# Návrh a realizácia zabezpečenia business centra

Bc. Patrik Ostrovský

Diplomová práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Patrik OSTROVSKÝ** |
| Osobní číslo: | **A12322** |
| Studijní program: | **N3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Forma studia: | **prezenční** |
| Téma práce: | **Návrh a realizace zabezpečení business centra** |
| Téma anglicky: | **The Design and Implementation of a Security System for a Business Center** |

Zásady pro vypracování:

1. **Analyzujte současný stav business centra a popište jeho stávající komplexní ochranu.**
2. **Navrhněte a realizujte poplachové zabezpečovací a tísňové systémy ? PZTS s možností využití pro jednotlivé kanceláře business centra.**
3. **Navrhněte a dle možností realizujte kamerový a přístupový systém s využitím biometrických prvků.**
4. **Popište vzájemné propojení a komunikaci výše uvedených systémů s ohledem na jejich obsluhu.**
5. **Zhodnoťte Vámi navržený systém jako celek a navrhněte jeho další případné vylepšení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:


1. **LUKÁŠ, Luděk. Bezpečnostní technologie systémy a management III.: Teorie a praxe ochrany majetku a fyzické bezpečnosti. Zlín: Radim Bučuvčík – VeRBuM, 2013. ISBN 978-80-87500-35-4.**
2. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. [S.l.: s.n.], 2003, 351 s. ISBN 80-902-9382-4.**
3. **KINDL, Jiří. Projektování bezpečnostních systémů I. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.**
4. **IVANKA, Ján. Systemizace bezpečnostního průmyslu [online]. 4. rozš. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011 [cit. 2012-02-01]. ISBN 978-80-7454-122-3. Dostupné z: https://web.fai.utb.cz/cs/docs/Skripta_Ivanka_SBP.pdf.**
5. **BIGELOW, Stephen J. Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.**
6. **VALOUCH, Jan. Projektování integrovaných systémů [online]. 2013 [cit. 2014-02-05]. ISBN 978-80-7454-296-1. Dostupné z: http://dspace.k.utb.cz/bitstream/handle/10563/25814/Skripta%20-%20Valouch.pdf?sequence=1.**
7. **ČANDÍK, Marek. Objektová bezpečnost II. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2004, 100 s. ISBN 8073182173.**
8. **UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Policejní akademie české republiky, 2005, 229 s. ISBN 80-7251-189-0.**


Vedoucí diplomové práce: **Ing. Petr Skočík**
Ústav elektroniky a měření

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

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

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

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

## ABSTRAKT

Témou diplomovej práce je návrh a realizácia zabezpečenia business centra. Zaoberá sa analýzou súčasného stavu business centra a popisuje jeho komplexnú ochranu. Teoretická časť práce obsahuje bližšie určenie prvkov poplachového zabezpečovacieho a tiesňového systému ďalej len PZTS, prístupového a kamerového systému a poukazuje na názorné príklady uvedené k nim. Praktická časť sa venuje návrhom a realizácií PZTS, prístupového a kamerového systému. Taktiež sa zaoberá programovaním týchto systémov a prepojenie medzi nimi. Ďalej sa práca sústreďuje na návrh vylepšenia systémov a lepšiu integráciu.


Kľúčové slová: poplachový zabezpečovací a tísňový systém, prístupový systém, kamerový systém


## ABSTRACT

The theme of the thesis is the design and implementation of business Security Center. An analysis of the current state of the business center and describes how it deals with its comprehensive protection. The theoretical part of the work includes the determination of the elements of the security and emergency alarm system closer to the access and CCTV, and shows the PZTS illustrative examples to them. The practical part is dedicated to the design and implementation of access and CCTV, PZTS. It also deals with the programming of these systems and the link between them. Further, the work focuses on the design of improvements to the systems and better integration.


Keywords: Intrusion and hold system, access control system, CCTV system

Poďakovanie

Týmto by som sa chcel poďakovať vedúcemu mojej diplomovej práce Ing. Petrovi Skočíkovi za poskytnutie odborných rád a odporúčaní. Súčasne vyjadrujem poďakovanie firme TECHNIK Security spol. s.r.o. za možnosť nadobudnutia potrebných informácií a poskytnutie podkladových materiálov. Taktiež poďakovanie patrí rodičom, priateľke a kamarátom za podporu počas celého štúdia.

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně …….

podpis diplomanta

# OBSAH

# ÚVOD

Témou tejto diplomovej práce je rozpracovanie stavu kompletnej ochrany business centra za pomoci poplachových zabezpečovacích a tiesňových systémov s využitím kamerových a prístupových systémov s biometrickými prvkami. Podobnou témou som sa zaoberal taktiež v bakalárskej práci, s názvom „Vstupné a výstupné externé zariadenia pripájané k elektronickému zabezpečovaciemu systému“. [13]

V dnešnej dobe sa zabezpečenie firemných, priemyselných a verejných objektov stalo bežným štandardom a značne preniká aj do súkromnej sféry. Je to spôsobené pokročilou modernou dobou, kedy je treba chrániť či už svoj alebo cudzí majetok pred rôznymi páchateľmi a zlodejmi. Polícia je často krát proti vynaliezavosti zlodejov bezradná a preto sa ľudia snažia si svoj majetok dobre poistiť, zabezpečiť a v zásade chrániť pred zničením a ukradnutím. Čím viac práce má zlodej s vniknutím do samotného objektu, tým viac ho to odradí od spáchania trestného činu a náš majetok zostane nepoškodený a naďalej chránený.

Zabezpečovaný objekt alebo business centrum sa nachádza v kritickej lokalite s častým výskytom škôd na majetku. Podľa najčastejšieho vniknutia do objektu bude návrh zabezpečenia riešený tak, aby prioritne boli chránené všetky okná a dvere cez ktoré je možné do objektu vniknúť.

Majiteľ business centra vedľa základnej ochrany pomocou poplachového zabezpečovacieho a tiesňového systému, ďalej len PZTS, dáva dôraz na kamerový systém, ako pre vonkajšiu tak i vnútornú kontrolu. Vedľa požiadaviek majiteľa objektu bude treba pre konkrétny návrh spracovať analýzu rizík súčasného stavu centra. Práca bude obsahovať konkrétny návrh typov a umiestnení jednotlivých komponentov PZTS, prístupového systému, popis ich prepojení a komunikácie medzi sebou.

Cieľom tejto diplomovej práce je zhodnotenie navrhnutého systému a následné navrhnutie ďalšieho prípadného vylepšenia súčasného systému.

# I. TEORETICKÁ ČÁST

# 1 ZARIADENIA POPLACHOVÉHO ZABEZPEČOVACIEHO A TIESŇOVÉHO SYSTÉMU

Poplachový zabezpečovací a tiesňový systém ďalej PZTS je elektronické zariadenie, ktoré slúži k zabezpečeniu pozemkov, domov, kancelárii a mnohých ďalších nehnuteľností. Jej využitie je hlavne zabezpečenie objektu voči krádeži v ňom.

PZTS tvorí viacero častí a to: samotná ústredňa, detektory, klávesnice, výstupné zariadenia a to sirény, komunikátor a mnoho ďalších externých zariadený na rozšírenie funkčnosti PZTS. Existujú dva druhy PZTS a to drôtové a bezdrôtové. Ako bezpečnejšie a spoľahlivejšie sa považujú drôtové PZTS, pri ktorých sa nemôže stať že by bol rušený signál medzi detektorom a ústredňou alebo medzi ústredňou a inými externými bezdrôtovými zariadeniami. [8]

## 1.1 Ústredňa

Centrálna časť každého PZTS je ústredňa, príklad ústredne je na obrázku 1. Pomocou vstupných zariadení (detektorov) vyhodnocuje pohyb v určitej časti stráženého prostredia. Ak je systém vo vypnutom stave ústredňa narušenie detektora neodovzdáva ďalej. Ale pri narušení detektora v stave zapnutého stráženia ústredňa informáciu o narušení odovzdáva ďalej a to na výstupné zariadenia, sirénu, GSM komunikátor alebo na pult centralizovanej ochrany a podľa funkcií a naprogramovania výstupné zariadenia upozorňujú na danú udalosť. Ústredňa slúži tiež ako napájanie pre ostatné zariadenia pripájané k nej. Jej umiestnenie by malo byť niekde v strede objektu, na čo najmenej viditeľnom a čo najbezpečnejšom mieste chránenom okamžitým pasívnym infračerveným detektorom ďalej len PIR. [2, 3]

Ústredne sa od seba líšia počtom pripojiteľných vstupov a výstupov čo znamená počtom pripojiteľných PIR, teplotných snímačov alebo ovládacích zariadení na zapnutie alebo vypnutie stráženia. Podľa tejto skutočnosti sa vyberajú ústredne či už na stráženie malých domov alebo na stráženie obchodných centier ukážka na Obr. 1. Na výstupy sa pripájajú zariadenia ako siréna, GSM komunikátor alebo zariadenie ovládané ústredňou (napr. osvetlenie, klimatizácia, vykurovanie...). Taktiež sa ústredne líšia vo vytvorení počtu oblastí a množstva pripojenia klávesníc.


*Obr. 1: Ústredňa Integra 128 [9]*

## 1.2 Klávesnice

Klávesnica je hlavná komunikačná jednotka pripájaná k ústredni. Na Obr. 2 je príklad klávesnice pripájanej k ústredniam firmy Satel. Užívateľ pomocou nej dokáže zakódovať a odkódovať PZTS, pozrieť si pamäť porúch, vyblokovať niektoré z čidiel, alebo zmeniť kód pomocou ktorého dokáže zakódovať PZTS, taktiež užívateľ dokáže pomocou klávesnice ovládať pripojené externé zariadenia.

Klávesnica je najčastejšie umiestňovaná pri vchodové dvere pre rýchle odkódovanie systému po vstupe do objektu.

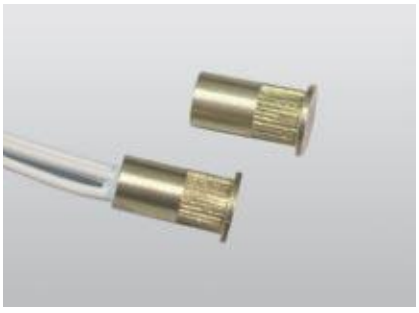

*Obr. 2: Klávesnica Integra - KLCD [9]*

## 1.3 Detektory

Sú veľmi dôležitá časť bezpečnostného systému. Od schopnosti detektorov rozlíšiť pohyb osôb od pohybu záclon alebo tepla od radiátorov sa odvíja aj počet falošných poplachov. Po zaznamenaní narušenia stráženého priestoru detektorom, detektor okamžite vysiela do ústredne signál o narušení zóny. Okamžité vyhodnotenie ústredne vysiela zase signál siréne, GSM komunikátoru, ktorý buď prostredníctvom SMS alebo hovoru oznámi užívateľovi informáciu o napadnutí. Detektory sa rozdeľujú do viacerých skupín podľa spôsobu využitia. V ďalších kapitolách tieto skupiny detektorov bližšie špecifikujem a dodávam k nim príklady, s ktorými som sa v praxi stretol. [1, 13]

### 1.3.1 Magnetické detektory

Tvorí ich dvojica dielov – jazýčkový kontakt a permanentný magnet. Magnetický kontakt je tvorený zatavenou trubičkou naplnenou ochranou atmosférou, kde sa nachádzajú dva feromagnetické kontakty. Permanentný magnet je najčastejšie zo zmagnetizovaného feritu. Magnet sa montuje na pohyblivú časť (dvere, krídlo okna, mreže) a kontakt sa montuje na pevnú časť (zárubne, rámy). Pri otvorení sa kontakt preruší a informácia je predávaná do ústredne PZTS. Magnetické kontakty sa dajú montovať či už povrchovo alebo zapustiť do dverí a zárubní. Ukážka zapúšťaných magnetov je na Obr. 3. Ďalej poukazujem na viacero druhov magnetických detektorov.



*Obr. 3: Magnetický kontakt CSA 314 [9]*

### 1.3.2 Pasívne infračervené detektory

Uvedené detektory sú označované ako PIR detektory. Príklad detektora je na Obr. 4. Detektory samé energiu nevyžarujú. Sú založené na princípe zachytávania zmien v infračervenom pásme kmitočtového spektra elektromagnetického vlnenia. Využívajú rozdiel teplôt jednotlivých telies, ktorých teplota sa pohybuje medzi –273 ºC a 560 ºC (teplota ľudského teľa je asi 36 ºC a pre túto teplotu je vlnová dĺžka 9,4 mm). Elektronika vyhodnotí signál spôsobený týmito zmenami a odošle do ústredne signál narušenia. Detektory sa neodporúča umiestňovať oproti zrkadlám, oknám a lesklým plochám taktiež sa neodporúča ich montáž nad zdroj tepla. Montáž by mala byť na pevnom podklade bez otrasov pre zaistenie bezproblémovej funkčnosti. Detektory sa navzájom neovplyvňujú čiže do jednej miestnosti je možné namontovať aj viac detektorov. Niektoré detektory používajú funkciu antimaskingu ktorá zaistí neprekrytie detektora skrinkou, zastriekanie sprejom alebo oblepenia. [3, 4]

*Obr. 4: Prestige IR [10]*

### 1.3.3 Mikrovlnné detektory

Veľmi spoľahlivé detektory, pracujúce na princípe Dopplerového efektu. V okolí detektoru sa nesmú nachádzať myši, netopiere a pri zapnutí stráženia sa kvôli čo najvyššej spoľahlivosti nesmie nachádzať výbojkové svetlo s možnosťou zapnutia počas stráženia. Montáž detektorov je zložitá kvôli jeho umiestneniu (detektor zachytáva objekty aj za stenou). V okolí detektora by sa nemali nachádzať veľké kovové objekty.

