentace (projekt) EPS se provádí podle ČSN 34 2710

V porovnání s předchozí normou byly provedeny tyto změny:

- tato norma je nově zaměřena zejména na zadávací podmínky pro návrh elektrické požární signalizace v rozsahu požárně bezpečnostního řešení podle § 41 Vyhlášky č. 246/2001 Sb.;
- z této normy jsou vypuštěny články, které se následně řeší podle ČSN 34 2710;
- je podstatně doplněno a zpřesněno názvosloví;
- nově je v ČSN 73 0875 řešeno, kdy je nutné instalovat EPS v požárním úseku, v celém objektu, i požadavek na instalace zařízení dálkového přenosu; dále je řešen požadavek na vybavení zařízením EPS i prostory nad podhledy nebo ve zdvojených podlahách;

- norma stanoví požadavky na zařízení EPS, umístění ústředny, požadavky na trvalou obsluhu apod. v návaznosti na skutečnost, zda je EPS v objektu požadovaná právními předpisy a/nebo normativními požadavky nebo nikoli;
- norma definuje hlavní zásady součinnosti a koordinace požárně bezpečnostních zařízení;
- nově je v normě řešeno provedení koordinačních funkčních zkoušek zařízení EPS a navazujících systémů požární ochrany (včetně ovládaných zařízení);
- v normě jsou stanoveny požadavky na zařízení dálkového přenosu;
- norma ruší výpočet hodnoty N – stanovení nutnosti střežení EPS.
- ČSN 342710 „Předpisy pro zařízení EPS“
- ČSN EN 54 – 1 „EPS - část 1: Úvod“
- ČSN EN 54 – 2 „EPS - část 2: Ústředna“
- ČSN EN 54 – 4 „EPS - část 4: Napájecí zdroj“
- ČSN EN 54 – 5 „EPS - část 5: Hlásiče teplot“
- ČSN EN 54 – 7 „EPS - část 7: Hlásiče kouře“
- ČSN EN 54 – 11 „EPS - část 11: Hlásiče tlačítkové“
- ČSN EN 54 – 3 „EPS - část 3: Požární poplachové zařízení sirény“
- ČSN EN 54 – 10 „EPS - část 10: Hlásiče plamene“
- ČSN EN 54 – 12 „EPS - část 12: Hlásiče kouře lineární“
- ČSN P CEN/TS 54 – 14 Aplikační návody

**Požadavky na kabeláž EPS:**

- EN 50 266 – 1 – definice požární odolnosti kabelu
- EN 50 266 – definice požární odolnosti kabelu ve svazku
- EN 50 267 – definice obsahu halogenových prvků v materiálu izolace
- EN 61034 – definuje emise kouře
- IEC 60331 – definuje celistvost obvodu při požáru

- VDE 4102 – 12 – definuje funkční schopnost celého nosného systému (včetně kabelu)
- ZP 27/2006 – zkušební předpis PAVUZ pro zkoušky funkční schopnosti [8]

## 2.3 Ochrana systémová (integrovaná)

*„Elektronické poplachové systémy se zrychleným tempem technicky proměňují a stávají se standardním informačním prostředkem pracujícím v prostředí lokálních počítačových sítí LAN nebo v prostředích sítí WAN. Možnost využití standardního komunikačního protokolu jako je internetový protokol TCP/IP umožnila výrobcům vyvinout novou generaci integrovaných systémů. Takové systémy se většinou označují pojmem Integrované bezpečnostní systémy (Integrated Security Management Systems – ISMS), neboť svými komplexními funkcemi pokrývají všechny požadavky organizací na podnikovou bezpečnost.*

*Integrované bezpečnostní systémy mohou vzájemně propojit různé bezpečnostní subsystémy (přístupový systém ACS, poplachový systém EZS, průmyslovou televizi CCTV), protipožární signalizaci EPS, technické systémy budov (klimatizace, osvětlení).*

*Integrované provedení poplachového systému může snížit celkové náklady za instalaci a způsobit zásadní změnu v chování investice omezením drahých manuálních úkonů. Je třeba zdůraznit, že hlavní přínosem je posílená bezpečnost, to, ţe nevznikají v systému zbytečné časové prodlevy, což bývá obvykle velkým problémem, nezávisle na tom, zda se jedná o organizace ve veřejném nebo soukromém sektoru. Jsou zde takové výhody, které přináší schopnost přijímat signály ze všech podsystémů do jednotného operátorského prostředí a možnost přímých vazeb signálů z přístupových a detekčních podsystémů na záznamy průmyslové televize. Vyhodnocovací proces může být tímto způsobem mnohem účinnější a omezuje požadavky vysílání zásahových pracovníků na fyzické prověření vzniklé poplachové události.“* [9]

**Normativní úprava**

Pro zařízení integrovaných bezpečnostních systémů jsou evropském i britském prostředí k dispozici soubory norem DD CLC/TS 50398:2002 (Alarm systems. Combined and integrated alarm systems. General requirements).

Norma uvádí všeobecné požadavky a struktury kombinovaných a integrovaných poplachových systémů. Norma má zajistit integraci jedné nebo i více aplikací do jednoho integrovaného systému. Tento dokument poskytuje další informace, které se týkají prvotního návrhu (projektu) systému, plánování, instalace, předávání, provozu a údržby (servisu) kombinovaného a integrovaného systému. Tato norma uvádí požadavky na poplachové systémy, které jsou kombinovány nebo integrovány s jinými systémy, které mohou a nemusí být poplachovými systémy. Definuje požadavky, které se týkající pravidel integrace s cílem zdůraznit význam jednotlivých aplikačních poplachových norem a objasnit případné rozpory. [15]

# II. PRAKTICKÁ ČÁST

# 3 POPIS OBJEKTU

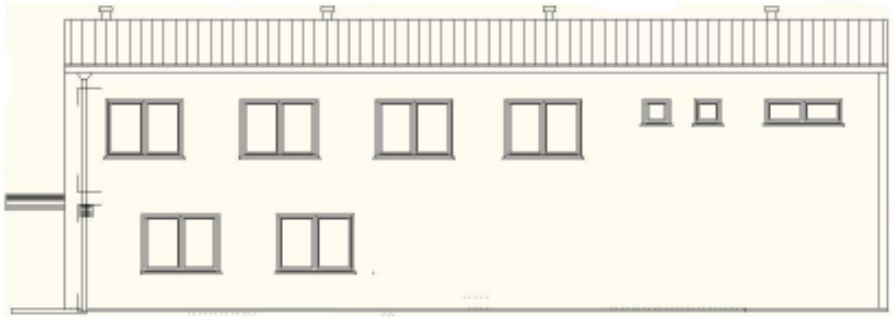
Zvolený objekt je budova banky, která se nachází v centru malého města. Budova má dvě patra a přilehlý dvůr. Budova banky má tři vstupy. Hlavní vstupní dveře slouží pro klienty a návštěvníky banky. Druhý vstup využívají běžní zaměstnanci banky. Třetím vstupem je brána, která slouží pro využití zaměstnanců bezpečnostních služeb při transportu cenin.

V prvním patře je rozsáhlá bankovní hala pro klienty, ve které se nachází tři bankovní přepážky. V tomto patře se nachází také místnost pro ostrahu, šatna pro zaměstnance, počítárna bankovek a mincí a trezorová místnost, tyto místnosti jsou nepřístupné klientům. Mohou je využívat pouze zaměstnanci banky.

V druhém patře se nachází jednací místnost, která má největší plochu. V tomto patře se dále nachází místnosti, jako jsou například: kancelář ředitele, kanceláře zaměstnanců banky, místnost pro řízení softwaru banky a archiv dokumentu.

Banka se nachází v lokalitě, která je přístupná klientům například pomocí městské hromadné dopravy. Zastávka městské hromadné dopravy leží naproti hlavnímu vchodu banky. Před bankou je vybudováno malé parkoviště s pakovacím místem pro čtyři automobily. Nedaleko od banky (cca 200m) je sídlo městské policie. Banka nepřímo sousedí s objekty, které slouží pro komerční využití.

Obr. 1. Pohled ze předu



Obr. 2. Pohled z boku

# 4 KRITERIA NÁVRHU BEZPEČNOSTNÍCH TECHNOLOGII

Podstatou je dosáhnout maximální bezpečnosti provozu příslušné banky s důrazem na zabezpečení hotovosti proti odcizení zvenku i zevnitř, na zabezpečení dat klientů a minimalizaci nebezpečí napadení klientských účtů. Není zde řešena ochrana proti napadení z informačních sítí, ale ochrana proti napadení osobou fyzicky přítomnou v objektu.

## 4.1 Návrh PZTS

Musíme vycházet z požadavků národního bezpečnostního úřadu, hlavním stanoviskem je zařazení objektu do stupně zabezpečení. Banky spadají do 3. stupně zabezpečení, to znamená střední až vysoké riziko.

**Orientační rozdělení stupňů zabezpečení:**

**Stupeň 1:** Nízké riziko (chaty, garáže, rodinné domy, strojovny)

**Stupeň 2:** Nízké až střední riziko (komerční objekty)

**Stupeň 3: S**třední až vysoké riziko (zbraně, ceniny, informace, narkotika)

**Stupeň 4:** Vysoké riziko (zejména objekty národního a vyššího významu)

Struktura bezpečnostní systému je úměrná třídě zabezpečení. Při návrhu PZTS se řídím následující tabulkou. Všechna zařízení a komponenty PZTS byly vybrány tak, aby byly v souladu všem požadavkům pro zabezpečení objektu spadajícího do 3. stupně zabezpečení (P – tajné). Prvky vybrané k použití zabezpečení objektu musí splňovat platné standarty a normativní úpravu tykajících se PZTS (ČSN 50 – 131 – 1), o kterých přesně hovoří Zákon 22/97 Sb. Optimální doporučená ochrana objektu je uvedena v následující tabulce. [18]

Tab. 1. Optimální doporučená ochrana objektu

| Ochrana objektu | Detekce | Stupeň 1 | Stupeň 2 | Stupeň 3 | Stupeň 4 |
|---|---|---|---|---|---|
| 1 Vstupy-otevření | Kontakt | ano | ano | ano | ano |
| 2 Vstupy-průnik | Prostorový detektor | vhodné | vhodné | ano | ano |
| 3 Vstupy-uzamčení | El. zámek | ne | ne | vhodné | ano |
| 4 Chodby prostor | Prostorový detektor | ano | ano | ano | ano |
| 5 Otevření oken | Kontakt | ne | ano | ano | ano |
| 6 Průraz oken | Akustické čidlo | ne | ano | ano | ano |
| 7 Prostor místnosti | Prostorový detektor | vhodné | přednostně | ano | ano |
| 8 Stěny stropy podlahy | Vibrační apod. | ne | ne | volba | ano |
| **Signalizace poplachu** | | | | | |
| 1 vnitřní siréna | | volba | volba | volba | volba |
| 2 venkovní siréna | | doporučeno | ano + volba | ano + volba | volba |
| 3 telefonní zpráva | | doporučeno | volba | volba | volba |
| 4 telefonní PCO | | volba | doporučeno | ano + volba | ano + volba |
| 5 RST přenos PCO | | volba | doporučeno | ano + volba | ano + volba |
| 6 fyzická ostraha | | x | x | volba | ano + volba |
| 7 Přivolání pomoci | | ano při b.3,4 | doporučeno | ano | ano |

## 4.2 Návrh EPS

Elektronická požární signalizace je navržena v souladu s ČSN 730875. Automatické hlásiče budou umístěny. Na chodbách, schodištích a u východů z budovy budou umístěny tlačítkové hlásiče. Umístění všech hlásičů musí umožňovat přístup pro periodické zkoušky a revize zařízení. Všechny hlásiče budou označeny popisnými identifikačními štítky s adresou hlásiče.

Systém požárního zabezpečení bude pracovat ve dvou režimech a to v denním, kdy je banka otevřena a v nočním, kdy se v bance nebude nikdo nacházet.

Popis signalizace požáru všeobecně - vyhlášení požáru je signalizováno jak akusticky, tak i opticky, přímo na požární ústředně. V režimu **DEN** (při obsluhované ústředně) je - při signalizaci požáru z automatických hlásičů požáru - vyhlášen nejdříve „Úsekový poplach”.

Na ústředně je započato s odměřováním času T1 (max. 3 minuty). Pracovník pověřený obsluhou ústředny EPS zruší na ústředně EPS akustickou signalizaci; pokud to nestihne, po uplynutí času T1 se automaticky vyhlásí všeobecný poplach. Zrušením akustické signalizace na ústředně je ukončeno odměřování času T1 a ústředna začne odměřovat čas T2 (max. 20 minut). V tomto čase T2 musí obsluha ústředny EPS prověřit skutečný stav prohlídkou daného místa, odkud je signalizován požár. Pokud obsluha ústředny v průběhu času T2 neprovede nulování poplachu nebo vyhlášení „Manuálního poplachu“, dojde k vyhlášení „Všeobecného poplachu“ automaticky po uplynutí času T2. Při signalizaci požáru tlačítkovým hlásičem je vyhlášen „Všeobecný poplach“ okamžitě.

V režimu **NOC**, to je v době, kdy je ústředna neobsluhovaná, je při signalizaci požáru libovolným hlásičem vyhlášen „Všeobecný poplach“ okamžitě. Po vyhlášení „všeobecného poplachu“ se uskuteční přenos informace do místa stálé služby, například na PCO u hasičského záchranného sboru. Tento přenos lze uskutečnit pomocí přenosového zařízení po JTS nebo pomocí ZDP.

Elektronickou požární signalizaci je nutné brát jako jeden z vyhrazených provozních souborů daného objektu, jehož smysl je dán tím, že umožní včasnou signalizací likvidovat požár v samém zárodku. Signalizace má buď automaticky, nebo pomocí lidského činitele rychle určit místo vzniku požáru a předat tuto informaci bezprostředně osobám, které mají možnost požár zlikvidovat.

Nelze tedy EPS považovat za komplexní ochranu objektu před požárem, ale jen jako pomocné zařízení, které slouží k podstatnému zkrácení doby od zjištění požáru k potřebnému protipožárnímu zákroku.