### 1.3.4 Ultrazvukové detektory

Aktívny ultrazvukový detektor je určený k priestorovej ochrane. Do monitorovaného priestoru vysiela ultrazvukové vlny a reaguje na zmenu kmitočtu odrazených vĺn. Pri narušení objektu vyhodnotí zmenu kmitočtu oznámi ústredni narušenie. Výhodou je, že nereaguje na zmeny teplôt a je ho možné použiť aj v členitých miestnostiach.

### 1.3.5 Infračervené závory

Sú zložené z dvoch častí z aktívnej časti vysielača a pasívnej časti prijímača. Pri prerušení lúča vysielaného z vysielača do prijímača nastáva narušenie je vyvolaný poplach. Dosah závory je 20 – 80 m. Závory sú chránené aj voči oklamaniu iným vysielačom. Infračervené závory sú často používané ako obvodová ochrana objektu. Pri zlých poveternostných podmienkach (dážď, hmla, padanie snehu) môžu nastať falošné poplachy. Infračervené závory sa najčastejšie montujú na železné konzoly umiestňované pri plotoch. Konzoly musia byť pevne ukotvené aby sa pri vetre nerozkývali a nespôsobovali tak falošné poplachy. Ukážka infračervených závor umiestňovaných do vonkajšieho prostredia je na Obr. 5. [13]

*Obr. 5: Infrazávory – Atsumi [9]*

### 1.3.6 Špeciálne detektory

- **Detektory rozbitia skla**

Detektor rozbitia skla príklad na Obr. 6, sníma zvukové vlny v úzkom kmitočtovom pásme. Detektor sníma buď piezoelektrickým meničom alebo elektretovým mikrofónom. Montáž detektorov sa odporúča na miesto odkiaľ detektor vidí na chránenú sklenú plochu. Medzi detektor a sklo sa neodporúča umiestňovať žalúzie alebo záclony. Negatívne na detektor vplýva vonkajšia premávka alebo blízkosť kontajnerov na sklo.

*Obr. 6: Detektor rozbitia skla – Satel Indigo [9]*

- **Dymový hlásič požiaru ionizačný**

Pri požiari hlásič zaznamená zmeny vodivosti v ionizačnej komore, medzi elektródami začne pretekať väčší prúd. Detektor sa umiestňuje na strop miestnosti, v ktorej hrozí potenciálna možnosť vzniku požiaru.

- **Opticko teplotný dymový senzor**

Princíp detektoru spočíva v rozptyle optického lúču na čiastočkách dymu. Po vniknutí dymu do detektoru sa čiastočky dymu rozptýlia na čiastočky aerosoly, čím sa časť lúčov dostane i na svetlocitlivý prvok. Hlásič sa neumiestňuje do výbušného prostredia.

- **Detektor úniku vody**

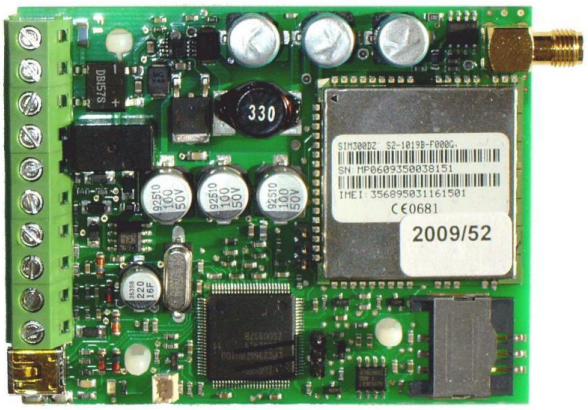
Detektor je určený pre detekciu zaplavenia priestoru alebo prekročenie povolenej výšky vodnej hladiny. Väčšinou máva externú sondu ktorá je pripájaná do samotného detektora, v ktorom sa vyhodnocuje hodnota vysielaná zo sondy. Tieto detektory sa hlavne využívajú v kúpeľniach , kotolniach alebo v bazénoch. [13]

*Obr. 7: Detektor úniku vody – Satel FD – 1 [9]*

## 1.4 GSM komunikátory

Zariadenia, ktoré pomocou pevnej telefónnej siete, mobilnej siete GSM lebo pomocou siete Ethernet prenášajú informácie o alarme, zakódovaní alebo odkódovaní systému. Samotný užívateľ si pomocou tohto zariadenia môže diaľkovo ovládať zariadenia pripojené ku komunikátoru. Najčastejšie používané sú GSM komunikátory príklad na Obr. 8, do ktorých treba pre funkčnosť vložiť aktívnu SIM kartu. Zariadenie sa

umiestňuje pri ústredňu pre jednoduchý prístup, anténa sa umiestňuje na zariadenie z vonku pre lepší signál. Programovanie sa robí pomocou pripojenia PC väčšinou cez MIKRO USB alebo cez zbernicu. Na programovanie sa používa priložený software, do ktorého sa zadávajú tel. čísla užívateľov, určuje sa ako majú vstupy a výstupy reagovať v aktívnom stave. [13]




*Obr. 8: GSM komunikátor – ESIM 151 [9]*

## 1.5 Sirény

Dôležitá časť PZTS, siréna, ktorá akusticky a opticky upozorňuje ľudí v okolí narušeného objektu o napadnutí. Táto časť PZTS je zobrazená na Obr. 9. Jedna z častí systému ktorá sa montuje do vonkajšieho prostredia a musí mať ochranu aspoň IP44. Sirény bývajú z pravidla zálohované akumulátorom pre možnosť odstrihnutia od ústredne. Umiestnenia býva na fasáde domu, na viditeľnom mieste pre lepšie počutie a upozornenie pri poplachu.

*Obr. 9: Siréna Satel SP 500-R [9]*

# 2 PRÍSTUPOVÉ SYSTÉMY

Jednou z hlavných častí bezpečnostného systému sú prvky ktoré slúžia k overeniu identity osôb. V tejto súvislosti je významným parametrom autentizácia, či daná osoba je skutočne tou osobou, za ktorú sa vydáva. Strážime objekty, kde je treba monitorovať aká osoba vstupuje, kam vstupuje a kedy vstupuje. Každá osoba je zatriedená do skupiny, ktorej sa pridávajú rôzne práva a prístupy. Systémy bývajú založené na jednoznačnej identifikácii osôb pomocou bezkontaktnej čipovej karty, kontaktných čipov alebo pomocou biometrickej identifikácie. Na základe načítaného vnútorného kódu karty/čipu príslušným terminálom je bez ohľadu na práva držiteľa karty, urobený záznam o tejto udalosti do systému s potrebnými parametrami (miesto, čas). Potom je na základe uložených údajov v systéme overované v časových, topologických a ďalších súvislostí či oprávnený držiteľ karty ma povolenie na prechod terminálom alebo dverami. Prístupové systémy zahrnujú funkcie:

- systém snímania prechodov,
- prístupový terminál,
- sledovanie stavu,
- definovanie prístupových modelov,
- sledovanie prechodov cez zámky,
- systém antipassback. [7]

## 2.1 Možnosti prístupu

Veľkou časťou autentizačných metód sú práve biometrické autentizačné prístupy, ktoré využívajú k overeniu identity osôb jej charakteristické rysy, ktoré sa nazývajú biometrické parametre. Systémy ktoré využívajú biometrickú identifikáciu už nepotrebujú žiadne vecné pomôcky (užívateľské kľúče, identifikačné karty), čo predstavuje značnú výhodu. Rozdelenie autentizačných prístupov je založený:

- na tom, čo človek vie ( autentizácia pomocou hesla ) – jednoduchá metóda na technickú a programovú realizáciu ale zato nie moc bezpečná jednoduché

odchytenie hesla. Použitie len v prostredí s minimálnymi bezpečnostnými požiadavkami.

- na tom, čo človek má ( autentizácia predmetom ) – najčastejšia identifikácia pomocou identifikačného predmetu, ktorý potvrdzuje identitu svojho vlastníka, užíva sa termín token. Tokeny by mali plniť požiadavku jedinečnosti a ťažkej napodobenosti. Nevýhodou je, že token môže byť ukradnutý. Preto sú často tvorené prístupy pomocou kombinácie autentizačného predmetu a hesla.
- na tom, čo človek je ( biometrická autentizácia ) – založená na biometrických charakteristikách osoby. Najčastejší spôsob identifikácie je pomocou odtlačku prstov. [7]

## 2.2 Zloženie prístupového systému

Prístupový systém sa najčastejšie skladá z čítačky a ovládaného prvku, ale taktiež sa používajú čítačky so samostatnou ovládacou ústredňou zvyčajne umiestňovanou mimo čítačky.

- **Čítačka**

Hlavnou časťou prístupového systému je identifikačný prvok (čítačka), ktorá má buď v sebe zabudovanú pamäť alebo je pripojená k ústredni, PC alebo serveru, v ktorom sa informácie z čítačky spracovávajú. V tejto pamäti sú uložené informácie o jednotlivých užívateľoch, kam a kedy má užívateľ prístup. Ukážka čítačky s vnútornou pamäťou na Obr. 10.


*Obr. 10: Čítačka Entry E KR11 [11]*

- **Ovládaný prvok**

Ovládaný prvok je ďalšia dôležitá časť prístupového systému. Ako ovládaný prvok sa používa buď to elektrický zámok zobrazený na Obr. 11, terminál, magnet alebo závora. Táto časť je ovládaná pomocou vyhodnotenia v čítačke. Ovládaný prvok má buď svoj napájací zdroj alebo je napájaný priamo z čítačky. Najčastejšie používaný elektrický zámok sa napája priamo z čítačky pre jeho nízky prúdový odber.

*Obr. 11: Elektrický zámok [11]*

# 3 KAMEROVÉ SYSTÉMY

Pre zabezpečovanie verejných a služobných priestorov objektov a ich okolí sa stále viac v tejto dobe využívajú kamerové systémy, tzv. CCTV (Closed Circuit Television – Uzavreté televízne okruhy). Účelom systému CCTV je zabezpečiť členité alebo niekoľko poschodové priestory, kde je nutné mať aspoň čiastočnú kontrolu nad pohybom zamestnancov alebo návštevníkov. Systém umožňuje efektívne monitorovať strážený priestor a zároveň kontrolovať veľmi rozsiahle priestory v reálnom čase. Vďaka moderným technológiám sa pre prenos obrazu používajú dátové linky alebo internet. CCTV dokáže zaznamenať zo stráženého priestoru obraz na digitálne dátové médium, alebo rovno na určený server. Tento záznam slúži k vyhodnocovaniu poplachových situácií, k spätnému dohľadaniu skôr nahratými informáciami. Systém CCTV je vhodný v kombinácii s PZTS, alebo je možné ho použiť ako samostatnú bezpečnostnú aplikáciu. Systémom CCTV sa zaoberá norma ČSN EN 50 132. [6]

## 3.1 Rozdelenie kamier

Základné rozdelenie bezpečnostných kamier: analógové a digitálne kamery. V súčasnosti sa stále viac vyskytujú digitálne kamery ako analógové.

Zásadný rozdiel týchto technológií je v spôsobe prenosu informácií a to ako sa prenáša obraz z kamier do nahrávacieho zariadenia. Analógové kamery príklad na Obr. 13, pre prenos používajú analógový prenos signálu. Prenosová norma pre TV prenos je stará viac ako 50 rokov a z tohto dôvodu sú možnosti tohto typu kamier obmedzené. Digitálne kamery (IP kamery) príklad na Obr. 12 používajú pre prenos obrazu bežnú PC sieť, kde je pre prenos informácií väčšia šírka pásma a kamery nie sú tak obmedzené, ako pri analógových kamerách. Technológie sa akurát stretajú v tom, že obidve používajú pri spôsobe získavania obrazu fyzikálno – optický princíp.

## 3.2 Zloženie kamerového systému

Kamerový systém, či už analógový alebo digitálny, sa skladá z troch hlavných častí a to je nahrávacie zariadenie (DVR, NVR alebo PC), samotných kamier a zobrazovacieho zariadenia.

### 3.2.1 Kamery

Kamery sú základným prvkom CCTV systémov. Kamera je snímacie zariadenie, ktoré posiela nasnímané dáta do nahrávacieho zariadenia. Svetelnú energiu odrazenú od predmetov v ich zornom poli následne prevádzať na elektrické signály určené na prenos a ďalšie spracovanie. Kvalita a správna voľba typu kamery, ako aj ostatných prvkov kamerového systému, ovplyvňujú výslednú hodnotu kamerového systému ako celku. [7]

*Obr. 12: IP kamera Dahua IPC – HDB4200CP [11]*


*Obr. 13: Analógová kamera CNB DFL-21S [11]*

### 3.2.2 Nahrávacie zariadenie

Záznamové zariadenie slúži na zachovanie (archiváciu) zachytených záberov pomocou kamerového systému. Na túto činnosť sa používajú rôzne druhy médií. Pri začiatkoch kamerových systémov sa používali klasické VHS zariadenia. V súčasnej dobe sa používa digitálny záznam videosignálu a jeho prípadná archivácia.