Pro vytvoření dobrého projektu musí mít projektant správné podklady dodané objednatelem. Z hlediska požární ochrany musí podklady pro EPS řešit následující otázky k zabezpečení daného objektu nebo technologického zařízení: [19]

- protokol o prostředí v dotčených prostorech,
- členění objektu podle požárních úseků a rozsah EPS (požárně technická zpráva, nebo vytipování prostor)
- požadavky na ovládání dalších technologických zařízení bránící dalšímu rozšíření požáru nebo umožňující snadnější protipožární zásah,

- návaznost EPS na další protipožární opatření, včetně způsobu vyhlášení požárního poplachu
- umístění ústředny EPS, případně paralelní signalizace na signálních panelech, podle stanoviště trvalé služby.

Projektant ke své činnosti potřebuje výkresové podklady objektu.

- Půdorys areálu nebo celkový přehledový výkres v měřítku, ze kterého je patrné rozmístění objektů chráněných zařízením EPS, umístění ústředny EPS v místě trvalé obsluhy a případně umístění paralelních signálních panelů. V situaci jsou zejména venkovní rozvody propojující zařízení EPS v jednotlivých objektech stavby.
- Stavební výkresy jednotlivých budov a jednotlivých podlaží (půdorysy a řezy) v měřítku, budou zde zakresleny polohy jednotlivých zařízení včetně kabelových rozvodů; ze stavebních výkresů je nutné mít možnost určit tvar a členění stropů a umístění technologických zařízení.
- Případně výkresy elektronické technologie (výkresy silnoproudých rozvodů kvůli souběhům, výkresy slaboproudých rozvodů - koordinace tras).

EPS musí být navržena tak, aby byla funkčně účelná, hospodárná a úměrná nákladům na požární ochranu ve vztahu ke chráněným hodnotám a pravděpodobnosti vzniku požáru. Musí být zajištěno co nejrovnoměrnější účinné střežení kteréhokoliv místa v požárním úseku. Musí být vyloučena nežádoucí funkce hlásiče (falešný poplach) Elektronické zařízení musí být provedeno dle příslušných ČSN a EN.

Každá projektová dokumentace EPS musí být předložena k vyjádření na místně příslušném HZS (dle ustanovení § 31 odst. 1 písm. b zákona č.133/1985 Sb. o požární ochraně ve znění zákona 67/2001).[19]

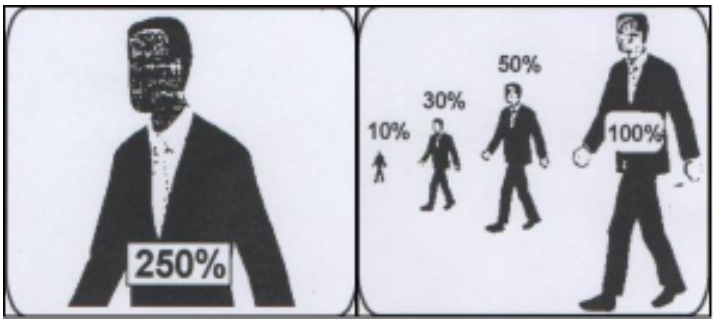
## 4.3 Návrh CCTV

Při návrhu instalace sledovacího CCTV systému je důležité brát v úvahu následující kriteria zohledňující funkční požadavky. Určení zón nebo objektů, které jsou předmětem sledování. Určení počtu a rozmístění kamer potřebných k monitorování vymezených zón a objektů. Vyhodnocení stávající úrovně osvětlení a provedení rozvahy o zavedení nového

nebo přídavného osvětlení. Volba kamer a jejich komponentů v závislosti na provozních podmínkách. Požadavky správné konfigurace řídícího pracoviště. Volba způsobu napájení a určení funkčních požadavků a provozních postupů.

Doporučená velikost objektu (cíle) na obrazovce monitoru by měla být odvozena od požadovaného stupně jeho rozpoznání. Jde – li o identifikaci (rozpoznání detailů na objektu), rekognoskaci (rozpoznání obrysů objektu) a detekci (zjištění přítomnosti objektu) nebo pouhé monitorování. Ve finančních institucích jde převážně o získání identifikace osoby a CCTV systém má omezenou rozlišovací schopnost cca. 400 televizních řádků doporučují se následující minimální velikost pozorovaného objektu na obrazovce:

- pro identifikaci by cíl neměl představovat méně než 120% výšky obrazovky;
- pro rekognoskaci by cíl neměl představovat méně než 50% výšky obrazovky;
- pro detekci by cíl neměl představovat méně než 10% výšky obrazovky;
- pro monitorování skupiny osob by cíl neměl představovat méně než 5% výšky obrazovky. [13]
- **Zachycení obrazu (EN 50132-7)**
- Detailní ID  1 mm/ pixel
- Identifikace  4 mm/ pixel
- Rekognoskace  8 mm/ pixel
- Sledování  16 mm/ pixel
- Detekce osoby  40 mm/ pixel
- Monitoring skupiny  80 mm/ pixel




Obr. 3. Doporučená velikost objektu [13]

# 5 NÁVRH TECHNICKÉHO ZABEZPEČENÍ FINANČNÍ INSTITUCE

## 5.1 Poplachový zabezpečovací a tísňový systém

Veškeré finanční instituce jsou řazeny do 3. bezpečnostní třídy. V této práci porovnávám dvě ústředny, které jsou dostupné na našem trhu. V jedné ze dvou variant je použit systém Galaxy G3V.6, který je známý pod novým názvem Galaxy Dimension. Tato ústředna je novým komplexně kombinovaným systémem zabezpečení a kontroly vstupu. Firma Honeywell Security, která vyvinula ústřednu Galaxy Dimension uvádí nové dokonalejší funkce v oblasti kontroly vstupu, při čemž nijak nesnižuje úroveň či stupeň požadovaného zabezpečení. Grafická klávesnice s dotykovým displejem umožňuje jednodušší ovládání a výrazně eliminuje chyby uživatelů. Výhodou pro uživatele je přiblížení celého systému, přehledné indikace stavu detektoru a nové možnosti zobrazení historie přímo na klávesnici. Kombinace funkcí dálkové správy (RS 232, TCP/IP) a automatické diagnostiky zajistí, že váš systém bude fungovat stále s optimálním výkonem.

Ústředny Galaxy jsou dlouhodobě využívány nejen ve finančních institucích, ale také v rozsáhlých podnicích zabývající se komerční sférou.

**Parametry Galaxy Dimension GD-264**

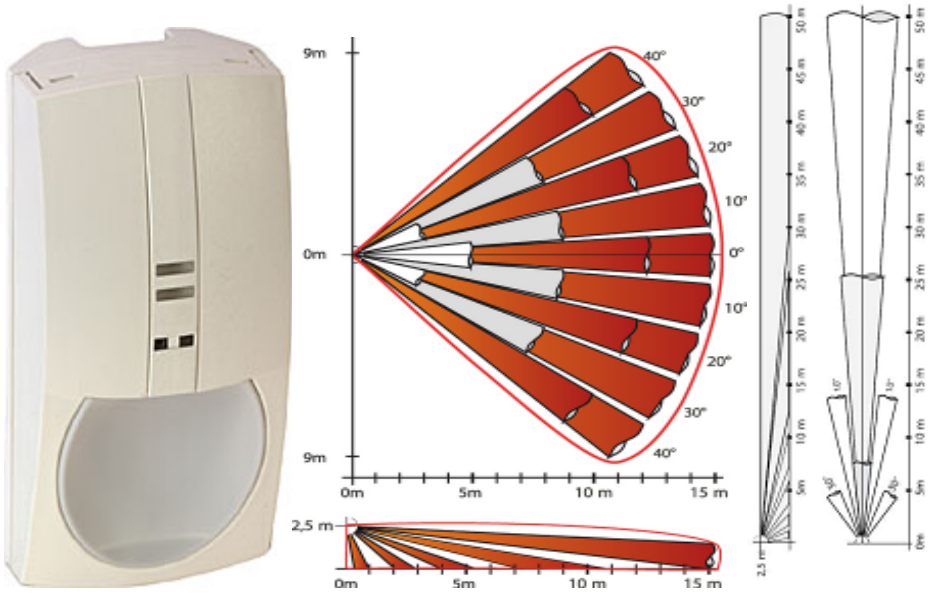
- až 264 zón
- až 32 podsystémů
- až 16 modulů kontroly vstupu
- až 1000 uživatelských kódů
- až 67 týdenních časových rozvrhů
- až 16 LCD klávesnic a 2 grafické dotykové klávesnice
- možnosti komunikace (Ethernet, RS-232, telefonní linka)
- možnost integrace grafické nadstavby
- vyhovuje normám EN 50 131-1 a CLC TS 50 131-3
- možnost hardwarového rozšíření [20]

Obr. 4. Ústředna Galaxy Dimension

### 5.1.1 Technické řešení systému

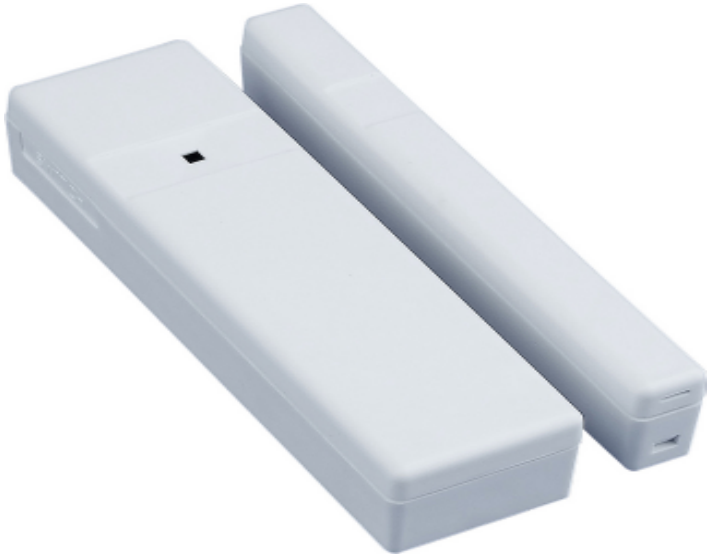
S ohledem na to, že finanční instituce podléhají vysokým nárokům na režimová opatření, bezpečnostní systém bude rozdělen na několik podsystému. Trezorová místnost bude jeden podsystém doplněný časovým zámkem při výdeji hotovosti. Další podsystémy jsou děleny na prosty vyhrazeny pouze zaměstnancům a prostory pro klienty.

**Prostorová ochrana** je řešena pomocí PIR detektoru VIEWGUARD se zrcadlovou optikou, funkcí antimasking (do 30 cm), nízká spotřeba (odběr proudu 4,6 mA). Detektory Viewguard analyzují typ příchozího signálu pomoci integrovaného mikroprocesoru. Při rozhodování zda vyhlásit poplach nebo ne, je klíčovým prvkem síla signálu. Detektory reaguji na příchozí signály s nesmírnou rychlostí, zabraňuji vyhlášení falešného poplachu z důvodu nekvalitního signálu a zároveň hlídají, zda se narušitel nesnaží snímač oklamat. Mechanická konstrukce zjednodušuje montáž a servis, protože elektronika detektoru je v předním krytu a nasouvá se na konektor ve spodní části krytu, který zůstává uchycen na svém místě. [12]




Obr. 5. PIR detektor viewguard a jeho charakteristiky[12]

**Obvodovou ochranu** objektu tvoří kombinace kvalitního duálního detektoru tříštění skla (dosah 2,4m) s magnetickým kontaktem, tedy dovoluje jedním prvkem detekovat jak rozbití skla tak otevření okna. Detektor tříštění skla lze použít i pro skleněné plochy s nalepenou bezpečnostní fólií. Na dveře je použity polarizovaný kontakt s vyšší bezpečností pro skrytou zápustnou montáž.



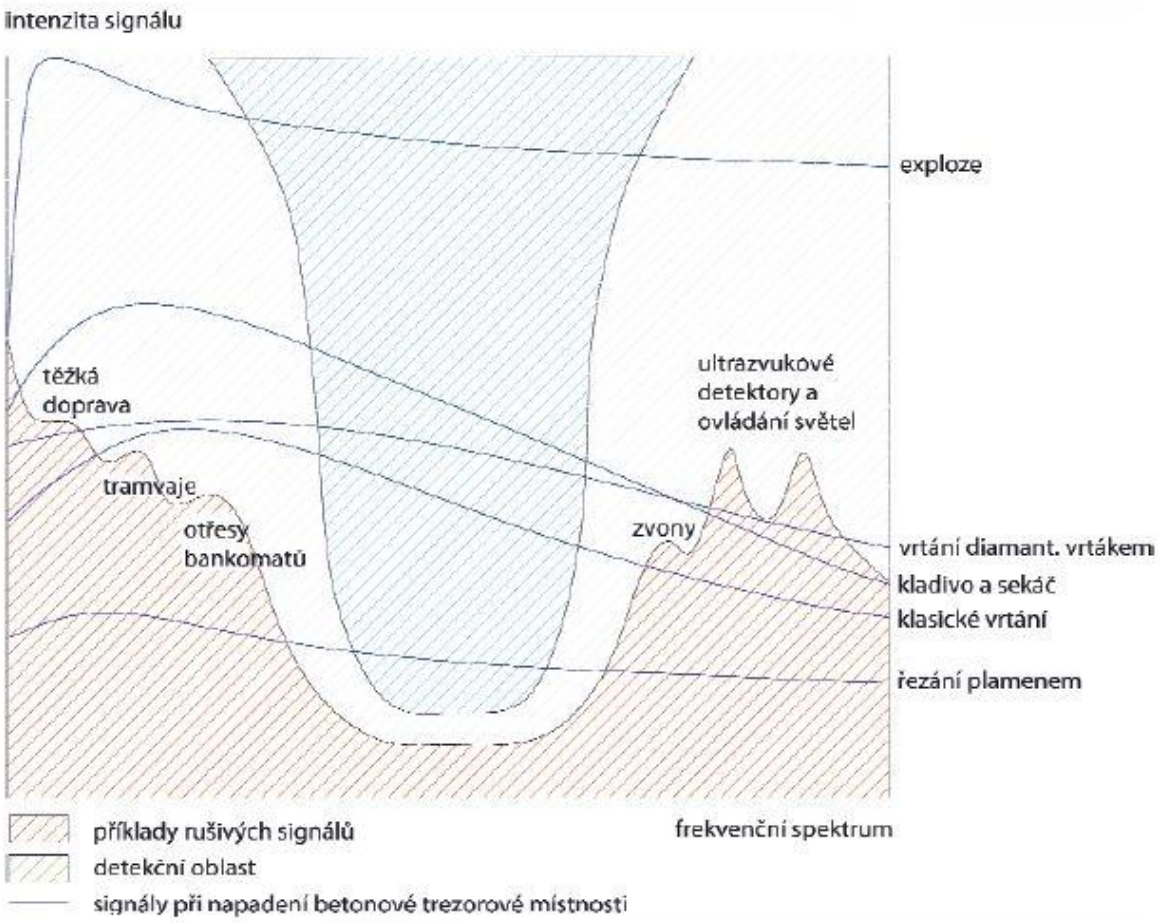
Obr. 6. Detektor  tříštění skla s mag. kontaktem [12]

**Předmětovou ochranu** rozumíme detektory posledních bankovek, trezor, trezorová místnost, bankomat, archiv.

Vibrační detektor Honeywell SC100 je navržena pro účely detekce vybraných otřesů od jednoduchých pokusů o vniknutí narušitelem do chráněných prostor až po napadení úložných trezorů, kde jsou uchovány cennosti. Univerzální otřesový detektor, který lze využít pro ochranu trezorů, dveří, pevných bankomatů, sejfů a dalších objektů s pevnou strukturou.

Každý typ mechanického napadení má specifické rysy, které je nutné detekovat, analyzovat a případně vyloučit rušivé vlivy. Například řezání plamenem nebo vodním paprskem má nízkou úroveň detekovatelných signálů; vrtání klasickým nebo diamantovým vrtákem, rozbrušování diamantovým kotoučem má střední úroveň signálu; sekání sekáčem, kladivem nebo útok výbušninou má naopak vysokou úroveň signálů. Součástí detektoru je i interní teplotní čidlo, které zajišťuje včasnou detekci případné sabotáže prudkou změnou teplot. [12]


Obr. 7. Otřesový detektor Honeywell SC100




Obr. 8. Detekční vlastnosti otřesového detektoru

Na ochranu dveří do trezorů je použit závrtný magnetický kontakt SENTROL S1078CS, který je vhodný k použití kovových dveří. Protože kontakt má vzduchovou distanční mezeru, která eliminuje vliv magneticky vodivého materiálu na velikost pracovní mezery. Kontakt je čtyř drátový pro snížení rizika sabotáže.

Obr. 9. Závrtný mag. kontakt

Detektor poslední bankovky je umístěn v trezoru a za přepážkou na vklad a výdej peněz. Detektor S3555 je připevněn pomocí samolepící pásky na dno kasy. Při vyjmutí všech peněz dojde k aktivaci tichého poplachu. Jeho tělo je z odolného plastu uvnitř je hermeticky utěsněné jazýčkové relé. Odolává vlhkosti, prašnému prostředí, nárazům a otřesům bez vyvolání falešných poplachů.

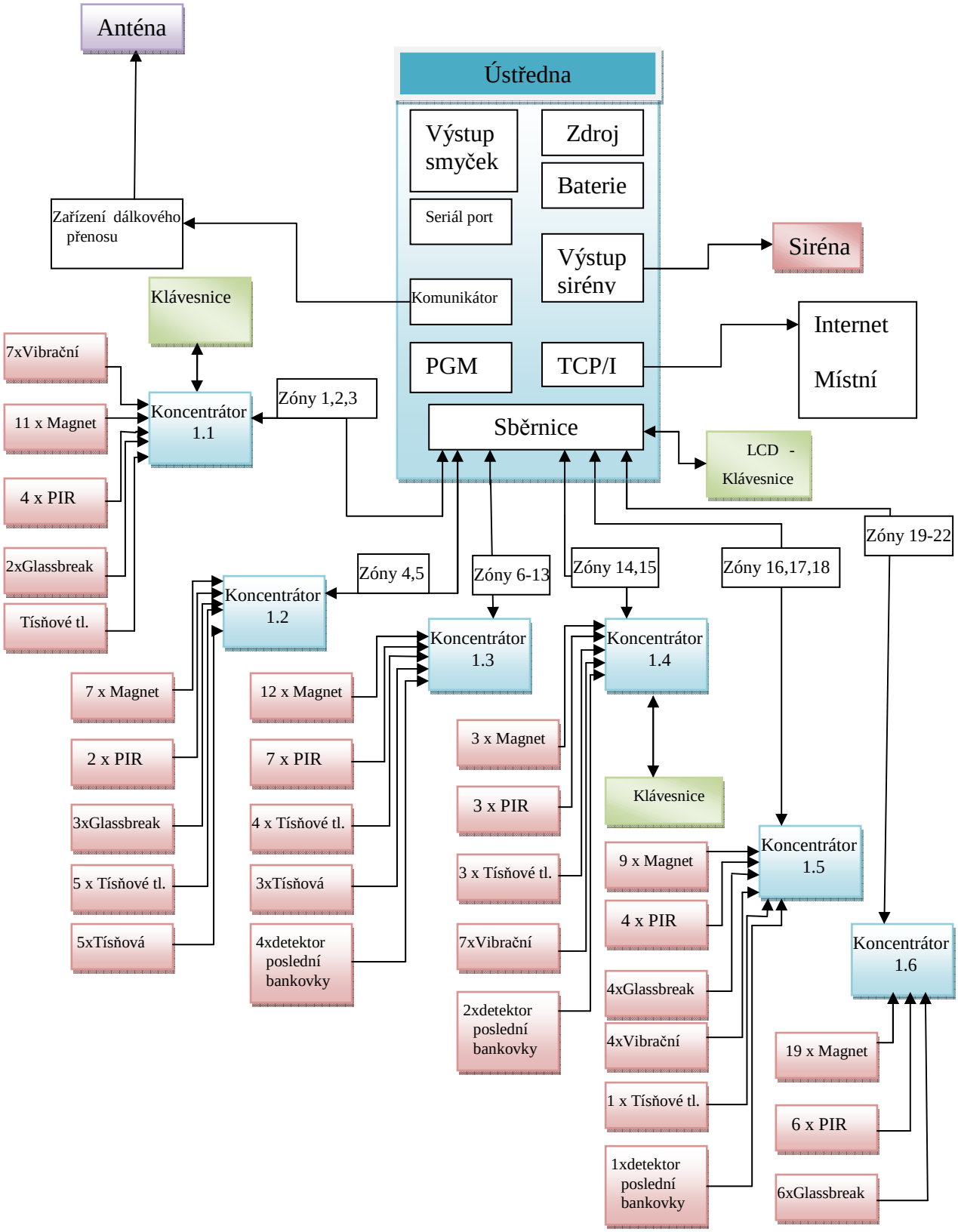
Jako prvek **tísňové ochrany** jsou použity tísňové tlačítka SENTROL S3040/SROV. Uživatel by při aktivaci tlačítka neměl budit pozornost, proto se umísťuje na vnitřní strany stolu nebo ze spodní strany pracovní desky tak, aby nebyl za normálního provozu vidět. Dále je použit u vchodů do trezorové místnosti. Při aktivaci poplachu se rozsvítí indikující dioda a je vyslán tichý poplach do ústředny. [12]


Obr. 10. Tísňové hlásič

Pro vyhlášení tichého poplachu je zde ještě výklopná tísňová lišta Menvier CSA TL485 s pamětí poplachu. Poplach se aktivuje vykopnutím nebo nadzvednutím pohyblivé části nohou. Brání vzniku falešných poplachů, jak tomu je u tísňových pedálů. Umístí se pod stůl na takové místo, aby nebylo za normálního provozu viditelné.

Obr. 11. Tísňová lišta

### 5.1.2 Blokové schéma návrhu PZTS




Obr. 12. Blokové schéma návrhu PZTS

### 5.1.3 Návrh rozmístění prvků

Viz. příloha č. 1.

## 5.2 Elektronická požární signalizace

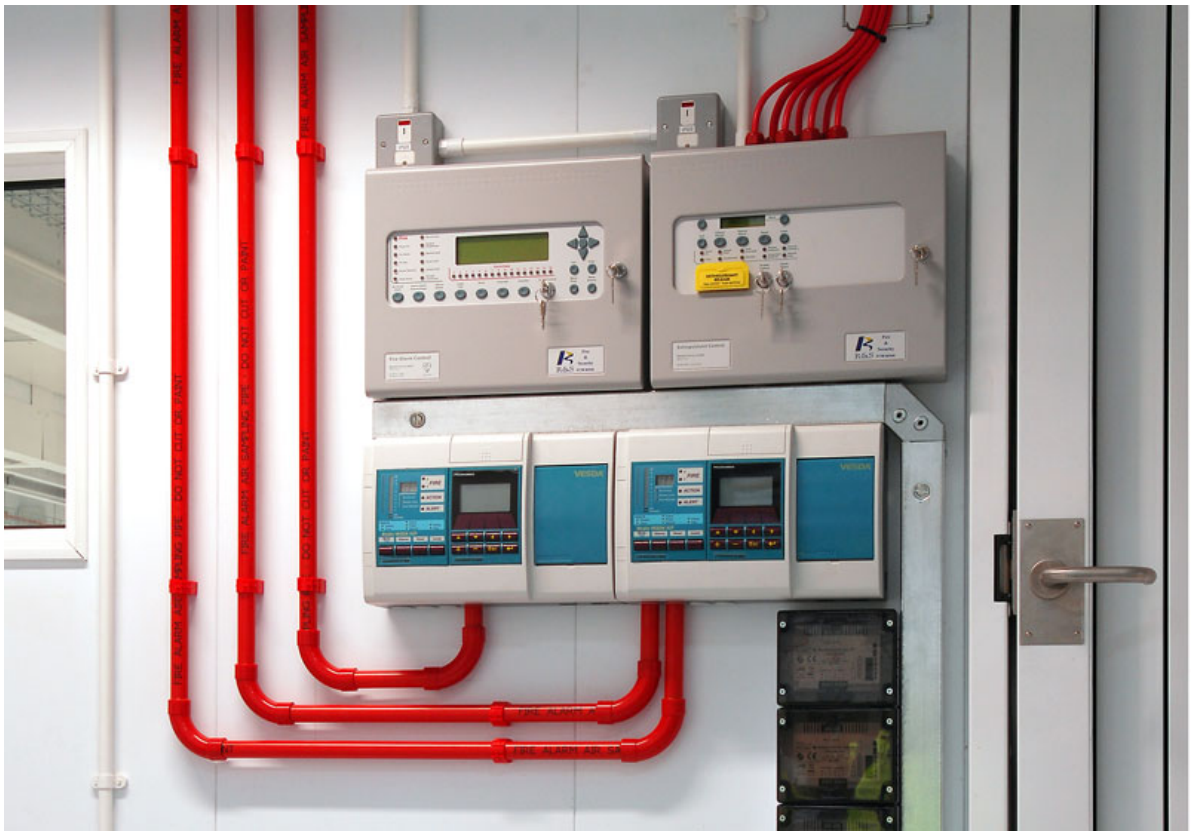
Nasávací kouřové hlásiče VESDA jsou jedny z nejcitlivějších kouřových hlásičů, které jsou k dispozici. Včasné zjištění požáru znamená detekovat jej s vysokou citlivostí. Kouř v nízké koncentraci, kdy ještě není ve viditelné formě, je příznakem vznikajícího požáru. Pro takovou detekci se používají vysoce citlivé kouřové nasávací hlásiče VESDA. Časový interval mezi okamžikem vzniku požáru a jeho rozšířením je důležitým pro význam rozsahu následků. Čím dříve je požár detekován, tím více času zbývá na evakuaci osob, potlačení požáru a tím jsou vzniklé škody menší. Hlásiče VESDA jsou aktivními detektory kouře. Vestavěné nasávací zařízení nasává sítí trubek vzorky vzduchu ze střežených prostor a poté je přivádí k laserovému detektoru v hlásiči. Síť nasávacího potrubí se skládá z 1 až 4 trubek. Každá z těchto trubek může mít množství nasávacích otvorů. Každý nasávací otvor je rovnoměrný s bodovým kouřovým hlásičem ve znění normy EN 54-7. Kouřové nasávací hlásiče VESDA je možno spojovat do sítě RS485 a všechny typy mají reléové výstupy pro jednodušší připojení k EPS. Kouřové nasávací hlásiče VESDA obsahují funkci "Autolearn", která po zkušebním provozu nastaví na optimálně rozhodovací úrovně v daném prostředí.

Hlásiče využívají principu rozptylu světelného paprsku. Vysokoenergetický laser generuje i při nízké koncentraci dostatečné množství rozptýleného světla, které je detekováno fotosenzory. Vestavěný filtr zachycuje prachové částice a propouští jen aerosoly kouře. Vysoká citlivosti laserové komory minimalizuje nebezpečí vyhlášení falešného poplachu.

Systém VESDA je zpravidla součástí systému elektrické požární signalizace. Způsob připojení na ústřednu EPS jsou k dispozici reléové kontakty s programovatelnými funkcemi. Hlásiče mohou být napájeny z ústředny EPS nebo ze samostatného zdroje. Signál na příslušný hasičský záchranný sbor musí být vyveden z ústředny EPS.