Najčastejším nahrávacím zariadením je DVR (Digital Video Recorder) a NVR (Network Video Recorder), ktoré sú určené na spracovanie a nahrávanie videosignálu ukážka na Obr. 14. [7]


*Obr. 14: Dahua NVR5216 [11]*

### 3.2.3 Zobrazovacie zariadenia

Zobrazovacie zariadenie slúži k zobrazeniu dejov, snímaných kamerou a k zobrazeniu záznamu, uloženého v záznamovom zariadení. Zobrazovacie zariadenia sa väčšinou pripájajú priamo k záznamovému zariadeniu. V súčasnosti sú veľmi používané LCD, plazmové a LED monitory, ukážka na Obr. 15. Do popredia sa však začínajú dostávať LED diódy. Tieto typy zobrazovacích zariadení je možné vyrábať v rôznych veľkostiach uhlopriečok obrazoviek. [7]

*Obr. 15: LCD monitor LG 32LN570R [12]*

# II. PRAKTICKÁ ČÁST

# 4 NÁVRH A REALIZÁCIA POPLACHOVÉHO ZABEZPEČOVACIEHO, PRÍSTUPOVÉHO A KAMEROVÉHO SYSTÉMU

Praktická časť tejto práce sa zaoberá požiadavkami od majiteľa business centra v blízkosti centra Bratislavy o zrealizovanie elektronického zabezpečovacieho systému, kamerového systému a prístupového systému, ako prvé bol objekt obhliadnutý a boli zistené možnosti napadnutia.

Objekt sa nachádza v kritickej lokalite s častými kriminálnymi činmi na majetku. Je to novostavba s tromi nadzemnými poschodiami a malým pozemkom. Budova nemá žiadne zabezpečenie, ani prístupový, ani kamerový systém. Po tejto obhliadke bola vypracovaná ponuka, s ktorou majiteľ súhlasil a zahrňovala všetky požadované systémy. Realizáciu projektu zabezpečuje firma TECHNIK Security, spol. s.r.o. Základom projektu je PZTS, ktorý bude doplnený o kamerový a prístupový systém. Podľa najčastejšieho vniknutia do objektu bude projekt zabezpečenia riešený tak, aby ako prioritné boli zabezpečované miestnosti s oknami a dverami do vonku. Do každej kancelárie bude umiestnený PIR detektor. Detektory sú umiestnené z väčšej časti do rohu, oproti dverám pre okamžité zachytenie páchateľa vstupujúceho cez dvere a na chodby boli umiestnené 360° detektory, ktoré zachytia plochu 6 m.

Ústredňa je navrhnutá do technickej miestnosti na vnútornú stenu budovy do výšky asi 2 m, aby nezavadzala ostatným zariadeniam a nebola úplne jednoducho prístupná a jasne viditeľná.

V tejto práci poukazujem na dve poschodia a to prízemie a jedno nadzemné poschodie. Na prízemie sa zameriavam, pretože v ňom je umiestnená ústredňa a zdrojová časť kamerového a prístupového systému, toto poschodie považujem za najdôležitejšie ohľadom zabezpečenia. Nadzemné poschodie je vybraté pre ukážku umiestnenia PIR snímačov, kamier, klávesníc a expandérov v kanceláriách a na chodbách.

V práci nie je zadaná presná poloha objektu a fotky z kamier, pretože tieto informácie si majiteľ neprial zverejňovať. Informácie by mohli poškodiť bezpečnosť budovy a poukázať na možné zraniteľné miesta.

## 4.1 Návrh poplachového zabezpečovacieho a tiesňového systému

Pri návrhu systému vopred menovanou firmou budú vyberané spoľahlivé zariadenia, firmou často montované a nenáročné na údržbu. Zariadenia musia byť medzi sebou kompatibilné a pri potrebe veľmi jednoducho rozšíriteľné.

Samotné ústredne sa od seba líšia svojimi funkciami, možnosťami rozšírenia a v spôsobe využitia. Zásadný výber ústredne, ovplyvní veľkosť zabezpečovaného objektu a množstvo klávesníc pripájaných k PZTS. Pre náš objekt sme vybrali ústredňu od firmy Satel, často montovanú našou firmou. Ústredňa Integra 64 je určená pre väčšie objekty, napr. veľké domy, obchodné centrá, business centrá alebo firmy. K tejto ústredni sa dá taktiež pripojiť až 8 LCD klávesnic a 16 zón, ktoré sa pripájajú priamo na dosku ústredne. Ústredňa sa dá rozšíriť o ďalších 48 zón pomocou expandérov vstupov.

### 4.1.1 Použité prvky PZTS

- **Integra 64**

Ústredňa Integra 64 od výrobcu Satel (Obr. 16) je určená pre veľké objekty (viacgeneračné domy, obchodné domy). Je možné k nej pripojiť až 64 vstupných a výstupných programovateľných zariadení. Možnosť rozdelenia systému na 32 skupín a 8 oblastí. Pamäť až 6143 udalostí, 64 nezávislých timerov a 192 užívateľov plus servisný technik. Ústredňa obsahuje funkciu kontroly prístupu a domovej automatiky riešenej pomocou programovateľných výstupov. Zabudovaný pulzný zdroj s výkonom 3 A s funkciou dobíjania akumulátora.[2]

Ústredňu sa odporúča osádzať do skriniek na to určených, a to kovových skriniek s transformátorom s výstupným napätím 20 V AC, s priestorom na 17 Ah akumulátor a tamperom na uzatváraní skrinky.

*Obr. 16: Zapojená ústredňa Integra 64*

- **Prestige IR**

PIR snímač vyrábaný firmou Texecom, zobrazený na Obr. 17 s dosahom do 15 m. Má vysokou odolnosť voči falošným poplachom pomocou utesnenia optiky voči rýchlej zmene teploty. Môže sa montovať do výšky 1,5 – 3 m. Veľmi jednoduchá montáž a vyvažovanie odporov pomocou jumprov. [5]

*Obr. 17: Namontovaný PIR snímač Prestige IR*

- **Texecom IMPAQ GLASS BREAK**

Snímač rozbitia skla obsahujúci duálny ohybovo akustický detektor s regulovaním dosahu snímania rozbitia skla do 9 m. Používa číslicové spracovanie zvuku pre vyššiu odolnosť voči falošným poplachom. Najčastejšie sa umiestňuje na strop, nad okno.

- **3045 – W**

Výklopné tiesňové tlačidlo, určené na povrchovú montáž pripájané do obvodu jako NC kontakt. Odporúčaná montáž je na spodnú stranu stola, alebo pultu. Návrat do kľudového stavu jednoduchým zasunutím tlačítka do pôvodnej polohy.

- **INT – KLCDR – BL**

Klávesnica s veľkým prehľadným LCD displejom, navrhnutá k ústredniam typu INTEGRA. Klávesnica zobrazená na Obr. 18 je vybavená bzučiakom, ktorý potvrdzuje vykonané príkazy a signalizuje rôzne stavy, ktoré sa vyskytli v zabezpečovacom systéme. Taktiež obsahuje bezkontaktnú čítačku kariet, čo zjednodušuje prístup užívateľov do objektu. Nad displejom sú osadené led diódy, ktoré indikujú poplach, poruchu, zapnutie alebo príchodový čas.


*Obr. 18: Namontovaná klávesnica INT – KLCDR - BL*

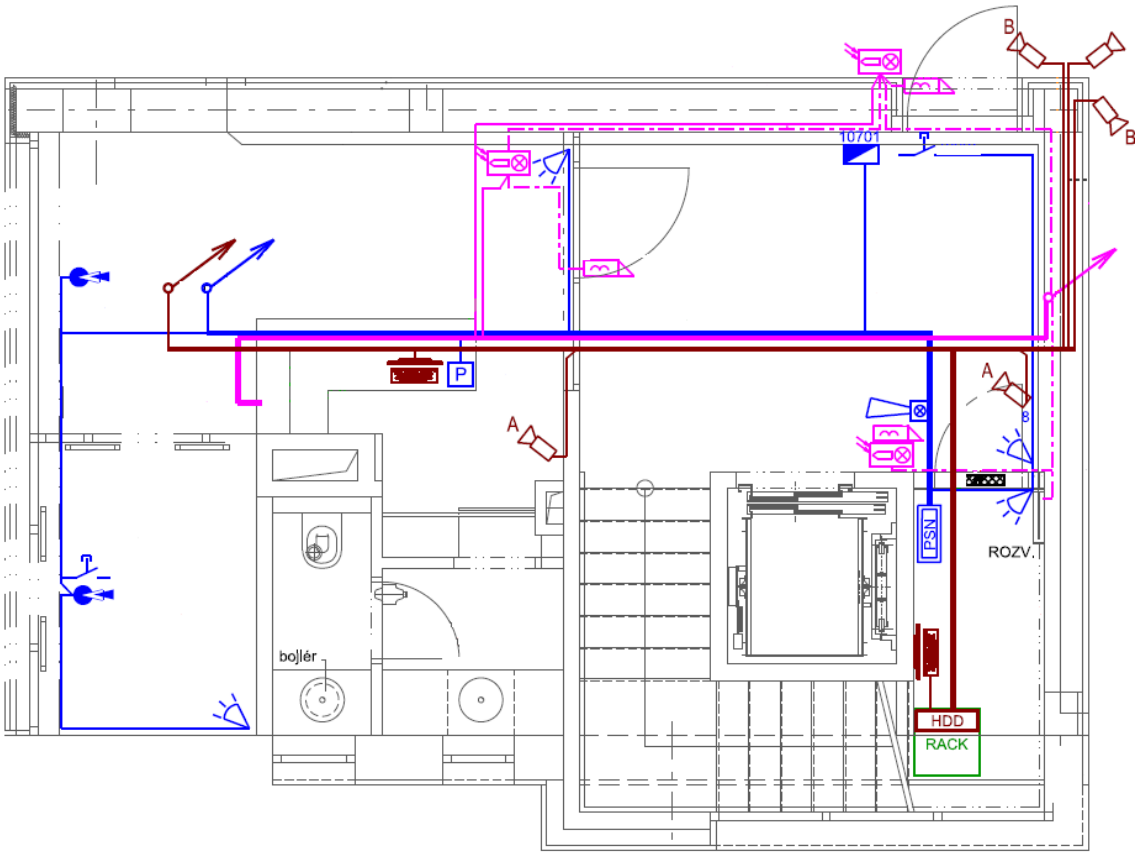
- **Satel – AQUA RING**

Je stropný 360° snímač, ktorý pri namontovaní do výšky 2,4 m zachytáva priestor o priemere 6 m a pri montážnej výške 3,7 m zachytí plochu v priemere 9 m. Regulácia citlivosti sa dá nadstavovať príslušnými jumpermi. [2]

### 4.1.2 Kabeláž a zapojenie poplachového zabezpečovacieho a tiesňového systému

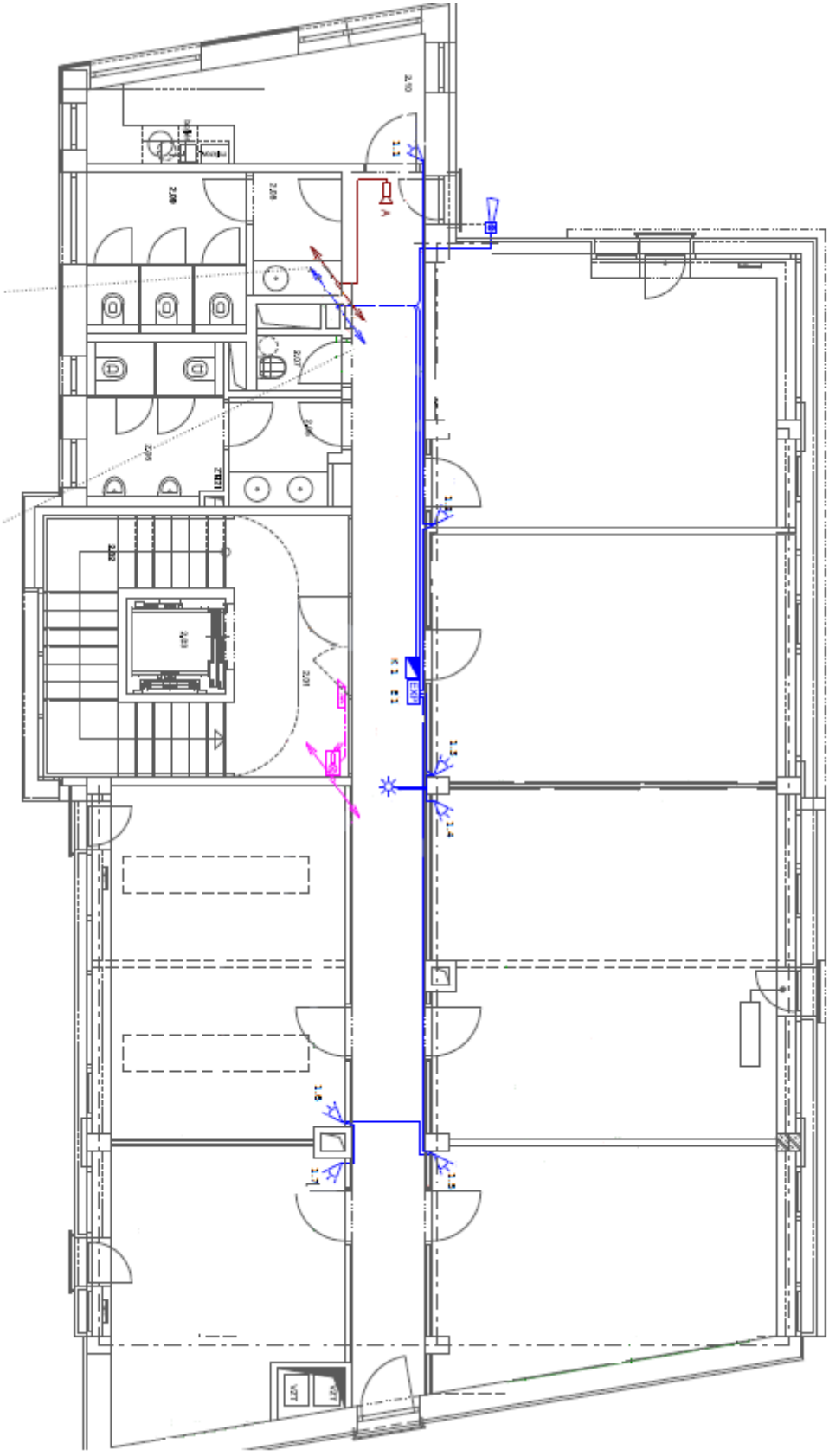
Ako prvý krok bolo privedenie napájania z elektrického rozvádzača k PZTS, podľa vopred vypracovaného projektu, ukázanom na Obr. 19. Na každom poschodí je umiestnený expandér pre jednoduchšiu kabeláž a ušetrenie FTP vodiča. Snímače a magnetické kontakty na jednotlivých poschodiach sú dovádzané k expandérom na týchto poschodiach a taktiež aj klávesnice sú dovádzané k jednotlivým expandérom. Expandéry sú jednotlivo privedené k ústredni. Siréna a GSM komunikátor sú pripojené priamo k ústredni. Snímače boli medzi sebou smičkované pre ušetrenie káblu a každá smička bola privedená do ústredne alebo k expandéru. Ďalšie metre káblu boli použité na prepoj k domácemu telefónu, rozvádzaču, racku a na prepoj medzi vonkajšou čítačkou a ústredňou.