V návrhu jsem použil ústřednu ALGOPLUS 1 v základu je jednokruhovou ústřednou rozšiřitelnou na dvě kruhové linky pomocí dalšího modulu. Kapacita jedné kruhové linky je 126 adresovatelných prvků Apollo. Ústředna splňuje požadavky evropských norem EN54-2: 1997 a EN54-4: 1997. Ústředna je napájena ze sítě 230V 50Hz.Připojení ústředny

k napájecí síti nízkého napětí musí být v souladu s platnými normami. Instalovat ústřednu, otvírat její kryt a zasahovat do ní jsou oprávněny pouze osoby s kvalifikací dle §5 až §8 Vyhlášky č.50/1978 a je nutno dodržet ČSN EN 50110. [21]

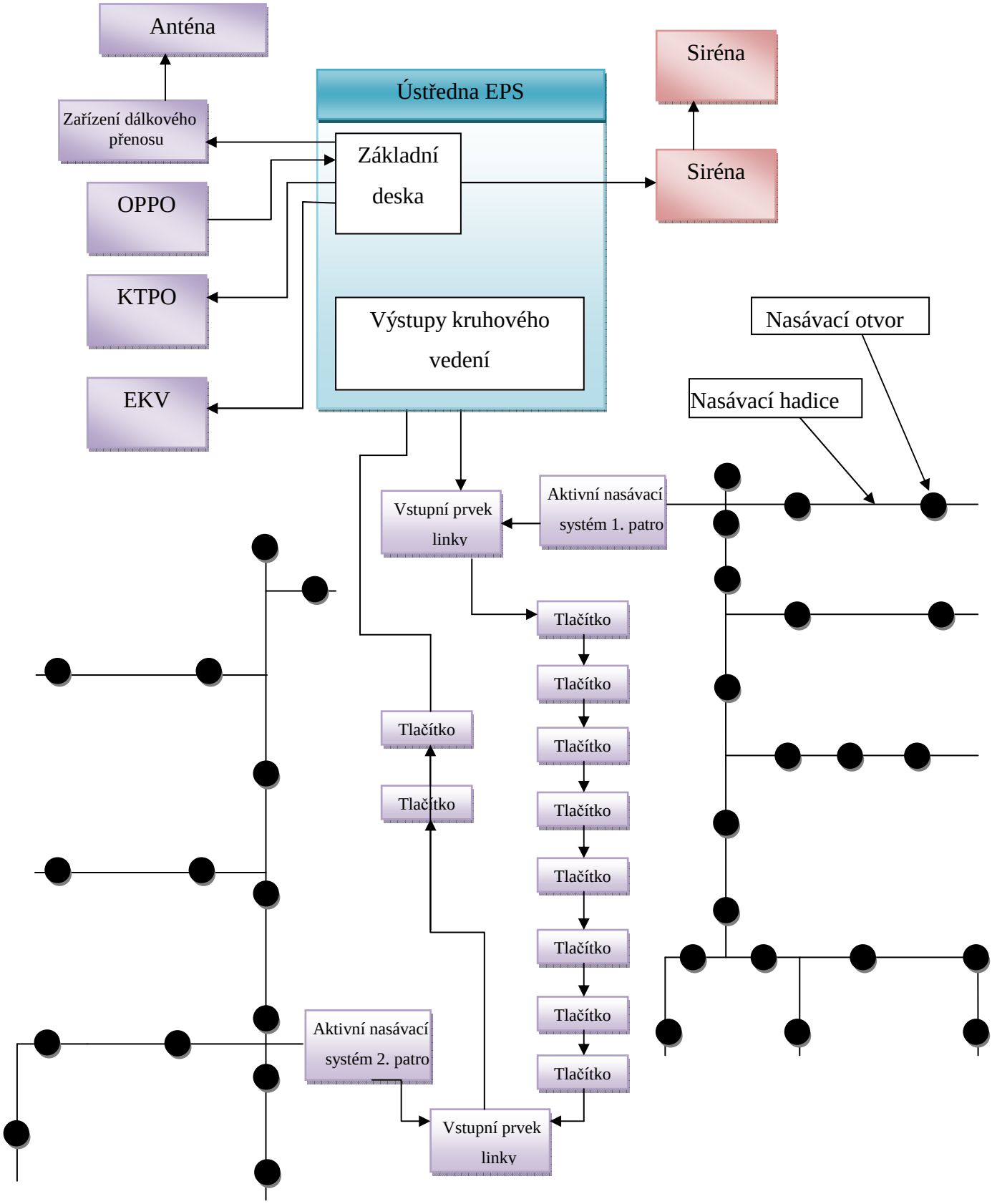


Obr. 13. Nasávací systém VESDA a ústředna EPS ALGOPLUS 1

K elektronické požární signalizaci patří ještě OPPO (obslužné pole požární ochrany). Zde je použito obslužné pole LITES MHY 912, je to prvek EPS pro systémy napojené prostřednictvím zařízení dálkového přenosu (ZDP) na útvary Hasičských záchranných sborů. OPPO je ocelová uzamykatelná krabice vyrobena pro montáž na zeď. V předním víku je průhled na ovládací a signalizační prvky. OPPO z hlediska uspořádání předního panelu, funkce i konstrukce odpovídá normě DIN 14661. [21]

Klíčový trezor požární ochrany KTPO slouží k úschově a ochraně klíče objektu, trezor je umístěný na přístupném místě. Klíče je uložen za dvěma dvířky a je elektronicky kontrolován. Při vyhlášení poplachu se vnější dvířka otevřou pomocí signálu z ústředny EPS, pro přístup zásahové jednotky hasičského záchranného sboru.

### 5.2.1 Blokové schéma návrhu EPS




Obr. 14. Blokové schéma návrhu EPS

### 5.2.2 Rozmístění prvků

Viz. příloha č. 2.

## 5.3 Kamerový systém CCTV

Kamerový záznam je důležitý k identifikaci osob pohybující se v objektu a jeho okolí. Kvalitní kamerový obraz je možno dosáhnout pomocí nové moderní technologie. Použil jsem síťové řešení Samsung iPolis. Samsung nabízí kompletní řešení IP kamerových systémů: síťová kamera, Kodér, NVR, klientský software, NVR hardware a NVR software (záznamový software). IPOLiS je založen na nejnovějších technologiích. V odvětví zabezpečování poskytuje uživatelům snadnou a jednoduchou správu a stabilní funkčnost. V návrhu jsem použil kamery Samsung Techwin Europe SNB-5000. Kamery budou umístěny tak, aby snímaly prostor v okolí budovy.

Popis kamery Samsung Techwin Europe SNB-5000:

IP kamera s rozlišením SXGA (1280x1024). Podpora rozlišení 16:9 HD. Kamera podporuje audio, záznam na SD kartu, redukci šumu, WDR (kompenzace protisvětla) a videoanalýzu Využívá Multi kodek H.264, MPEG-4, MJPEG. Možnost uchycení objektivu C/CS způsobem. Způsob napájení PoE 802.3af, 12VDC/24VAC-6W. Je vhodná do velmi náročných vnitřních i venkovních aplikací s důrazem na detail za všech podmínek. [17]


Obr. 15. Kamera Samsung Techwin Europe SNB-5000

Další kamera snímající prostor před budovou je PTZ IP kamera Samsung Techwin Europe SNP-3430HP. Venkovní kamera s 43x zoom objektivem, snímačem obrazu 1/4" PS CCD, celkový počet pixelu 795 x 596. Kamera podporuje audio, redukci šumu, WDR (kompenzace protisvětla), napájená (24 VAC) je pomocí Hi PoE. Využívá formát komprese videa H.264, MPEG-4, MJPEG. [17]


Obr. 16. PTZ kamera Samsung Techwin Europe SNP-3430HP

Prostor v bankovní hale snímají dvě kamery. První kamera bude nasměrována na hlavní vchod do bankovní haly, druhá kamera bude snímat dění v celém prostoru haly.

Kamera PiXORD PD 636E je IP kamera s rozlišením 2 MPix, obrazový senzor Color CMOS. Vybaven objektivem rybí oko, poskytuje náhled na celou místnost. Využívá formát kodeku H.264 / MJPEG, rozlišení UXGA 1600 x 1200. Kamera má napájení 12 VDC pomocí PoE. [22]

Obr. 17. Snímaná scéna s objektivem "rybí oko"


Obr. 18. Kamera PiXORD PD 636E

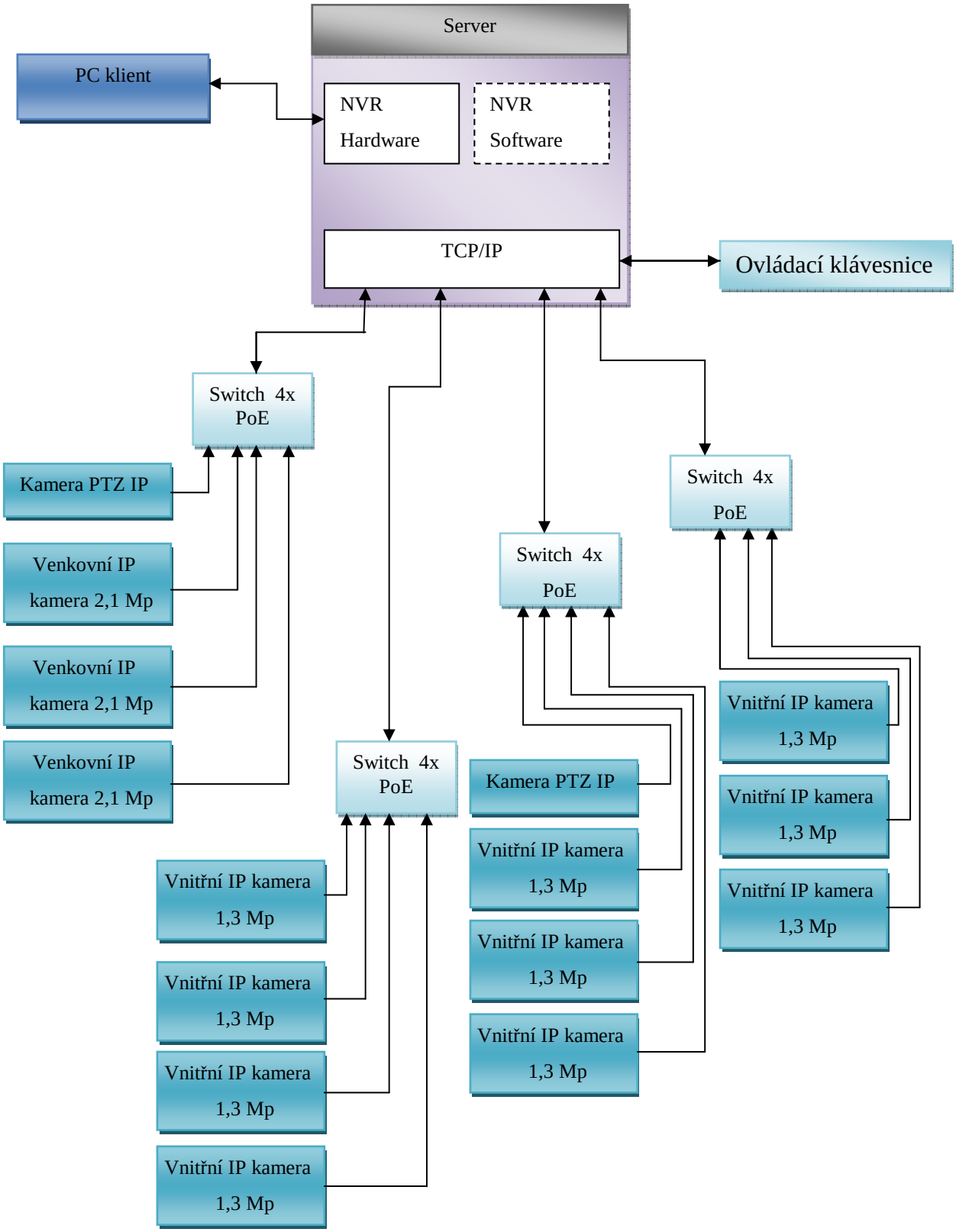
Všechny signály z IP kamer jsou zpracovány v síťovém záznamovém zařízení. Zde je použito 16ti kanálové záznamové zařízení Samsung SRN-1670D. Využívá vícečetné kodeky H.264 / MJPEG, umožňuje živé sledování v rozlišeni: VGA, 4CIF, 1,3M, 2M. Vysoké rozlišení obrazu 4CIF 480 snímků/s (NTSC), 400 snímků/s (PAL) v reálném čase. Operační systém umožní rychlost záznamu až 120 snímků/s při 1280 x 1024 (1,3 M). Sledování záznamu je prováděno buď pomocí softwaru Net-i viewer nebo webového prohlížeče. Všechny záznamy jsou ukládány na pevný disk, který je připojen přes rozhraní SATA. Propojení záznamového zařízení s monitorem je pomocí rozhraní HDMI s rozlišeni 720p / 1080 p (60Hz), nebo VGA analogovy s rozlišením 1280 x 1024 (60 Hz). Připojení k sítí ethernetu je pomocí konektoru RJ-45. [21]


Obr. 19. Záznamové zařízení Samsung SRN-1670D

Software centrální správy Net-i viewer podporuje tato zařízení síťovou kameru, enkodér, DVR, NVR. Živé sledováni až 16 kanálů současně na monitoru počítače. Ovládání PTZ kamer (posun, náklon, přiblíženi, zaostřeni, předvolba) je realizované pomocí softwaru a ovládací klávesnice systému. Systémové požadavky: procesor: Intel Core2Quad 2,5 GHz a vyšší, RAM: 3 GB a vice, paměť videa: 512 MB, HDD: 200 GB a vice, OS: Windows XP Professional, Windows 2000 Professional, Windows Vista Home Basic/Premium/Ultimate, Windows 7, DirectX 8.1 a vyšší. Rozlišeni zobrazeni: 1280 x 1024 a vyšší, kompatibilní s OpenGL. [21]

Obr. 20. Ovládací klávesnice

### 5.3.1 Blokové schéma návrhu CCTV




Obr. 21. Blokové schéma návrhu CCTV

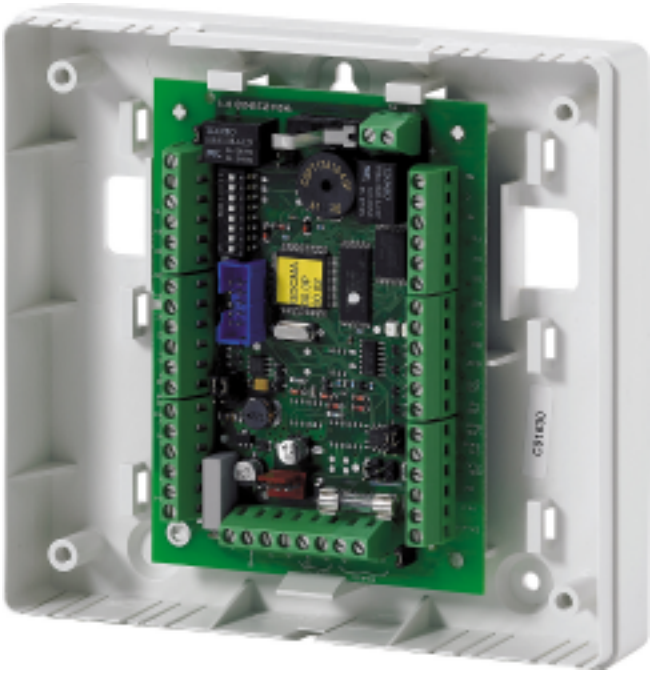
### 5.3.2 Rozmístění prvků

Viz. příloha č. 3.

## 5.4 Elektronická kontrola vstupu (EKV)

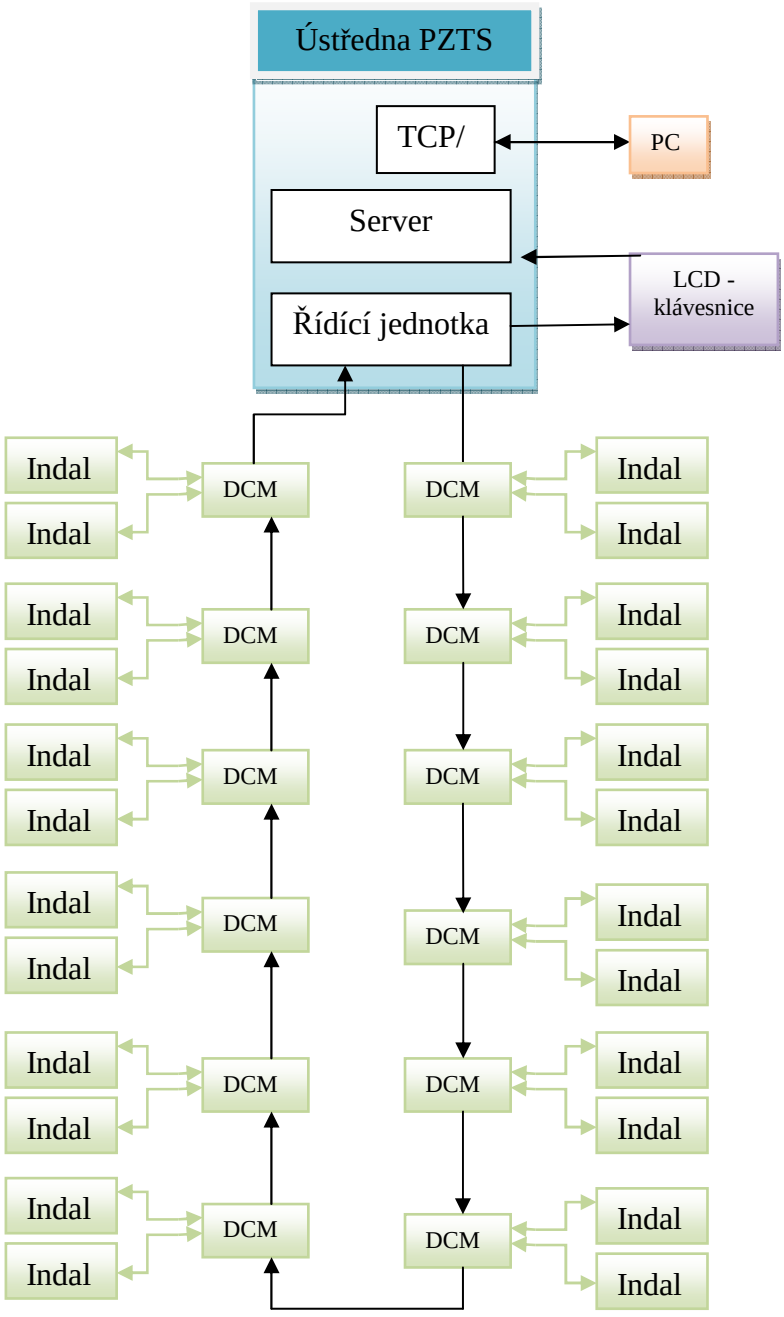
Kontrola vstupu je realizována integrací do zabezpečovací ústředny Galaxy Dimension, pomocí přídavných modulů. Velká dotyková klávesnice umožňuje přehledné prohlížení záznamu pohybu osob v objektu. Systém umožní ovládat až 32 dveří napojených na dveřní modul DCM, který umožňuje připojit dvě bezkontaktní čtečky. Oprávnění uživatelů v zabezpečení i kontrole vstupu definují grupy. Je-li oblast zastřežena, není možné dveře otevřít, pokud neproběhne odkódování. Tento princip předchází falešným poplachům.

Inovace se dočkal i program DSI Galaxy, který je určený pro konfiguraci ústředny a správu uživatelů. Vytvořili zcela nové uživatelské prostředí tak usnadňuje práci instalačním technikům, ale i správcům a uživatelům. [21]



Obr. 22. Dveřní modul DCM

### 5.4.1 Blokové schéma návrhu EKV




Obr. 23. Blokové schéma návrhu EKV

### 5.4.2 Rozmístění prvků

Viz. příloha č. 3.

# 6 FINANČNÍ HODNOCENÍ

V cenovém rozpočtu řeším dvě cenové nabídky. První je finanční zhodnocení navrhovaných systému v této práci. Druhou cenovou nabídku tvořím dle možnosti nabídky trhu v České republice.

## 6.1 Cenový rozpočet PZTS

V této kategorii jsem použil již dříve zmiňovanou ústřednu Galaxy Dimension, která bude porovnána s ústřednou Digiplex EVO 192. Rozdíl mezi těmito zabezpečovacími ústřednami je především v ceně a kvalitě. Obě tyto ústředny jsou dostupné na našem trhu.

Kvalitnější ústřednou je Galaxy Dimension s kombinací nové dotykové klávesnice, umožňující vynikající správu elektronické kontroly vstupu. Do budoucna tento systém lze rozšířit i o další moduly. Cenový rozdíl mezi systémy je zhruba 100 000 Kč. Do cenového rozpočtu není započtena montáž systému. Levnější systém Digiplex sice vyhovuje veškerým normám pro instalaci do 3. třídy zabezpečení, ale finančním institucím obvykle nezáleží na množství vynaložených peněžních prostředků. Prioritou je mít kvalitní systém, který je „ochrání“ před pachateli.

Tab. 2. Cenový rozpočet PZTS

| **Komponenty** | Počet kusů | Galaxy Dimension | Digiplex EVO 192 |
|---|---|---|---|
| Ústředna | 1 | 23 390,- | 7 329,- |
| Klávesnice | 3 | 31 860,- | 12 697,- |
| Magnetický kontakt | 62 | | 12 338,- |
| Detektor tříštění skla | 16 | 32 880,- | 11 184,- |
| Doplňkový zdroj | 7 | 16 500,- | 13 993,- |
| Pohybový detektor | 26 | 38 740,- | 36 374,- |
| Vibrační detektor | 17 | 52 530,- | 32 283,- |
| Tísňové tlačítko | 14 | 12 236,- | 10 066,- |
| Siréna | 1 | 1 690,- | 999,- |
| Detektor poslední bankovky | 7 | 5 103,- | 5 103,- |
| Tísňová lišta | 8 | 12 000,- | 12 000,- |
| Přístupový modul | 6 | 29 980,- | 15 648,- |
| Čtečka karet | 12 | 18 450,- | 9 588,- |
| GSM modul | 1 | 6 390,- | 5 299,- |
| Radiový vysílač | 1 | 15 000,- | 15 000,- |
| Signalizační tablo | 1 | 7 460,- | 6 500,- |
| Kabeláž + spojovací materiál | 600m | 7 000,- | 7 000,- |
| **Celkem** | | **311 209,-** | **213 401,-** |

## 6.2 Cenový rozpočet EPS

U elektronické požární signalizace jsem porovnal nasávací hlásič VESDA s hlásičem multisenzorovým. Ústředna v obou případech bude stejná. Nasávací hlásič vyhodnotí vznik požáru mnohem rychleji než klasické hlásiče požáru. V objektech banky je možnost instalovat i samočinné hasicí zařízení. Banka se nachází v blízkosti stanice hasičského záchranného sboru, na který je přiveden výstupní signál z vysílače. Cenové nabídky se od sebe příliš neliší. Dražší je nabídka s nasávacím detektorem, který je určitě účinnější k vyhlášení poplachu.

Tab. 3. Cenový rozpočet EPS

| **Komponenty** | Počet kusů | Algoplus 1 | Komponenty | Počet kusů | Algoplus 1 |
|---|---|---|---|---|---|
| Ústředna | 1 | 18 200,- | Ústředna | 1 | 18 200,- |
| Tl. hlásič XP95 | 10 | 45 990,- | Tl. hlásič XP95 | 10 | 45 990,- |
| Detektor VESDA | 1 | 65 771,- | Detektory multi. Senzor. | 19 | 26 581,- |
| OPPO | 1 | 5 999,- | OPPO | 1 | 5 999,- |
| Siréna | 1 | 6 450,- | Siréna | 1 | 6 450,- |
| Klíčový trezor | 1 | 18 990,- | Klíčový trezor | 1 | 18 990,- |
| Zdroj 24V | 3 | 16 580,- | Zdroj 24V | 4 | 22 120,- |
| Spojovací materiál | 150m | 3 000,- | Spojovací materiál | 800m | 20 000,- |
| **Celkem** | | **180 980,-** | **Celkem** | | **164 330,-** |

## 6.3 Cenový rozpočet CCTV

Použitý kamerový systém využívající IP technologii, porovnám s analogovým kamerovým systémem. U finančních institucí je zapotřebí identifikovat osoby pohybující se v objektu. Zvolené IP kamery vyhovují podmínkám, které k identifikaci potřebujeme. Při propojení analogových kamer pracujeme s koaxiálním kabelem, s kterým táhneme i současně napájecí kabel. U IP kamer natahujeme jen UTP kabel šesti žilový, po kterém vedeme obrazový záznam v digitální podobě, ale také napájení do kamery. Cenově se obě nabídky liší zhruba o 100 000Kč. S ohledem na kvalitní monitorování prostorů je táto investice vyhovující.

Tab. 4. Cenový rozpočet na kamerový systém

| **Komponenty** | Počet kusů | IP kamery | Analog. Kamery |
|---|---|---|---|
| Záznamová zařízení | 1 | 65 990,- | 72 990,- |
| **Kamery** | | | |
| SNB-5000 | 10 | 115 900,- | - |
| SNP-3430HP | 1 | 44 990,- | - |
| PiXORD PD 636E | 1 | 16 990,- | - |
| Licence SNS-SF016 | 1 | 22 990,- | - |
| switch 4x PoE | 6 | 98 990,- | - |
| SCP-3120VHP | 1 | - | 20 990,- |
| SCO-2120RP | 3 | - | 38 990,- |
| SCZ-3430P | 1 | - | 23 890,- |
| SCP-3120VP | 1 | - | 19 990,- |
| SCB-3001P | 3 | - | 24 550,- |
| SCB-4000 PH | 5 | - | 42 950,- |
| Zdroj PTZ | 2 | - | 9 890,- |
| 24nZ4 | 4 | - | 18 890,- |
| Ovládací klávesnice | | 25 990,- | 8 990,- |
| kabeláž + spoj. Materiál | 600m | 8 000,- | 12 000,- |
| **Celkem** | | **399 840,-** | **294 120,-** |

# ZÁVĚR

Cílem této bakalářské práce je analyzovat a zhodnotit bezpečnostní rizika zabezpečení finančních institucí. Většina pachatelů orientovaných na loupežné přepadení finančních institucí jsou amatéři a neberou ohled na to, že je v objektu instalovaný bezpečnostní systém. Když pachatel potřebuje peněžní hotovost, tak si pro ni kolikrát bez rozmyslu dojde a finanční instituce se brání pouze časovým zámkem na trezoru. Časová prodleva musí být delší než příjezd zásahové skupiny. Tato časová prodleva většinou pachatelům nesedí do plánu přepadení a díky tomu může stoupat agresivní chování pachatele vůči zaměstnancům a zákazníkům banky. Ze zahraničních zkušeností vyplývá, že účinným způsobem je zřízení bezpečnostní kabiny se systémem komorového vstupu, který zabraňuje náhlým vpádům ozbrojených skupin nebo jednotlivců.

Kombinaci kvalitního bezpečnostního systému s touto bezpečnostní kabinou tvoří zabezpečení finanční instituce na vyšším stupni cenového rozpočtu, ale také jej můžeme zařadit mezi úspěšné systémy v boji s pachateli.

V této práci jsem navrhl dvě cenové varianty pro zabezpečení finančních institucí. Cena těchto variant se liší zhruba o 200 000 Kč. Jelikož veškeré finanční instituce spadají do 3. třídy zabezpečení, proto bych doporučil variantu cenově dražší a to z toho důvodu, že velké obnosy peněz lákají větší množství pachatelů. Především moderní technologie kamerového systému nám umožní monitorovat a zaznamenat data, potřebné pro identifikaci znaků pachatele. Díky těmto záznamům se usnadní práce pro vyšetřovatelé této trestné činnosti a stoupne objasnění těchto případů.

Celkově lze do budoucna předpokládat změny operandi pachatelů a to především nárůst agresivity, vzetí rukojmích a ostatních násilných jednání. Proto bych finančním institucím doporučil modernizovat a rozvíjet svůj bezpečnostní systém, protože na prvním místě je bezpečnost zaměstnanců, zákazníků a nakonec i uložených peněžních hotovostí.

# ZÁVĚR V ANGLIČTINĚ

The objective of this bachelor thesis is analyze and rate security risk security financial institution.

The most of attackers focused on robbery assault financial institutions are amateurs and they don't give respect that object has installed security system. When attacker need the cash, attacker go without thinking and financial instituion defend against only with the time lock on the safe. Time delay must be longer than arrive of security service. This time delay mostly attackers not fit to the plan of attack and attackers use agresive behavior to the employees and customers of bank.

From abroad experiences is reasonable that effectively way establishment of a security cabin ventricular system input, which prevents sudden invasions of armed groups or individuals.

The combination of high quality security system that consists of a safety cab securing financial institution at a higher price level of the budget, but it can also include the successful systems in the fight against offenders.