Rozmiestnenie snímačov na prízemí budovy je jasne vidieť na Obr. 19. Snímače sú rozmiestňované tak, aby pokryli celé prízemie a miestnosti v ňom. Väčšina snímačov je namontovaná v rohoch miestností pre lepšiu funkčnosť a estetiku miestnosti. Klávesnica je umiestnená hneď za vstupnými dverami pre dobrú dostupnosť a rýchlu možnosť odkódovania systému po vstupe do budovy. Okná na recepcii sú taktiež zabezpečené snímačmi rozbitia skla, pre rýchle vyhodnotenie poplachu pri rozbitý skla. Vstupné dvere, aj bočné, aj elektrické sú zabezpečené magnetickým kontaktom, ktorý má pridelený príchodový čas 30 s. Pod stolom na recepcii je umiestnené panik tlačítko, ktoré zabezpečuje bezpečnosť recepčnej pri prepade počas prevádzky. V chodbe je umiestnená vnútorná siréna, ktorá hlási poplach tak, ako vonkajšia, ale popri tom hlási ešte navyše tamper na hociktorom zo zariadení, či už snímačoch alebo vonkajšej sirény. Popis ostatných systémov z obrázku je v iných častiach mojej diplomovej práci.

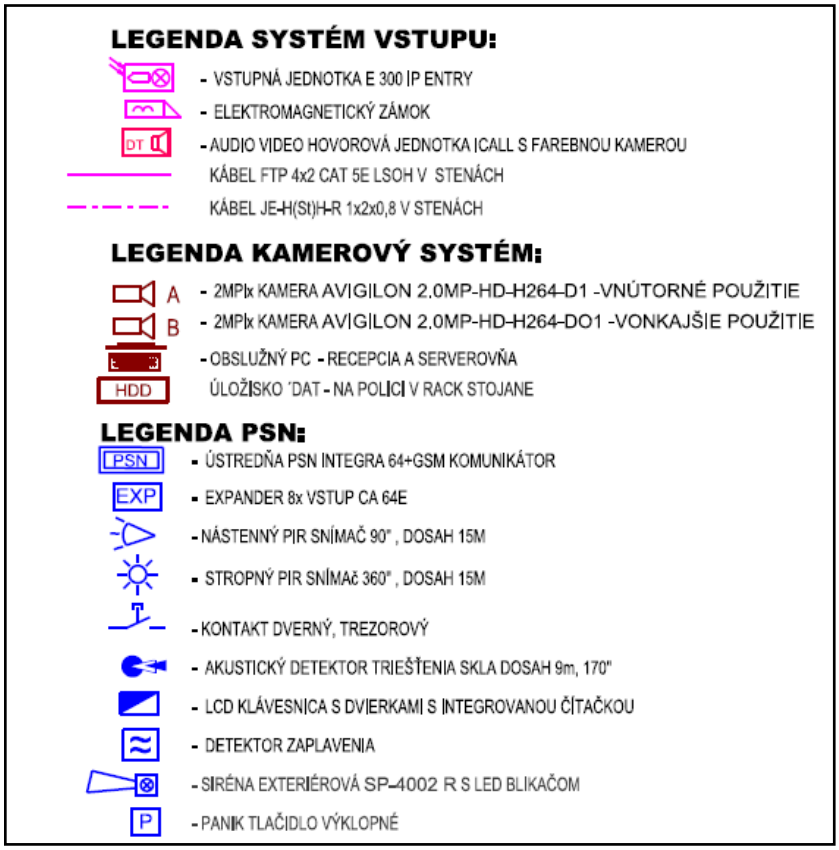



*Obr. 19: Ukážka zabezpečovacieho, prístupového a kamerového systému na prízemí*

Ukážka druhého nadzemného poschodia je na Obr. 20, kde je vidieť umiestnenie PIR snímačov v každej miestnosti s oknom, okrem sociálnych zariadení, ktoré majú len malé okná, cez ktoré sa nepredpokladá napadnutie budovy. Na chodbe sa nachádza 360° pohybový snímač, pre snímanie čo najväčšej časti chodby. Snímač pri našej výške pokrýva až 7 m okolo seba. Klávesnica je umiestnená priamo pred dverami pre jednoduchý prístup. Nad klávesnicou, pod stropom, v priestore nad kazetovým stropom je umiestnený expandér, do ktorého sú privedené všetky snímače a klávesnica z daného poschodia. Expandér je priamo pripojený k ústredni cez stupačku, pri sociálnom zariadení. Na tomto poschodí z vonku budovy sa taktiež nachádza vonkajšia siréna umiestnená do ulice. Siréna je nakáblovaná priamo do ústredne. Na obrázku je vidieť prístupový a kamerový systém, ktorý popisujem v inej časti mojej diplomovej práce.



*Obr. 20: Ukážka zabezpečovacieho, prístupového a kamerového systému na druhom poschodí.*

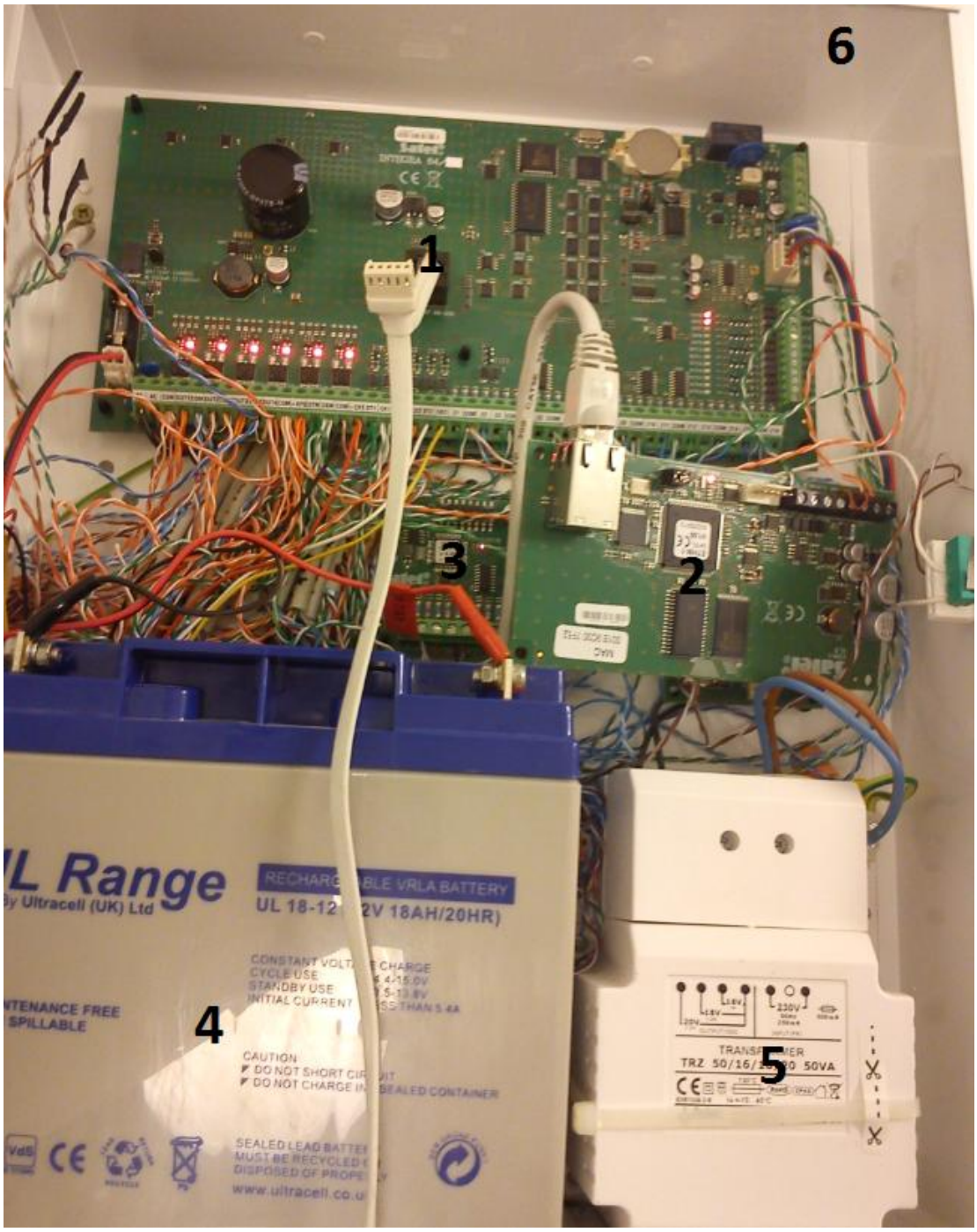



*Obr. 21: Legenda k Obr. 16 a 17*

Pri kompletáži PZTS boli ako prvé namontované PIR detektory, pre následné jednoduchšie zapájanie ústredne a expandérov (nameranie odporu 2,2 kΩ medzi vodičmi, na ktorých sa nachádza PIR detektor). Tieto veľmi jednoducho vyvažované detektory Prestige IR, vyvažované 1kΩ odpormi, boli montované do rohov pre lepšiu estetiku. Každý detektor bol pripájaný na zvlášť slučku, čiže v každom boli pripájané 4 vodiče - dva pre napájanie detektora a dva pre slučku. Magnetické kontakty boli pripájané na priamo, bez vyvažovania odpormi. Zapojenie klávesníc je jednoduché a zreteľne označené. Ale pri zapojení a najumprovaní sirény je to o niečo zložitejšie. Po nahodení všetkých externých zariadení, bolo začaté s vyskladaním ústredne do železnej skrine pre ústredňu určenej. Po namontovaní ústredne na stenu začíname zo zapojením ústredne, ukážka na Obr. 22.

Ústredňa bola prepojená s transformátorom pomocou priložených vodičov. Bola napájaná pomocou 16V transformátora. Do skrinky pri ústredňu bol pripevnený GSM komunikátor a prepojený s ústrednou pomocou 8 žilového FTP káblu. Dva výstupy z ústredne boli pripojené na vstupy do GSM komunikátora, jeden bol použitý ako poplachový a druhý bol

použitý ako výpadok napájania. Taktiež bolo privedené napájanie do GSM komunikátora z AUX výstupu z ústredne.




*Obr. 22: Zapojená ústredňa s pridanými zariadeniami*

1 – Ústredňa Integra 64

2 – Ethernetový modul ETHM - 1

3 – Expandér vstupov CA – 64 E

4 – Záložný akumulátor 12 V, 18 Ah

5 – Zdroj pre napájanie ústredne 16 V , 2,7 A

6 – Skrinka pre osadenie ústredne AWO 250

PZTS je zálohovaný záložným 18 Ah akumulátorom ktorý automaticky nabehne pri výpadku elektrickej energie a udrží systém až 12 hodín v prevádzke. Po spätnej obnove elektrickej energie sa akumulátor začne nabíjať. Priemerná životnosť akumulátora je 6 rokov. Ak sa akumulátor systémom nedokáže dobiť na požadovanú hodnotu systém vyhodnotí akumulátor ako nežiaduci a na klávesnici sa zobrazí systémová chyba. Výmenu akumulátora zabezpečuje servisný technik.

## 4.2 Návrh prístupového systému

Objekt je oplotený a dá sa doň vojsť, buď to vstupnou bránkou pre peších alebo veľkou bránou určenou pre vjazd vozidiel.

Vstup do budovy je cez hlavné dvere, na recepciu, kde je voľný vstup iba po recepciu alebo bočným vstupom, dverami pre vstup osôb s prideleným oprávnením na vstup.

### 4.2.1 Vonkajší systém vstupu

Pre vstup cez bránku pre peších bude osadená biometrická čítačka a domáci videovrátnik s elektromagnetickým zámkom, pre otvorenie ramena bránky. Vstup je povolený buď to osobám s prideleným oprávnením na vstup, alebo pomocou videovrátnika osobou na recepcii. Po vstupe do objektu, osoba musí zase buď to prejsť cez hlavný vchod k recepcii, alebo vojsť bočným vstupom, kde znovu musí prejsť cez biometrickú čítačku.

Pri vstupe návštevníkov autom do areálu bude pri vstupnej bráne osadená jednotka domáceho videovrátnika. Po zazvonení, pracovník recepcie môže diaľkovým ovládačom otvoriť vstupnú bránku pre vjazd. Návštevník sa po vjazde hlási na recepcii. Pri vstupovaní oprávnenej osoby autom, si osoba bránu otvorí vlastným diaľkovým ovládačom.

### 4.2.2 Vnútorný systém vstupu

Návštevník sa vždy prihlási na recepcii, kde mu bude na základe rozhodnutia informátora pridelená identifikačná bezdotyková karta, ktorá bude naprogramovaná pre možnosť návštevy v jednotlivých podlažiach. Po upovedomení informátora navštívenej osoby má návštevník možnosť vstupu iba na podlažie , kde sa nachádza navštívená osoba.