In my bachelor thesis I suggest two price variants for security financial institutions. Price for these variants are different about 200 000 Kč. As all financial institutions are covered by 3 security class, that's why I would recommend the option price expensive. Above all, modern technology, the camera system will enable us to monitor and record the data necessary to identify the characteristics of the offender. Thanks to these records will facilitate the work of the investigators of this crime will rise and shed light on these cases. Overall changes in future assume operandi of offenders primarily increase aggression, hostage taking and other violent actions. This is the reason, why I would recommend financial institutions to modernize and develop its security system, because at first the safety of employees, customers and ultimately of cash deposited.

# SEZNAM POUŽITÉ LITERATURY

[ 1 ] BRABEC, František. Ochrana bezpečnosti podniku. : EUROUNION, 1996. 368 s. ISBN 80-85858-29-0.

[ 2 ] PROTIVINSKÝ, Miroslav,et al. Bankovní loupeže. Praha: Armex, 2001. 279 s. ISBN 80-86244-21-0.

[ 3 ] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Zlín: UTB, 2004. 122 s. ISBN 80-7318-231-9.

[ 4 ] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Zlín: UTB, 2003. 64 s. ISBN 80-7318-119-3.

[ 5 ] *Trezortest.cz* [online]. 2004 [cit. 2011-05-22]. Seznam certifikovaných výrobků. Dostupné z WWW: <http://www.trezortest.cz/seznam-certifikovanych-vyrobku/>.

[ 6 ] *Delnet - Elektroinstalace a slaboproudé systémy* [online]. 1998 [cit. 2011-05-22]. Dostupné z WWW: <http://www.delnet.cz/slaboproude-systemy/elektronicka-zabezpecovaci-signalizace-ezs.html>.

[ 7 ] *Trade FIDES, a. s.* [online]. 1995 [cit. 2011-05-22]. Dostupné z WWW: <http://www.fides.cz/cs/>

[ 8 ] Katalogové listy a informační materiály firmy- Variant, Dostupné na WWW: < http://www.variant.cz

[ 9 ] ŠEJNOHA, Jiří. *Http://www.ijs-security.cz* [online]. 2003 [cit. 2011-05-22]. Průvodce integrovanými bezpečnostními systémy. Dostupné z WWW: <http://www.ijs-security.cz/text/903PIBS.pdf>.

[ 10 ] *Http://www.cctv-prodejce.cz* [online]. 2010 [cit. 2011-05-22]. Jak vybrat CCTV kameru. Dostupné z WWW: <http://www.cctv-prodejce.cz/technicka-podpora/rady-informace/jak-vybrat-kameru>.

[ 11 ] *Nahledy.normy.biz* [online]. 2007 [cit. 2011-05-22]. ČESKÁ TECHNICKÁ NORMA. Dostupné z WWW: <http://nahledy.normy.biz/nahled.php?i=78248>.

[ 12 ] Katalogové listy a informační materiály firmy- ADI Global Distributions, Dostupné na WWW: < http://www.adiglobal.cz

[ 13 ] ČSN EN 50132. Poplachové systémy: CCTV sledovací systémy pro použití v bezpečnostních aplikacích: ČNI, 1999.

[ 14 ] *Http://www.sovte.cz/* [online]. 2010 [cit. 2011-05-22]. Elektronické kontrola vstupu a docházky. Dostupné z WWW: <http://www.sovte.cz/systemy/ekv.php>.

[ 15 ] *Http://shop.normy.biz* [online]. 2009 [cit. 2011-05-22]. ČESKÁ TECHNICKÁ NORMA. Dostupné z WWW: http://shop.normy.biz/d.php?k=84164.

[ 16 ] ČR. Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. Sbírka zákonů, Česká republika. 2000.

[ 17 ] Firemní materiály: Bosch, Honeywell, Siemens, Paradox.

[ 18 ] Studijní materiály z průběhu studia.

[ 19 ] *Http://www.lites.cz* [online]. 2001 [cit. 2011-05-22]. Projektování EPS. Dostupné z WWW: <http://www.lites.cz/tp/Pokyny_pro_projektovani.pdf>.

[ 20 ] *Http://www.radiostanice-vysilacky.cz* [online]. 2010 [cit. 2011-05-22]. Zabezpečovací ústředny Galaxy Dimension. Dostupné z WWW: <http://www.radiostanice-vysilacky.cz/zabezpeceni/galaxy-dimension/>.

[ 21 ] *Tyco FIS &* [online]. 2009 [cit. 2011-05-22]. Dostupné z WWW: <http://www.tycofis.cz/central-tech-info/VESDA>.

[ 22 ] *Http://www.t-cz.com* [online]. 2011 [cit. 2011-05-22]. PIXORD PD636E (2MP, H.264, rybí oko). Dostupné z WWW: <http://www.t-cz.com/panorama-ip-kamera-pixord-pd636e-2mp-h-264-rybi-oko-_d8643.html>.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

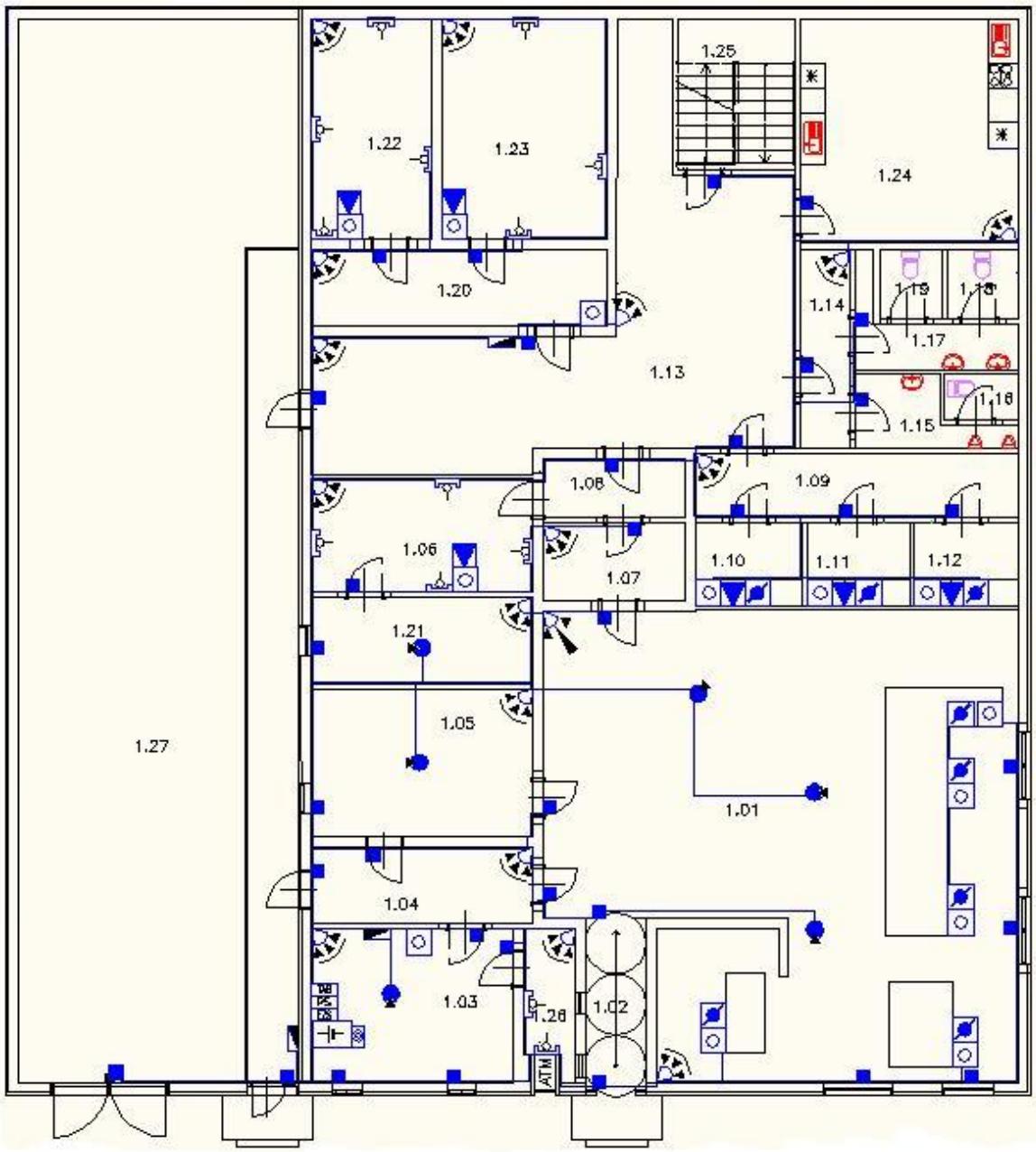
| | |
|---|---|
| PZTS | Poplachové zabezpečovací a tísňové systémy |
| CCTV | Uzavřený televizní okruh. |
| EPS | Elektronická požární signalizace. |
| EKV | Elektronická kontrola vstupu. |
| I&HAS | Poplachový systém pro detekci vniknutí a přepadení. |
| IAS | Poplachový systém pro detekci vniknutí. |
| HAS | Poplachový systém pro detekci přepadení. |
| PCO | Pult centralizované ochrany. |
| MZS | Mechanické zábranné systémy. |
| KTPO | Klíčový trezor požární ochrany |
| IP | Internet protokol |
| NVR | Network video recorder |
| PTZ | Otočné kamery |
| PoE | Power over Ethernet |
| MPix | Megapixel |

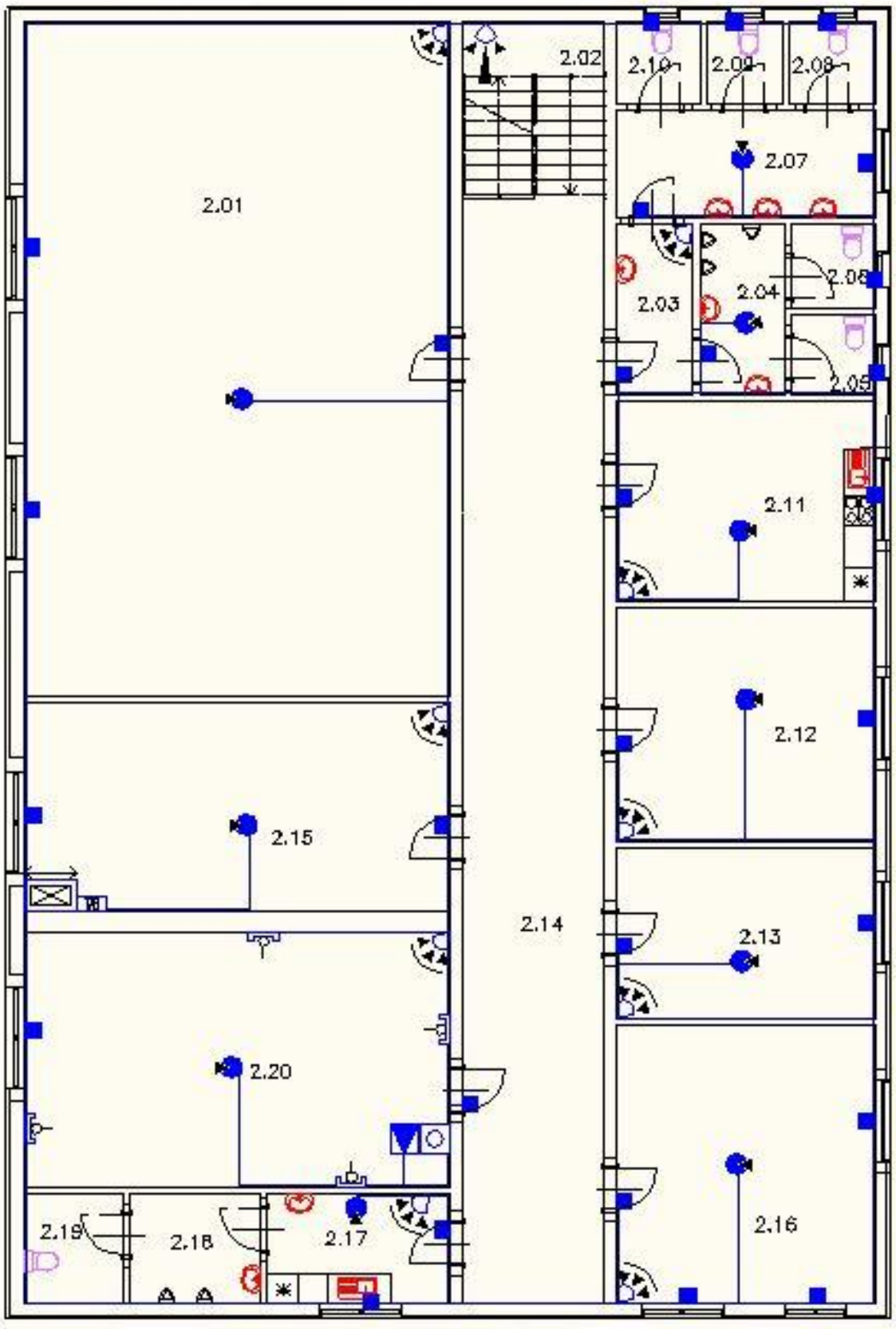
# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