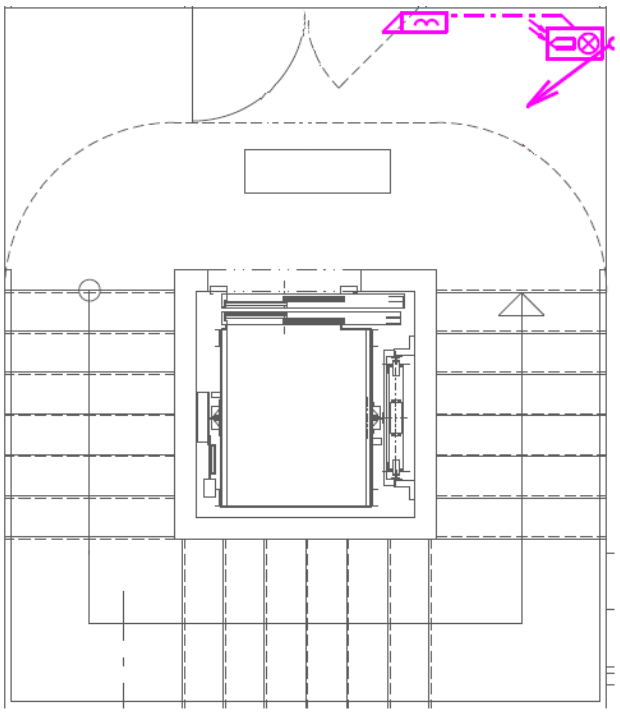
Oprávnená osoba – pracovník budovy má vlastnú kartu, ktorá mu umožňuje vstup iba na svoje pracovisko.

### 4.2.3 Kabeláž a samotné riešenie systému

Prístupový systém je riešený pomocou samostatných biometrických čítačiek, pripojených do switchu, ktorý je prepojený s vnútornou sieťou budovy, ukážka na Obr. 24. Každá čítačka je taktiež prepojená s jedným elektronickým zámkom, pomocou ktorého tieto dvere ovláda a po identifikácii povoľuje, alebo zamieta vstup. Pre pridávanie a určovanie práv užívateľom je používaný počítač na recepcii, v ktorom je nainštalovaný ovládací software, pomocou ktorého sa dajú tieto úlohy plniť.

Ako vstupná jednotka bola použitá antivandal, bezdotiková čítačka s biometrikou E 300IP ENTRY, osadená na vybraných miestach objektu so zdrojom napájania v racku.

Ukážka umiestnenia prístupového systému na jednotlivých poschodiach (Obr. 23). Pred dverami sa nachádza biometrická čítačka, ktorá ovláda elektrický zámok dverí.



*Obr. 23: Príklad umiestnenia prístupového systému na jednotlivých poschodiach*

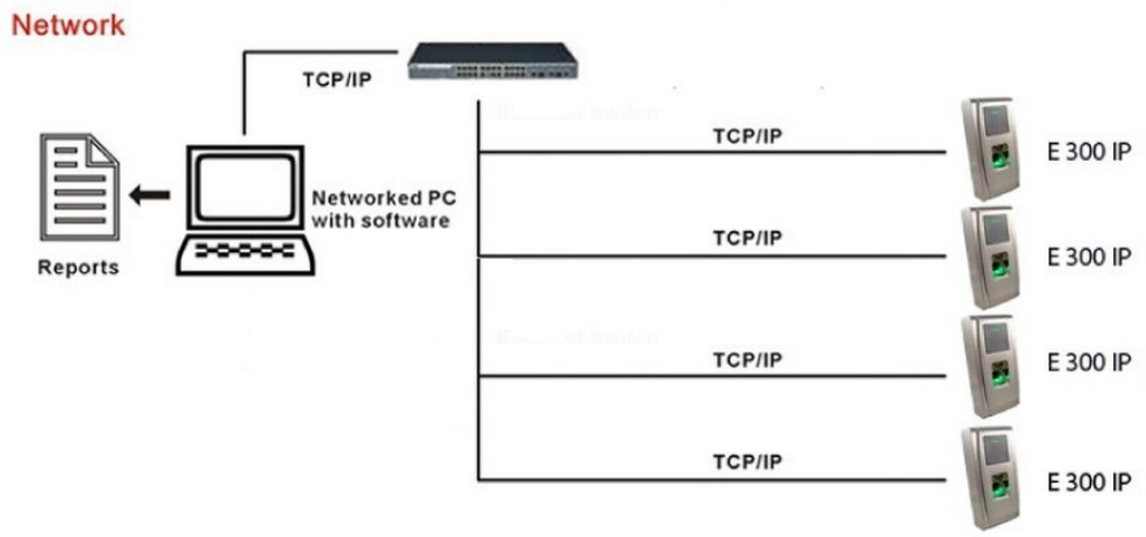
Legenda k Obr. 23:

 - Vstupná biometrická jednotka E 300 ENTRY

 - Elektronický zámok

- **ENTRY E 300IP**

IP prístupová jednotka s biometrickým snímačom odtlačku prsta s bezdotykovou RFID čítačkou, čítačka má kapacitu 1500 odtlačkov, 10 000 kariet a 100 000 udalostí. Komunikácia s PC je cez TCP/IP a RS232/485. Pri priložení neuloženého odtlačku čítačka upozorní užívateľa na nemožný prechod dverami, zvukovou a LED signalizáciou. Obsahuje relé kontakt pre ovládanie zámku. Prístupová jednotka je napájaná 12VDC a maximálny odber je 0,23A. Prístroj je určený na použitie do vonkajšieho prostredia a má IP54. [11]




*Obr. 24: Prepojenie čítačiek [11]*

Prístupová jednotka je montovaná aj vo vnútorných, aj vo vonkajších častiach budovy.


*Obr. 25: Čítačka interiér (obrázok vľavo) a exteriér (obrázok vpravo)*

## 4.3 Návrh a výber kamerového systému

Kamerový systém tvorí len časť tejto diplomovej práce, a preto nie je spracovaný úplne dopodrobna.

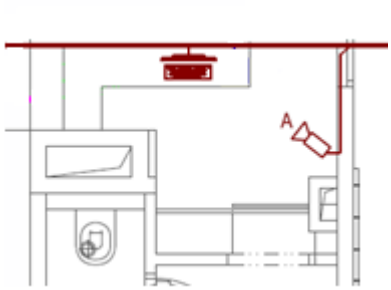
Ako prvé bolo riešené, či sa budú používať analógové, alebo digitálne kamery. V tejto časti bol rozhodujúci rozpočet, bo vo väčšine častí boli viac vyhovujúce digitálne kamery. Rozhodované bolo podľa parametrov v Tabuľke 1.

| Vlastnosť | Analogový systém kamier | IP systém kamier |
|---|---|---|
| **Rozlíšenie kamier** | 0,4 MPix | **Štandartne 1,3 - 2 MPix** |
| **Citlivosť kamier** | **Vyšší** | Nižší |
| **Snímková frekvencia** | 25 FPS | **6 - 60 FPS** |
| **Detekcia pohybu v obraze** | Áno (často len pri použití záznamového zariadenia) | **Áno** |
| **Inteligentná analýza** | Ne | **Áno** |
| **Je možné sledovať cez internet a na mobilných zariadeniach** | Väčšinou áno (len pri použití záznamového zariadenia) | **Áno** |
| **Nároky na diskovú kapacitu** | **Nižší**<br>Jedna kamera pri plnej snímkovej frekvencii spotrebuje cca 20GB denne | Vyšší<br>Jedna kamera v rozlíšení 2MPix pri plnom snímkovaní frekvenciou, vyžaduje cca 100GB denne |
| **Kabeláž** | **Vyhradená**<br>Káble už nie je možné využiť k prenosu iných informacií, k jednej kamere niekedy musí viesť niekoľko káblov | **Zdieľaná**<br>Káble je možné využiť i k iným účelom (napr. pre pripojenie počítačov). Jeden kábel často prenáša niekoľko rôznych typov dát a môže slúžiť i k prenosu napájania |
| **Úroveň zabezpečenia** | Nižší | **Vyšší** |
| **Štandartizácia** | **Vyšší** | Nižší |
| **Finančné nároky** | **Nižší** | Vyšší |

*Tabuľka 1: Výhody a nevýhody analógových a IP kamier*

Kamerový systém bol navrhovaný tak, aby pokryl čo najväčšiu časť dvora, a to hlavne vstup doň, predný, bočný vstup do budovy a parkovisko v objekte. Ako záznamové zariadenie bol navrhnutý PC s dvomi 3TB HDD, uložený v technickej miestnosti v racku a využívajúc záložný napájací zdroj UPS systému štrukturovanej kabeláže.

Kamerový systém je riešený IP kamerami s PoE napájaním pomocou prívodného kábla. Pre PoE napájanie je použitý 8 násobný PoE adaptér s pripojením na zdroj.
Na recepcii bude osadená pracovná stanica PC s monitorom, pre možnosť viacnásobného monitorovania viacerých kamier naraz. [5]




*Obr. 26: Umiestnenie kamery a PC na recepcii*

Legenda k Obr. 26:

- IP kamera Avigilon

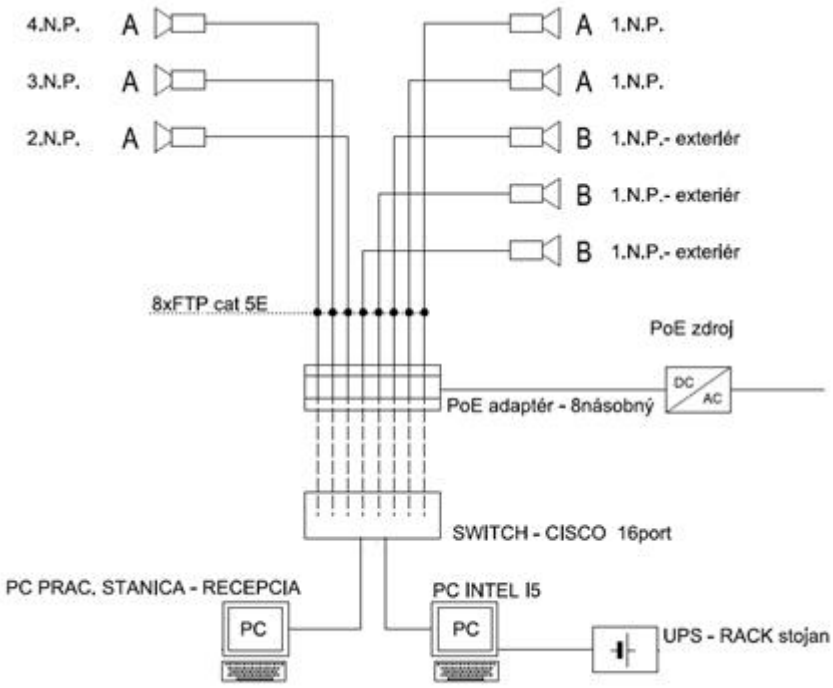
- Obslužný PC

### 4.3.1 Kabeláž a návrh systému

Ku každej kamere bol privedený samostatne FTP kábel, ktorý kamere zabezpečuje napájanie a taktiež dátový tok k úložnému zariadeniu, ukážka na Obr. 27. Systém bol navrhnutý tak, že do vonkajšej časti objektu bolo osadených 5 kamier, z toho dve snímajú predný plot, bránku a bránu. Ďalšie dve snímajú parkovisko a vstup cez bočné dvere ukážka na Obr. 19. Kamera je taktiež umiestnená aj na streche objektu, kde sníma zariadenie klimatizácie a strešnú terasu.

Vo vnútornej časti je umiestnených 6 kamier, a to kamera na každom poschodí na chodbe pre snímanie vstupujúcich osôb, na recepcii a jedna kamera je taktiež umiestnená v garáži.

Kamery boli navrhované tak, aby boli aspoň čiastočne chránené aj vo vonkajšom prostredí a tým nemuseli odolávať až takým poveternostným podmienkam.




*Obr. 27: Schéma zapojenia kamier*

**Použité kamery:**

- AVIGILON 2.0 MPx Dome IP kamera

Progresívna CMOS kamera (Obr. 28) navrhnutá pre široké spektrum použitia. Integrovaný a plne motorizovaný objektív umožňuje zoomovanie a ostrenie kamery na diaľku, čo uľahčuje inštaláciu pri vynikajúcej kvalite obrazu. Snímky sú prenášané cez 100 Mbit sieť s použitím technológie H.264 pre dosiahnutie najnižšej šírky pásma. Táto technológia zaberá minimálnu kapacitu záznamového média s vysokým počtom snímok za sekundu a vynikajúcou kvalitou obrazu.

Počas snímania z kamery, systém automaticky nastavuje čas expozície, clonu a IR CUT filter, ktorý zabezpečuje maximálne dosiahnuteľný obraz nasnímaný v nočnej scéne. Táto kamera je určená pre vonkajšie priestory a možno k nej použiť základovú dosku pre povrchovú montáž. Prevedenie je antivandal s krytím IP66 a zabudovaným vyhrievaním.

Kamera sa integruje so softvérom Avigilon Control Center NVMS a High Definition NVR s použitím štandardných sieťových technológií s jednoduchou obsluhou a ľahkou inštaláciou.

Napájanie je navrhnuté buď pomocou PoE, 12VDC = , alebo 24VAC ~.

*Obr. 28: Namontované kamery AVIGILON*

**Použité nahrávacie zariadenie:**

- Rackový PC

Použitý počítač musí splňovať určité požiadavky pre správny chod softwaru. Počítač, so sieťovou kartou 100 Mbit pre rýchly prenos dát z kamier a procesorom i5. Úložný priestor 6 TB, ktorý zaručí uchovanie záznamu minimálne na 30 dní. HDMI výstup, pre kvalitné zobrazenie kamier na výstupnom monitore a 4 GB pamäťou RAM pre rýchle spracovanie údajov.

Použitý software je Avigilon Control Center NVMS, v ktorom boli kamery pridávané podľa IP adresy a nadstavené na snímanie pri pohybe.

Software Avigilon Control Center NVMS slúži pre monitorovanie, nahrávanie a ovládanie megapixelových kamier. Je jednoducho ovládateľný a prezeranie záznamu je prehľadné a rýchle. V našom prípade má software licenciu pre 16 IP kamier.


*Obr. 29: Rackový PC so switchom*

# 5 PROGRAMOVANIE A PREPOJENIE SYSTÉMOV

Programovanie systémov bude riešené podľa požiadaviek zákazníka. Pri PZTS je požiadavka na rozdelenie systému na viacero podsystémov, pre možnosť kódovania každej kancelárie zvlášť. Taktiež sú podľa zákazníka určené práva jednotlivým užívateľom. Systém vstupu bude programovaný tak, aby čítačka ovládala len zámok pri nej. Vstup osôb bude riešený podľa požiadavky zákazníka. Kamerový systém pre úsporu miesta bude snímať len pri pohybe. Prepojenie systémov bude volené čo najjednoduchšie a najprehľadnejšie.

## 5.1 Programovanie poplachového zabezpečovacieho a tiesňového systému

Programovanie bude robené pomocou programu DLOADX, ktorý je priamo určený k programovaniu PZTS firmy SATEL. Pomocou tohto programu je možné naprogramovať celú ústredňu ,od vstupov cez výstupy až po určovanie časov v timeroch. Program je dodávaný k ústredniam na CD.

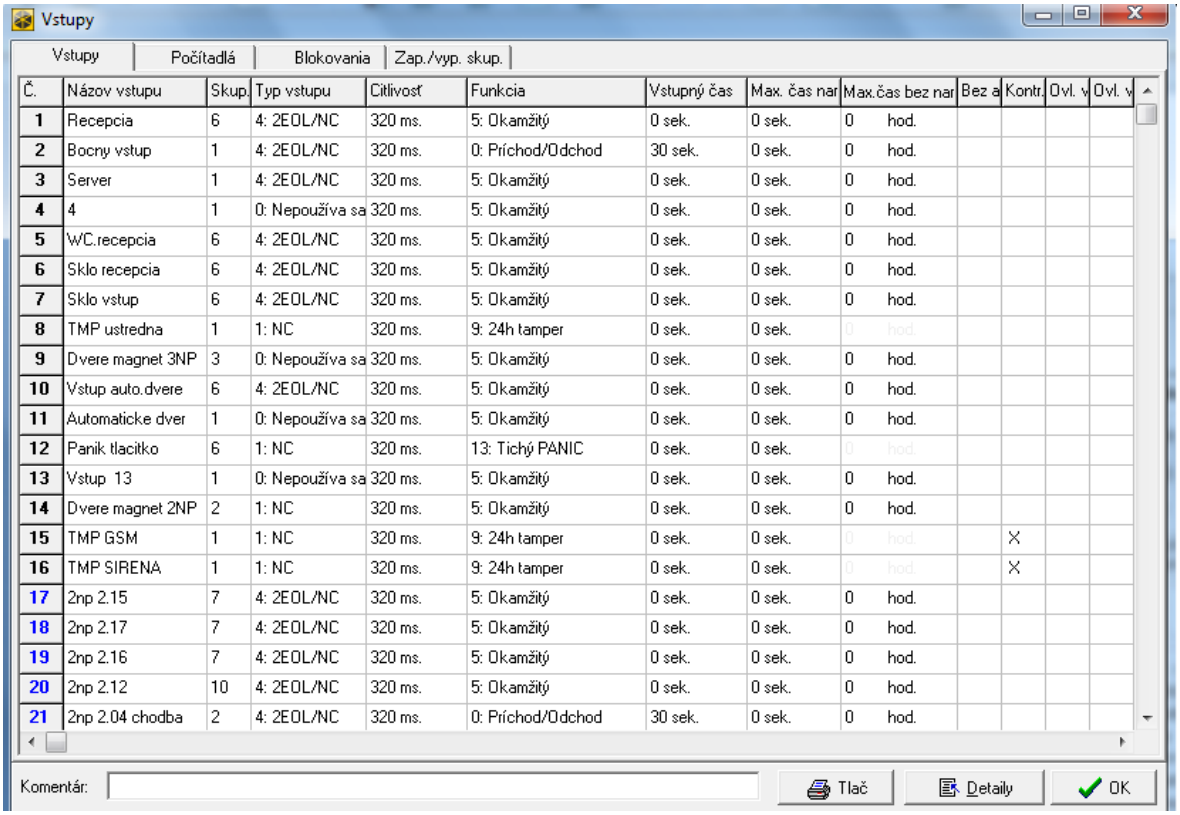
Po zapojení celého systému začíname s pripojením ústredne k el. sieti a to zasunutím sklenej poistky do poistkového púzdra. Zadaním výrobného servisného kódu na klávesnici bolo vbehnuté do menu klávesnice, bol povolený Download a vojdené do servisného režimu. Pomocou kábla určeného na pripojenie sa k ústredni, ústredňa bola s PC prepojená a zahájená komunikácia medzi ústredňou a PC pomocou programu DLOADX. Ako prvé boli načítané expandéry, ktorých je k ústredni pripojených sedem a to päť expandérov vstupov, jeden expandér výstupov a jeden zvukový expandér. Ako ďalšie sa načítajú klávesnice, ktoré si ústredna pridelí podľa adresy klávesnice. Klávesníc je v systéme šesť a to na každom poschodí a pri vstupných dverách jedna.

Systém bol rozdelený na 11 podsystémov pre možnosť zakódovania a odkódovania jednotlivých kancelárii a zasadacích miestností zvlášť. Tri z týchto podsystémov sú podsystémy logické, ktoré sú zakódovavané a odkódovavané pomocou logického ‘’AND‘‘ a to pri zakódovaní jednotlivých podsystémov, sa zakóduje taktiež logicky vytvorený podsystém. V každom podsystéme sa dajú zvlášť nadstaviť odchodové časy a taktiež klávesnice, z ktorých sa dá daný podsystém zakódovať alebo odkódovať.

- **Programovanie vstupov**

Ako ďalší krok bolo začaté programovanie vstupov ústredne, začaté bolo popisovaním jednotlivých zón, ukážka na Obr. 30. Popisovanie bolo robené podľa popisov na kábloch, alebo podľa narušenia na detektore. Detektory boli programované na typ zóny 2EOL/NC, čo sa určuje podľa pripojenia snímača k ústredni a vyváženia snímača pomocou odporov. K ústredni sú taktiež pripojené tri magnetické kontakty a jedno panik tlačítko, ktoré sú nadstavené ako NC.

Boli určené príchodové snímače a magnetické kontakty, ktoré sa nachádzajú na miestach, cez ktoré musíme prejsť, aby sa bolo možné dostať ku vstupnej klávesnici. Tieto snímače musia mať oneskorenie vyhlásenia poplachu. Vstupný čas bol určený na každom snímači odlišný. Všetky ostatné snímače boli nadstavené ako okamžité. Pri náhodnom zabudnutí určiť vstupné snímače ako príchodové by bol pri každom narušení potenciálneho vstupného snímača vyhlásený poplach. Ostatné nastavenia boli robené podľa vyžadovanej situácie. Napr. každý snímač môže spustiť behom jedného dňa pri zakódovaní, poplach len tri krát táto možnosť bola využitá pre náhodnú poruchu snímača.



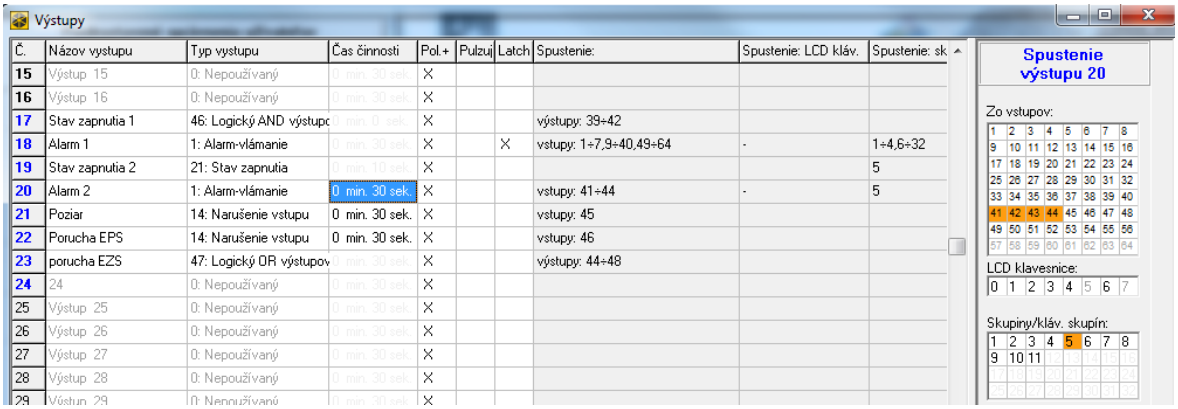

| Č. | Názov vstupu | Skup. | Typ vstupu | Citlivosť | Funkcia | Vstupný čas | Max. čas nar | Max.čas bez nar | Bez a | Kontr. | Ovl. v | Ovl. v |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Recepcia | 6 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 2 | Bocny vstup | 1 | 4: 2EOL/NC | 320 ms. | 0: Príchod/Odchod | 30 sek. | 0 sek. | 0 hod. | | | | |
| 3 | Server | 1 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 4 | 4 | 1 | 0: Nepoužíva sa | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 5 | WC.recepcia | 6 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 6 | Sklo recepcia | 6 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 7 | Sklo vstup | 6 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 8 | TMP ustredna | 1 | 1: NC | 320 ms. | 9: 24h tamper | 0 sek. | 0 sek. | 0 hod. | | | | |
| 9 | Dvere magnet 3NP | 3 | 0: Nepoužíva sa | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 10 | Vstup auto.dvere | 6 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 11 | Automaticke dver | 1 | 0: Nepoužíva sa | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 12 | Panik tlacitko | 6 | 1: NC | 320 ms. | 13: Tichý PANIC | 0 sek. | 0 sek. | 0 hod. | | | | |
| 13 | Vstup 13 | 1 | 0: Nepoužíva sa | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 14 | Dvere magnet 2NP | 2 | 1: NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 15 | TMP GSM | 1 | 1: NC | 320 ms. | 9: 24h tamper | 0 sek. | 0 sek. | 0 hod. | | X | | |
| 16 | TMP SIRENA | 1 | 1: NC | 320 ms. | 9: 24h tamper | 0 sek. | 0 sek. | 0 hod. | | X | | |
| 17 | 2np 2.15 | 7 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 18 | 2np 2.17 | 7 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 19 | 2np 2.16 | 7 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 20 | 2np 2.12 | 10 | 4: 2EOL/NC | 320 ms. | 5: Okamžitý | 0 sek. | 0 sek. | 0 hod. | | | | |
| 21 | 2np 2.04 chodba | 2 | 4: 2EOL/NC | 320 ms. | 0: Príchod/Odchod | 30 sek. | 0 sek. | 0 hod. | | | | |

*Obr. 30: Programovanie vstupov ústredne EZTS*

Ako ďalšie boli programované vstupy ako tamper sirény, tamper ústredne. Tieto vstupy sa nadstavujú ako NC, čo znamená v kľude uzatvorený obvod a funkciu ako 24h tamper, čo znamená, že pri narušení vodiča alebo odtrhnutí sirény obvod prerušený a následne vyhlásený poplach. Tento poplach je vyhlasovaný aj pri vypnutom strážení ale len na vnútornej siréne.

- **Programovanie výstupov**

Po naprogramovaní vstupov ústredne bolo začaté s programovaným výstupov, čo je o niečo zložitejšie. Zase bolo začaté s popisovaním výstupov (ukážka na Obr. 31) podľa toho, ako boli popripájané. V tomto prípade bolo ako prvé programované napájanie expandérov na jednotlivých poschodiach. Pri napájaní typ vstupu programujeme ako napájanie a bola pridelená len polarita výstupu ako stály plus. Toto bolo spravené zo štyrmi výstupmi a to na pridelenie jedného výstupu k jednému poschodiu. Výstup 5 a 6 boli programované ako alarm vlámania pre akustiku a optiku, kde optika je určená tak, aby blikala až do odkódovania po alarme a akustika nadstavená na jednu minútu. K výstupu 5 sú pridané všetky vstupy a k výstupu 6 sú pridané len snímače, ktoré sú na chodbách, recepcii a schodišti. Ďalší výstup bol nadstavený ako stav zapnutia, pomocou logického AND výstupov a to pomocou výstupu 39-42, ktoré sú nadstavené ako kódovanie jednotlivých častí systému. Privedené výstupy do komunikátora boli nadstavené ako poruchový výstup, ktorý zahŕňal poruchu akumulátora, poruchu napájania a taktiež pokles napätia na expanréry. Ďalšie bol nadstavené ako alarm, požiar a stav zapnutia.




*Obr. 31: Ukážka programovania výstupov*

- **Programovanie GSM komunikátora**

Po naprogramovaní výstupov začíname s programovaním vstupov GSM komunikátora. Ku komunikátoru sa pripájame pomocou micro usb káblu a pomocou programu Config Tool, kde si ako prvé zmeníme heslo a pokračujeme pridaním všetkých telefónnych čísiel, na ktoré by mal GSM komunikátor volať. Po zadaní čísel pridelíme jednotlivému telefónnemu číslu vstup komunikátora, pri ktorom zopnutí bude číslo vytočené. Taktiež možno pridať k jednotlivým vstupom SMS, ktorá bude odoslaná pridelením číslam. Napr. SMS o poruche systému, alebo o presnom určení, kde poplach vznikol. Do GSM komunikátora musíme vkladať SIM kartu, ktorá je bez hesla a je odskúšaná jej funkčnosť. Nadstavenie GSM komunikátora otestujeme pomocou prepnutia polarity na výstupoch ústredne.