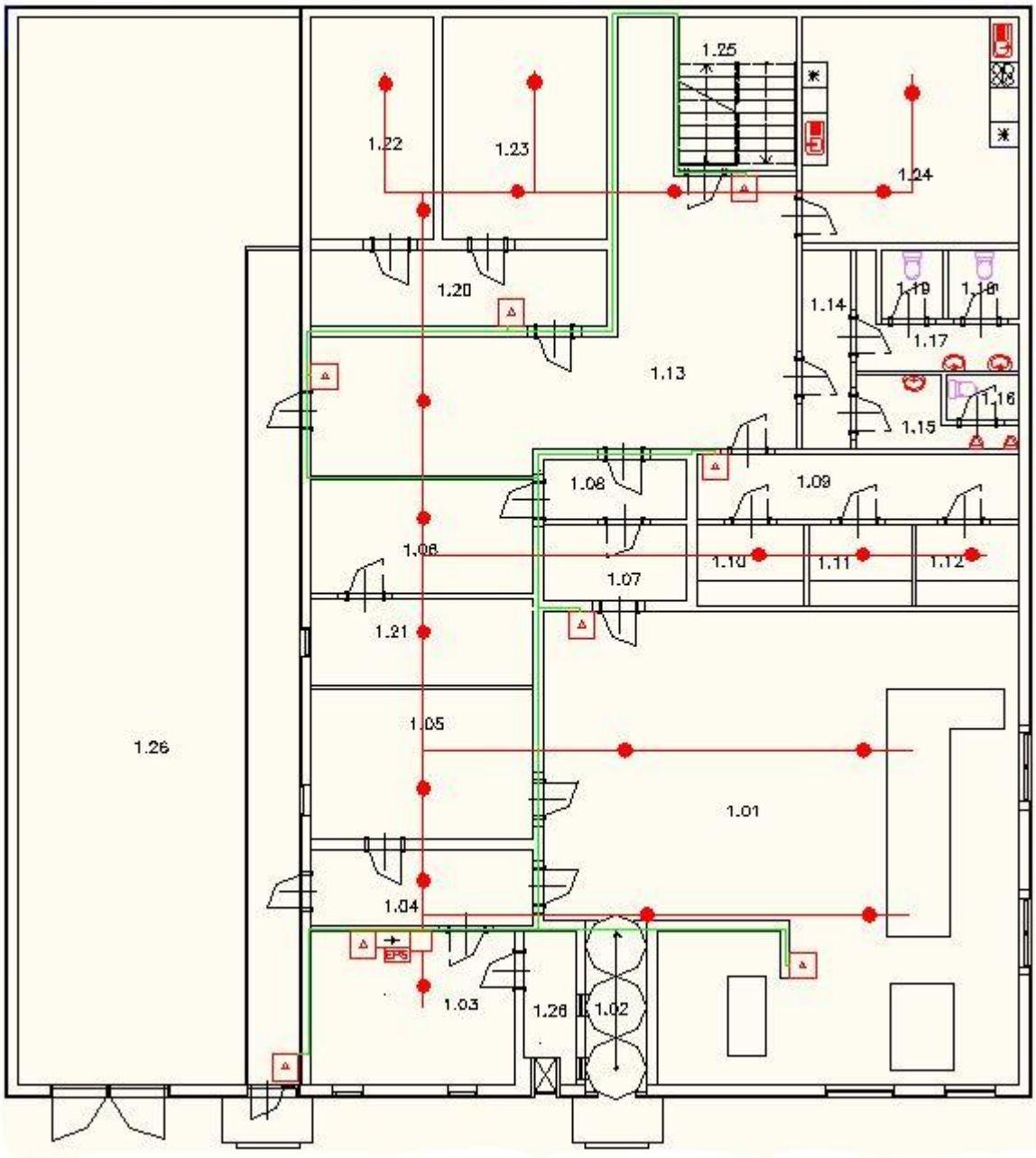
# SEZNAM PŘÍLOH

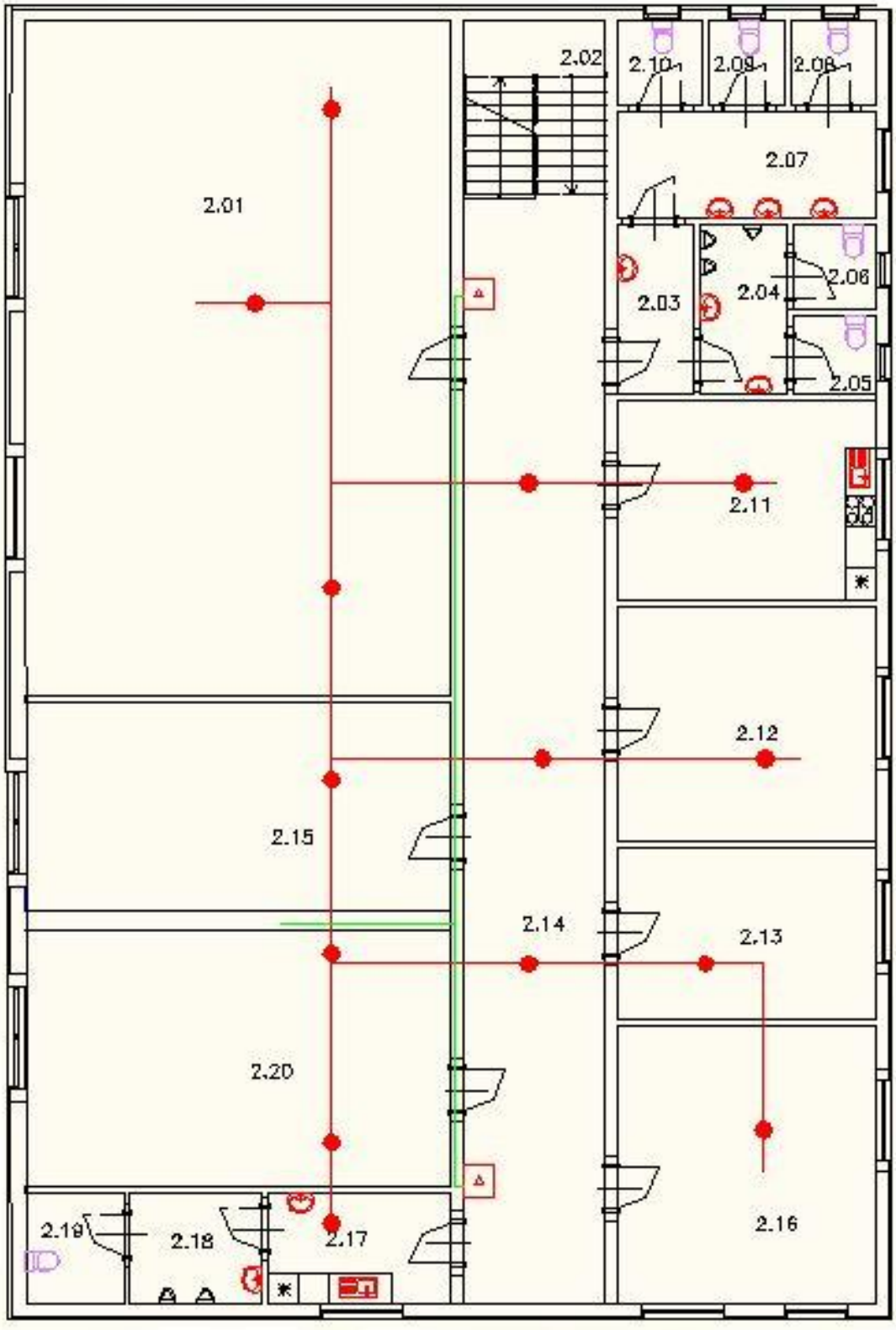
# PŘÍLOHA P I: NÁVRH ROZMÍSTĚNÍ PRVKŮ PZTS



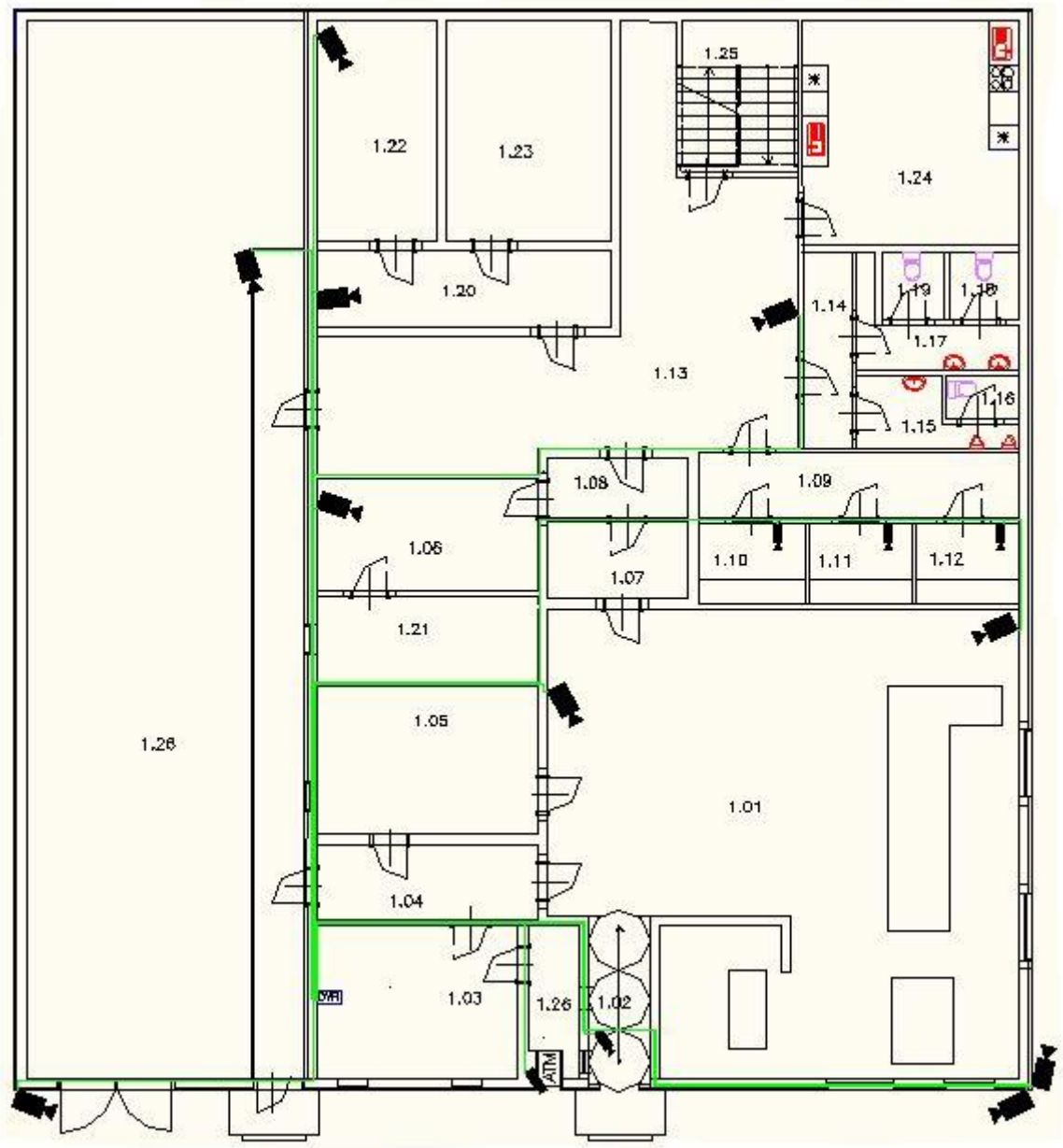

2.01
2.02
2.10
2.09
2.08
2.07
2.03
2.04
2.06
2.05
2.11
2.12
2.15
2.14
2.13
2.20
2.19
2.18
2.17
2.16

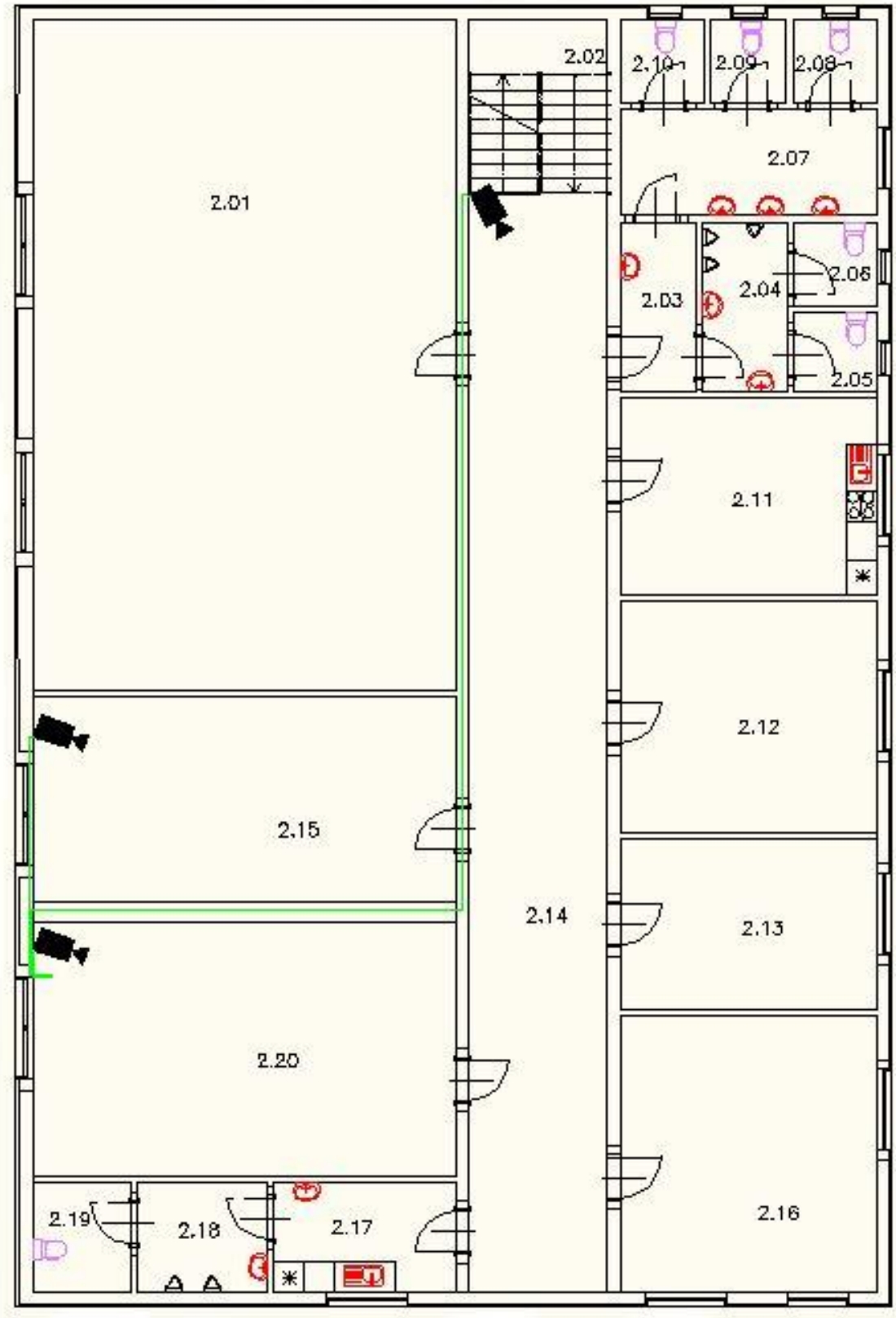
# PŘÍLOHA P II: NÁVRH ROZMÍSTĚNÍ PRVKŮ EPS