- **Konfigurácia celého PZTS**

Asi najhlavnejšia požiadavka od majiteľa budovy bola, aby sa dali jednotlivé kancelárie kódovať zvlášť a po zakódovaní poslednej, sa zakódovala taktiež celá budova. Táto možnosť bola dosiahnutá tým, že systém bol rozdelený na viacero podsystémov, kde každý podsystém obsahoval jednu kanceláriu a teda každá kancelária má prideleného užívateľa, ktorý ju môže zakódovať alebo odkódovať. Ale dosiahnuť to, že po zakódovaní posledného subsystému sa zakóduje aj chodba nebolo také jednoduché. Musel byť vytvorený subsystém, ktorý je typu AND a zakóduje sa len pri zakódovaní všetkých kancelárií. Tento subsystém sa nedá jednotlivo samostatne ovládať a kódovať je ho možné zakódovať len pri kódovaní celej budovy, alebo teda pri zakódovaní všetkých kancelárií.

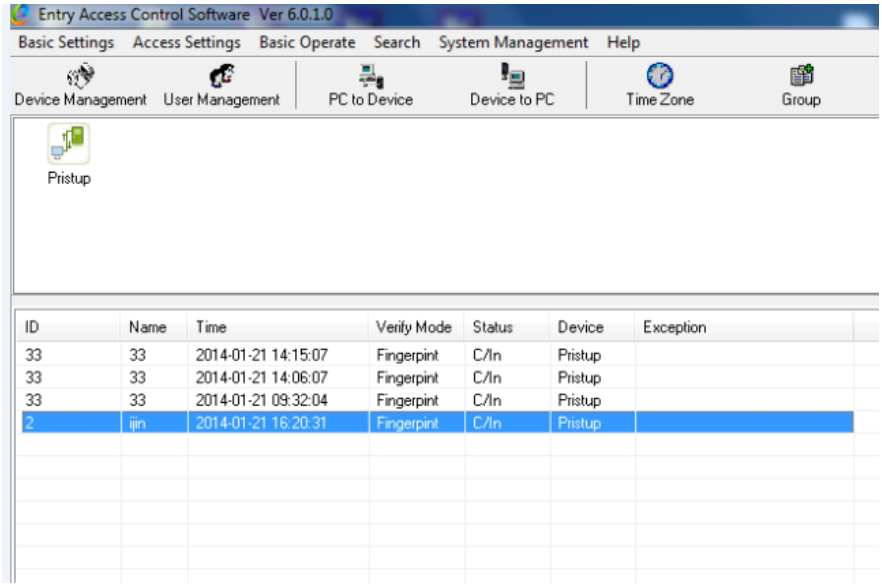
Systém je nadstavený tak, aby sa po desiatej hodine večer zakódoval sám, ak zakódovaný nie je a táto možnosť bola dosiahnutá nadstavením timerov ústredne.

V systéme boli povytváraný užívatelia, kde ku každému subsystému bol pridaný aspoň jeden, ktorý mal prístup do chodieb a do danej kancelárie. Recepčnej bol pridaný kód, pomocou ktorého môže odkódovávať rôzne časti budovy a taktiež môže hociktorý snímač aj vyblokovať, pre možnosť vyblokovania daného snímača v neprítomnosti niektorého z nájomcov kancelárií.

## 5.2 Programovanie prístupového systému

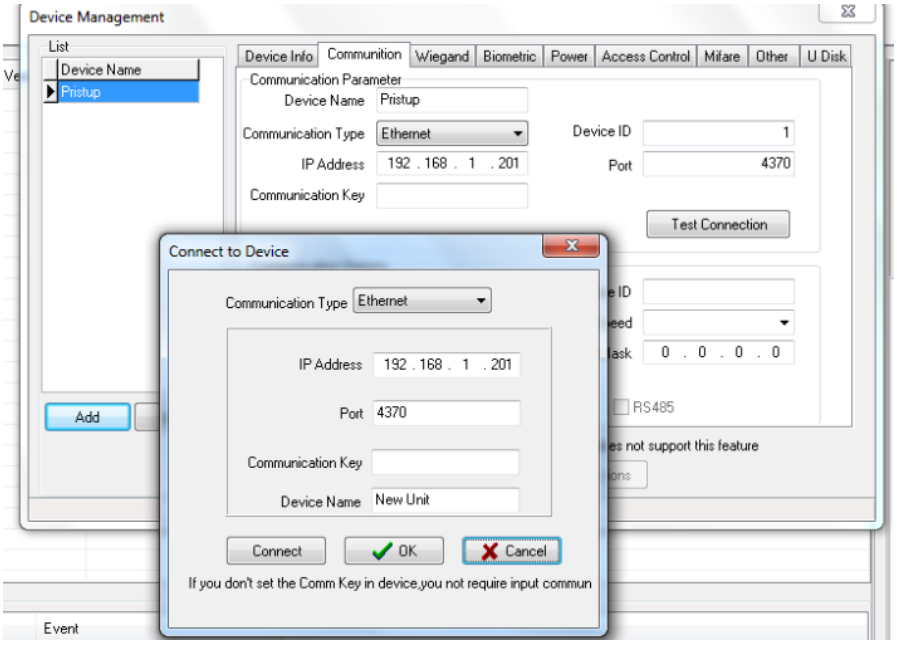
Programovanie bolo robené pomocou programu dodávaného priamo k čítačkám, a to programom Entry Access Control. Tento program slúži od pridávania užívateľov, až po určovanie funkcii jednotlivých čítačiek.

Ako prvé bolo treba každú čítačku samostatne pripojiť k PC a zmeniť jej IP adresu, podľa ktorej sa v softwary identifikuje. Na Obr. 32 vidno priraďovanie k programu a testovanie funkčnosti jednotlivých čítačiek.



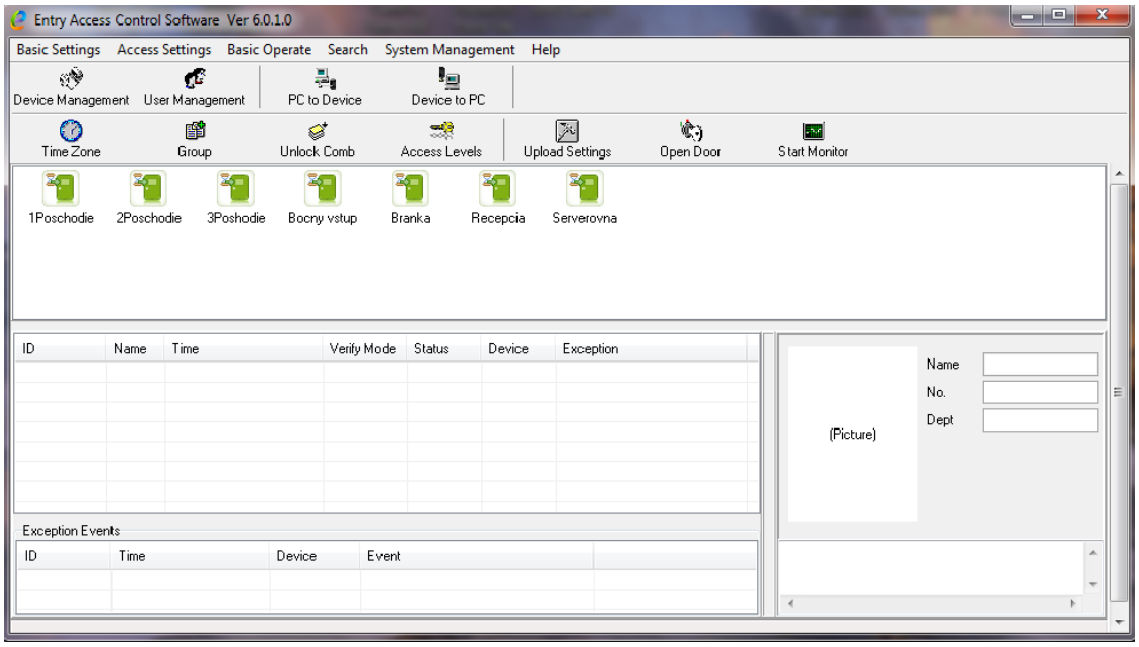

*Obr. 32: Testovanie jednotlivých biometrických čítačiek*

Softwer bol nainštalovaný do počítača na recepcii a čítačky boli jednotlivo pridávané podľa ich IP adries do programu. Obr. 33 zobrazuje všetky údaje zadávané pri priraďovaní čítačiek.




*Obr. 33: Pridávanie jednotlivých čítačiek*

Pri čítačkach bolo určené ako majú pracovať. Bolo im zadané, aby pri priložení prsta pridanej osoby prepli relé, pomocou ktorého sa do zámku dostalo 12 V na 5 s a zámok bol otvorený. Každá čítačka má pridelené, aby snímala či už biometriu alebo prístupové karty.



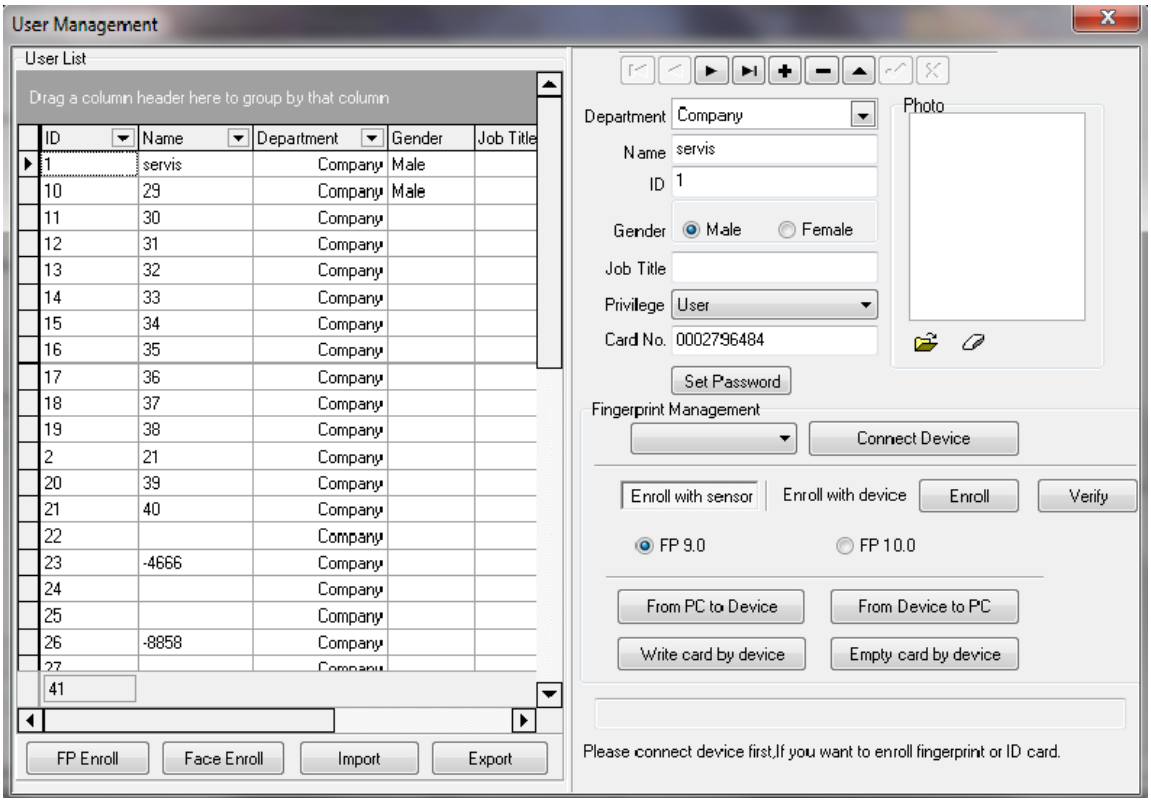

*Obr. 34: Ukážka pridaných čítačiek v programe*

Po pridaní všetkých čítačiek ako na Obr. 34, začíname v programe vytvárať užívateľov. Užívatelia, ktorý budú vstupovať pomocou biometrickej identifikácie, musia fyzicky otlačiť svoj prst na čítačke. Pre možnosť zranenia prsta do systému boli pridané u každého užívateľa aspoň tri prsty. Odtlačky sa ukladajú z danej čítačky v programe a odtiaľ sa ďalej rozposielajú do ostatných zariadený.

Každému užívateľovi sa určujú práva do akej časti budovy má prístup a v akom časovom intervale. A to tým, že do jednotlivých čítačiek sa nahrávajú tieto informácie postupne a do čítačky, cez ktorú má užívateľ vstup, sa údaje nahrajú a do čítačky, cez ktorú prístup nemá, sa údaje nenahrávajú. Užívateľom sa pridáva meno užívateľa a firmy. Pri náhodnej strate identifikačnej karty, sa podľa mena karta odstráni z jednotlivých čítačiek pre nemožnosť vstupu neoprávnenej osoby.

V systéme sa dá taktiež zistiť kto, kedy a kde vstupoval. Podľa týchto údajov sa dá overiť príchod a odchod z práce a taktiež zistiť kto odchádzal posledný z budovy. Z recepčného PC sa taktiež dajú manuálne ovládať jednotlivé čítačky podľa potreby otvorenia dverí.

Ukážka pridávania užívateľov do systému je na Obr. 35.




*Obr. 35: Pridávanie užívateľov do systému*

## 5.3 Prepojenie systémov

Už pri návrhoch systémov bolo riešené to, aby sa systémy navzájom negatívne neovplyvňovali, nerušili svoju funkcie schopnosť a boli navzájom kompatibilné. Preto boli v PZTS navrhované prvky od jedného dodávateľa a zväčša aj výrobcu. Tieto prvky medzi sebou bezproblémovo komunikujú a spolupracujú. Prístupový systém bol navrhovaný tak, aby mali biometrické čítačky možnosť pripojenia do siete a taktiež bolo po sieti možné konfigurovať a pridávať užívateľov.

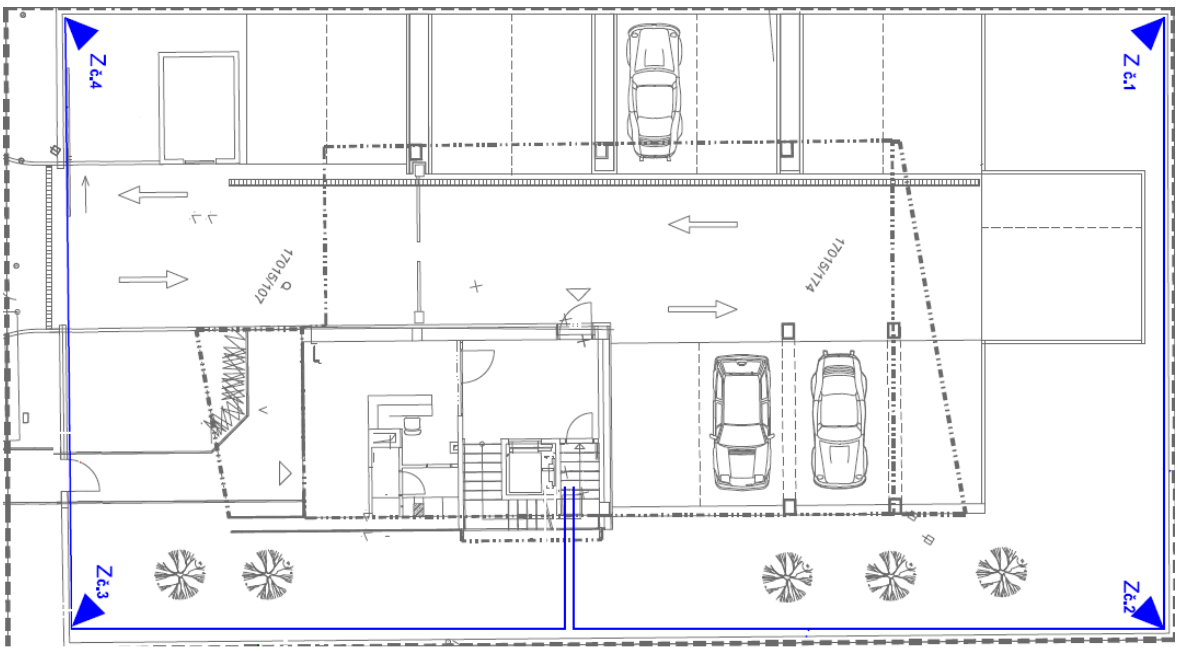
Spojenie týchto systémov sa dosiahlo v jednom PC na recepcii, kde je nainštalovaný program na ovládanie prístupového systému, taktiež PZTS a program pre prehliadanie záznamu kamier a live snímania. Týmto spojením sme dosiahli jednoduchosť v pridávaní užívateľov, kde je jasne dané, že ak pridávam užívateľa k PZTS, tak pridám užívateľa aj k prístupovému systému. Podľa možnosti vstupu, mu bude určená časť, ktorú môže odkódovávať a taktiež pridané biometrické čítačky, cez ktoré má užívateľ možnosť prechádzať. PZTS je pripojený do počítačovej siete pomocou LAN modulu pripojeného priamo k ústredni. Ako software v PC bol použitý GuardX, pomocou ktorého sa dá ústredňa kódovať, pridávať užívatelia, prezerať poplachy a taktiež nadstavovať základné nastavenia. Software pre kamerový systém Avigilon Control NVMS Center je jednoduchý, prehľadný a rýchly pri prezeraní záznamov.

Toto spojenie systémov v jednom PC nám umožňuje rýchlu kontrolu objektu po poplachu. A to pomocou software GuardX je možné skontrolovať kedy poplach nastal, a v ktorej časti budovy a následne je možné pomocou softwaru Avigilon Control Center NVMS skontrolovať danú časť objektu, v danej dobe z vybranej kamery.

# 6 NÁVRH VYLEPŠENIA SYSTÉMOV

Systémy sú podľa mňa dobre navrhnuté a spĺňajú požadované požiadavky. Celé vnútro budovy je chránené PZTS, kde v každej miestnosti s oknom je osadený PIR snímač a vstupné dvere sú chránené magnetmi. Vstupy do budovy sú taktiež zabezpečené prístupovým systémom, kde sa dá bez prístupu dostať len po recepciu. Ak sa chce návštevník dostať ďalej, musí mu to povoliť recepčná a prideliť mu, buď kartu alebo mu tlačítkom manuálne otvoriť elektrický zámok dverí. Kamery v objekte sú umiestnené tak, aby snímali prechod osôb cez predný alebo bočný vstup.

Ako každý systém, tak ani tento nie je výnimkou a pri vyššej investícii by sa určité veci na ňom dali vylepšiť. Ako prvé by som riešil vylepšenie PZTS tým, že by som celý objekt chránil perimetrickou ochranou a to infrazávorami, ukážka na Obr. 36. Ktoré by som napojil k PZTS a vytvoril nový podsystém, ktorý by bol chránený 24 hodín okrem predného plotu, ktorý by sa automaticky kódoval 10 minút po zakódovaní posledného podsystému. Infrazávory by som osadil na konzoly pri plot tak, aby sa nedali pri prípadnom preskočení alebo prestrihnutí plotu obísť.




*Obr. 36: Návrh osadenia infrazávor*

Legenda k Obr. 36:

◀ Z - Infrazávora, dvojlúčová

Infrazávory by zaručili okamžité vyhlásenie poplachu, už pri snahe sa dostať na pozemok budovy.

Pri dodatočnom zabezpečovaní a dostatku financií, by som na dva rohy pozemku ešte umiestnil dome kamery. Boli by v rohoch pozemku oproti seba, odkiaľ by pokryli celý pozemok. Použil by som kamery od firmy Avigilon, od ktorej sú kamery použité v celom objekte. IP kamera na Obr. 37, ktorá ma PTZ ovládanie, 2 MPx snímanie a dá sa jej nastaviť presný chod snímania.


*Obr. 37: Avigilon IP vonkajšia kamera [11]*

Systémy by som v PC na recepcii zintegroval do jedného, pre prehľadnejšie a jednoduchšie vytváranie užívateľov a hľadanie záznamov podľa alarmu na PZTS.

Toto vylepšenie systému by bolo finančne náročné, ale PZTS by bol účinnejší a vyvolanie poplachu by nastalo už pri vstupe na pozemok. Kamerový systém by pokryl celý perimeter, čo znamená, že by bol celý objekt monitorovaný. Navrhnuté vylepšenie som majiteľovi budovy odprezentoval. Majiteľovi sa návrh páčil a pri najbližšej investícii do zabezpečenia budovy sa ním bude určite zaoberať.

# ZÁVER

Cieľom tejto diplomovej práce je nielen popis zariadenia poplachového zabezpečovacieho a tiesňového systému, kamerového systému a prístupového systému s použitím biometrických prvkov, ale aj realizácia návrhu zabezpečenia objektu, teda návrh na vykonanie komplexného zabezpečenia Business centra. Práca je rozdelená na teoretickú a praktickú časť.

Teoretická časť sa zameriava na popis PZTS a jeho jednotlivých častí. Ďalej popisom typov a druhov kamerových a prístupových systémov, doplnené o konkrétne príklady riešení s cieľom prístupu k danej problematike.

Praktická časť je zväčša zameraná na PZTS, kamerové systémy a prístupové systémy, ich návrh, kabeláž a programovanie. Do tejto konkrétnej časti práce vkladám moje vlastné skúsenosti z firmy TECHNIK Security, ktorá sa zaoberá návrhom a montážou elektrických zabezpečovacích a prístupových zariadení, na ktorých v spolupráci s nimi pracujem už 4 roky.

Časť k PZTS sa venuje návrhu systému, kabeláži a programovaniu ústredne v programe DLOADX. Určitá časť je venovaná aj programovaniu GSM komunikátora, ktorý je dôležitou súčasťou PZTS. Nasledujúca časť práce pojednáva o návrhu a kabeláži kamerového a prístupového systému. V praktickej časti sa taktiež zaoberám softwarovým prepojením systémov medzi sebou.

Systémy sú už 3 mesiace v prevádzke, systém zabezpečenia je plne funkčný, neboli na ňom vykonávané žiadne dodatočné úpravy. Prístupový systém je taktiež funkčný ale asi mesiac po uvedení systému do prevádzky boli tri čítačky reklamované, pre ich výpadok spojenia s PC na recepcii a nemožné spätné pripojenie sa k nim. Pripájanie a programovanie čítačiek bol najväčší problém z celého zabezpečenia, čítačky od začiatku nekomunikovali a bol problém už pri prvom spojení, so zmenou IP adresy čítačky. Bez zmeny IP adresy v čítačke sa v programe čítačky nedali od seba odlíšiť. Po opätovnom resetovaní čítačiek sme zmeny IP adresy dosiahli a konfigurácia systému bola vykonaná. Kamerový systém od spustenia funguje, jediný zásah do systému bolo doladenie kamier v prítomnosti majiteľa budovy, podľa jeho žiadosti a priania.

Zadané požiadavky majiteľa boli v plnej miere splnené a majiteľ je s funkčnosťou a pracovaním systémov spokojný.

Osobne si myslím, že objekt je v súvislosti investovanej sumy dobre zabezpečený. Pri možnej dodatočnej investícii do zabezpečenia som vypracoval v diplomovej práci svoj návrh vylepšenia systémov. Vo vylepšení som sa zameral hlavne na zabezpečenia pozemku, na ktorom je budova postavená.

# ZOZNAM POUŽITEJ LITERATÚRY

*[1] LUKÁŠ, Luděk. Bezpečnostní technologie systémy a management lll.: Teorie a praxe ochrany majetku a fyzické bezpečnosti. Zlín: Radim Bučuvčík - VeRBuM, 2013. ISBN 978-80-87500-35-4.*

*[2] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. [S.l.: s.n.], 2003, 351 s. ISBN 80-902-9382-4.*

*[3] KINDL, Jiří. Projektování bezpečnostních systémů I. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.*

*[4] IVANKA, Ján. Systemizace bezpečnostního průmyslu [online]. 4. rozš. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011 [cit. 2012-02-01]. ISBN 978-80-7454-122-3. Dostupné z: https://web.fai.utb.cz/cs/docs/Skripta_Ivanka_SBP.pdf.*

*[5] BIGELOW, Stephen J. Mistrovství v počítačových sítích : správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.*

*[6] VALOUCH, Jan. Projektování integrovaných systémů [online]. 2013 [cit. 2014-02-05]. ISBN 978-80-7454-296-1. Dostupné z: http://dspace.k.utb.cz/bitstream/handle/10563/25814/Skripta%20-%20Valouch.pdf?sequence=1.*

*[7] ČANDÍK, Marek. Objektová bezpečnost II. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2004, 100 s. ISBN 8073182173.*

*[8] UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Policejní akademie české republiky, 2005, 229 s. ISBN 80-7251-189-0.*

*[9] Satel. HDsecurity [online]. 2007 [cit. 2014-05-13]. Dostupné z: http://www.hdsecurity.sk/*

*[10] K construct - elektro. SERIF. [online]. 2010 [cit. 2014-05-13]. Dostupné z: http://kconstruct.sk/*

*[11] Total Security System. TSS group [online]. 2002 [cit. 2014-05-21]. Dostupné z:* http://www.tssgroup.sk/

*[12] Alza. Alza [online]. 2000 [cit. 2014-05-21]. Dostupné z: http://www.alza.sk/*

*[13] OSTROVSKÝ, Patrik. Vstupné a výstupné externé zariadenia pripájané k elektronickému zabezpečovaciemu systému. Zlín, 2012. Bakalárka. UTB.*

# ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

| | |
|---|---|
| 2EOL/NC | Spôsob pripojenia detektora |
| AND | Logická funkcia |
| CCTV | Uzavretý televízny okruh |
| CMOS | Technológia výroby logických integrovaných obvodov |
| DVR | Digitálny videorekordér |
| GSM | Globálny systém pre mobilné komunikácie |
| HDD | Hard disk |
| HDMI | Rozhranie pre multimediálny prenos signálu |
| IP | Internetový protokol |
| LCD | Druh podsvietenie monitoru |
| LED | Druh podsvietenie monitoru |
| NC | Normálne otvorený obvod |
| NVR | Sieťový videorekordér |
| PC | Počítač |
| PIR | Pasívny infračervený detektor |
| PoE | Napájanie po dátovom sieťovom kábli |
| PTZ | Funkcia kamery (diaľkové ovládanie) |
| PZTS | Poplachový zabezpečovací a tiesňový systém |
| RAM | Pamäť s priamym prístupom |
| RFID | Identifikácia na rádiovej frekvencii |
| RS 232 | Sériový port |
| SMS | Krátka servisná správa |
| TCP | Primárny prenosový protokol |
| TV | Televízny prijímač |
| UPS | Neprerušiteľný zdroj energie |

| | |
|---|---|
| USB | Univerzálna sériová zbernica |

# ZOZNAM OBRÁZKOV

# ZOZNAM TABULIEK