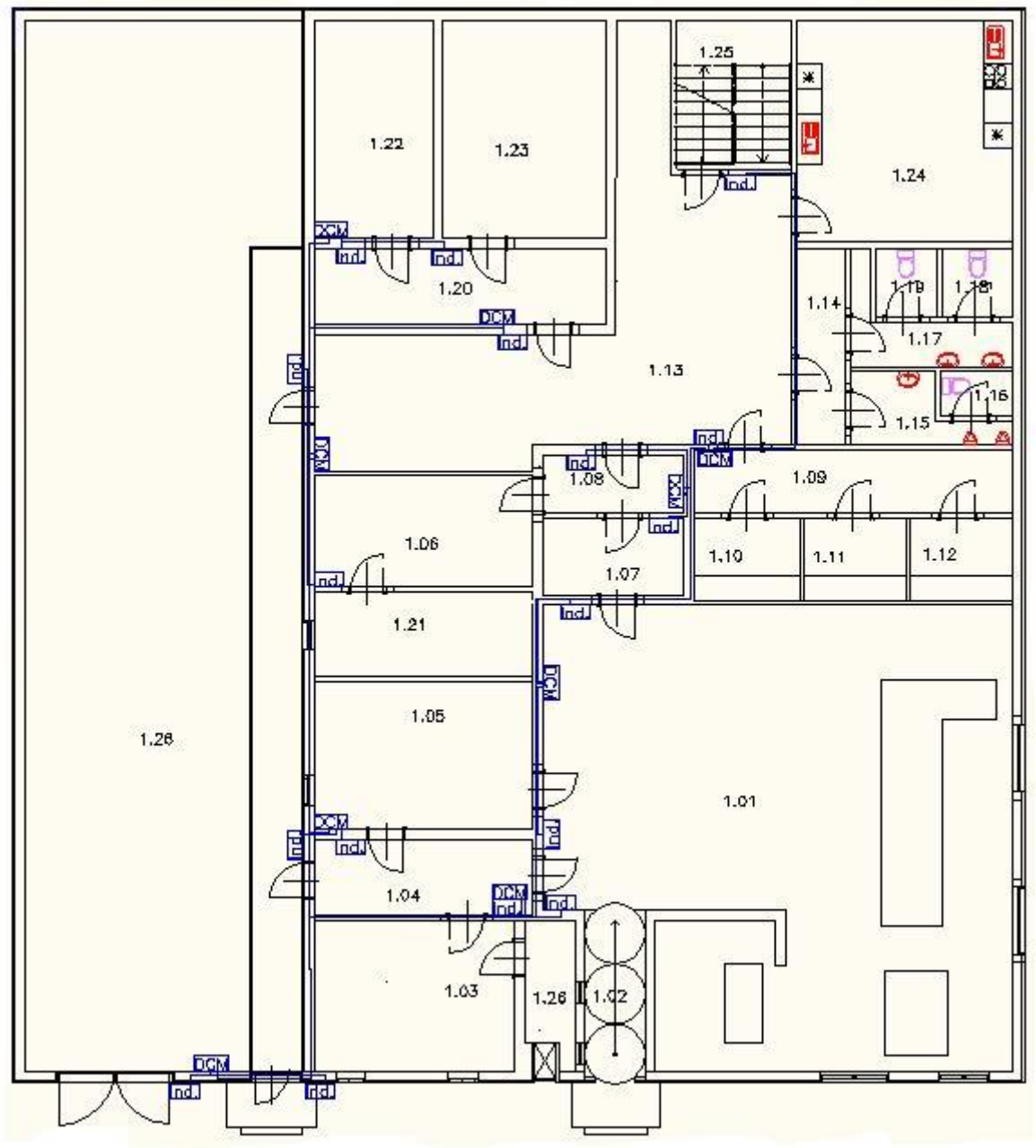

2.01
2.02
2.10
2.09
2.08
2.07
2.03
2.04
2.06
2.05
2.11
2.12
2.15
2.14
2.13
2.20
2.19
2.18
2.17
2.16

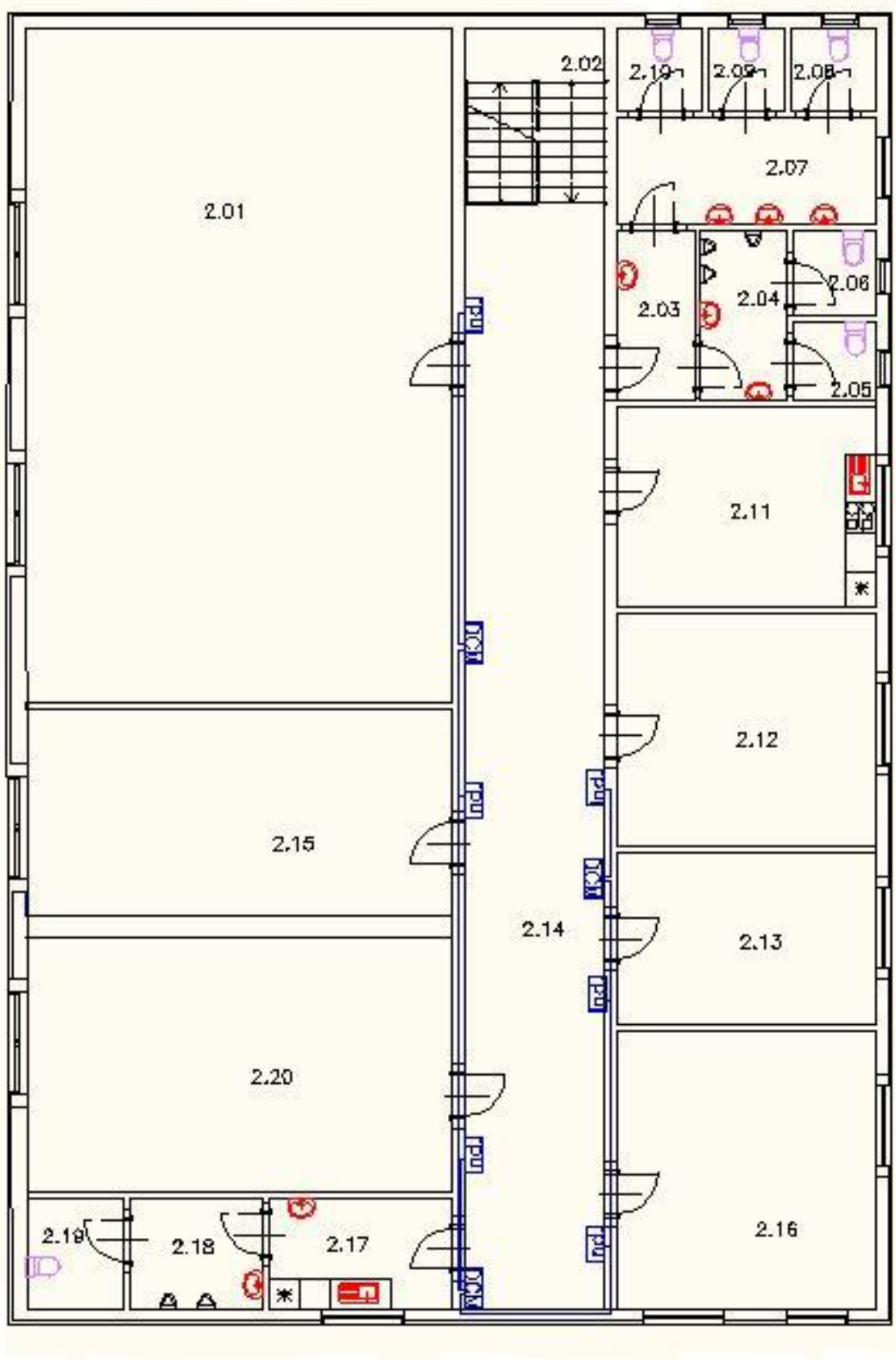
# PŘÍLOHA P III: NÁVRH ROZMÍSTĚNÍ PRVKŮ CCTV




2.01
2.02
2.10
2.09
2.08
2.07
2.03
2.04
2.06
2.05
2.11
2.12
2.15
2.14
2.13
2.20
2.19
2.18
2.17
2.16

# PŘÍLOHA P IV: NÁVRH ROZMÍSTĚNÍ PRVKŮ EKV




2.01
2.02
2.10
2.09
2.08
2.07
2.03
2.04
2.06
2.05
2.11
2.12
2.15
2.14
2.13
2.20
2.19
2.18
2.17
2.16

# PŘÍLOHA P V: SCHÉMATICKÉ ZNAČKY

| Značka | Blok | Zkratka | Popis |
|---|---|---|---|
| | U011 | MS | Magnetické čidlo otevření |
| | U012 | MST | Magnetické čidlo otevření odolné ("těžké") |
| | U013 | DTS | Čidlo rozbití skla (detektor tříštění skla) |
| | U137 | DTS AM | Čidlo rozbití skla antimask (detektor tříštění skla antimasking) |
| | U014 | PI | Čidlo kontaktní PIEZO |
| | U015 | PIR | PIR vější |
| | U133 | PIR V | PIR vější venkovní |
| | U016 | PIR AM | PIR vější antimasking |
| | U152 | PIR D | PIR dlouhý dosah |
| | U018 | PIR Z | PIR záclona |
| | U019 | PIR ZAN | PIR záclona antimasking |
| | U139 | PIR ID | (PIR) čidlo s vlastní adresou |
| | U118 | UZ | Ultrazvuková čidlo |
| | U017 | PIR DV | PIR záclona dveřní |

| Značka | Blok | Zkratka | Popis |
|---|---|---|---|
| | U011 | PIR S | PIR stropní čidlo |
| | U011 | PIR/DTSS | PIR stropní kombinovaný s DTS |
| | U012 | IZ | IR infrazávora |
| | U125 | IZV | IR infrazávora – vysílač |
| | U124 | IZP | IR infrazávora – přijímač |
| | U013 | MV nebo MW | Mikrovlnné čidlo |
| | U014 | PIR/MW | Duální (PIR a MW) čidlo |
| | U126 | PIR/MWS | Duální (PIR a MW) stropní čidlo |
| | U015 | VIB | Otřesové (vibrační) čidlo |
| | U019 | MC | Čidlo poslední bankovky (peněžní svorka – Money Clip) |
| | U016 | TH | Tísňový hlásič tlačítkový |
| | U017 | TL | Tísňový hlásič lišta |
| | U134 | TC | Technologický hlásič |
| | U117 | GH | Hlásič úniku plynu ("GAS") |

| Značka | Blok | Zkratka | Popis |
|---|---|---|---|
|  | VB19 | PH | Hlásič požáru (použitý v systému EZS, jinak má samostatnou značku) |
|  | VB20 | SG | Signalizace optická |
|  | VB21 | IZ | Signalizace akustická a optická |
|  | VB22 | SI | Siréna vnitřní s blikačem (výstražné zařízení) |
|  | VB23 | SS | Siréna vnitřní (výstražná akustická zařízení) |
|  | VB24 | SE | Siréna vnější s blikačem (výstražné zařízení) |
|  | VB25 | SB | Siréna vnější bez blikače (výstražné akustická zařízení) |
|  | VB26 | NJ | Najíž (výstražná optická zařízení) |
|  | VB29 | US | Ústředna EZS |
|  | VB41 | PS | Napájecí zdroj (Power Source) |
|  | VB31 | EXP | Expandér, linkový modul, koncentrátor |
|  | VB38 | TAB | Tablo EZS |
|  | VB28 | ATS | Přenosová zařízení - komunikátor |
|  | VB51 | TR | Trafo TR 230 / 16 V |

| Značka | Blok | Zkratka | Popis |
|---|---|---|---|
|  | VB41 | Z | Modul zdroje PS ("Power Source") |
|  | VB33 | AKU | Záložní akumulátor |
|  | VB35 | WLV | Bezdrátový (wireless) vysílač |
|  | VB36 | WLP | Bezdrátový (wireless) přijímač |
|  | VB28 | KS | Klíčový spínač |
|  | VB27 | ZE | Propouštěcí (entry) zámek |
|  | VB32 | KL | Ovládací klávesnice (ovladač EZS) |
|  | VB37 | PCO | Pult centrální ochrany (poplachová přijímací centrum) |
|  | VB29 | VVN | Vstupně-výstupní modul (in / out) |
|  | VB42 | REL | Reléový modul |
|  | | | Dveřní modul DOM |
|  | VB18 | TH-WP | Tísňový hlásič bezdrátový (wireless) - přijímač |
|  | VB27 | TH-WV | Tísňový hlásič bezdrátový (wireless) - vysílač |
|  | | | Bezkontaktní čtečka (indoor) |

# PŘÍLOHA P VI: SEZNAM MÍSTNOSTÍ

| | | | |
|---|---|---|---|
| 1.03 | Místnost ostrahy | 2.03 | Předsíň WC |
| 1.04 | Úklidová místost | 2.04 | WC muži předsíň |
| 1.05 | Šatna | 2.05 | WC muži |
| 1.06 | Pokladna | 2.06 | WC muži |
| 1.07 | Předsíň | 2.07 | WC ženy předsíň |
| 1.08 | Předsíň | 2.08 | WC ženy |
| 1.09 | Chodba | 2.09 | WC ženy |
| 1.10 | Bankoní přepážka 1 | 2.10 | WC ženy |
| 1.11 | Bankoní přepážka 2 | 2.11 | Kuchyňka |
| 1.12 | Bankoní přepážka 3 | 2.12 | Kancelář 1 |
| 1.13 | Chodba | 2.13 | Kancelář 2 |
| 1.14 | Předsíň WC | 2.14 | Chodba |
| 1.15 | WC muži předsíň | 2.15 | Rozvodna/server |
| 1.16 | WC muži | 2.16 | Vedoucí manager |
| 1.17 | WC ženy předsíň | 2.17 | Kuchyňka |
| 1.18 | WC ženy | 2.18 | Předsíň WC |
| 1.19 | WC ženy | 2.19 | WC |
| 1.20 | Předsíň komorového trezoru | 2.20 | Archiv |
| 1.21 | Počtárna | | |
| 1.22 | Počtárna mincí | | |
| 1.23 | Komorový trezor | | |
| 1.24 | Kuchyňka | | |
| 1.25 | Schodiště | | |
| 1.26 | Místnost pro bankomat | | |