Návrh a realizace víceúčelového objektu pomocí poplachového zabezpečovacího systému

The Design and Implementation of Multipurpose Building with Intruder Alarm System

Bc. Zdeněk Petlák

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Zdeněk PETLÁK**
Osobní číslo:	**A10330**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh a realizace zabezpečení víceúčelového objektu pomocí poplachového zabezpečovacího systému**

Zásady pro vypracování:

1. **Stanovte bezpečnostní rizika vybraného víceúčelového objektu a přilehlého okolí.**
2. **Zvolte optimální řešení technického a režimového zabezpečení objektu.**
3. **Navrhněte vhodné zabezpečení objektu pomocí systému IAS.**
4. **Vypracujte a realizujte projekt zabezpečení objektu s vyčíslením finančních nákladů aplikovaného systému.**
5. **Naprogramujte technický systém pomocí softwaru WinLoad.**
6. **Práci doplňte grafickou a obrazovou dokumentací realizovaného zabezpečení objektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KINDL, Jiří. Projektování bezpečnostních systémů I. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-807-3185-541.**
2. **ČANDÍK, Marek. Objektová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-731-8217-3.**
3. **UHLÁŘ, Jan. Technická ochrana objektů. 1. vyd. Praha: Policejní akademie České republiky, 2001, 205 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-725-1076-2.**
4. **IVANKA, Ján. Riadenie a bezpečnosť inteligentních budov. Security magazín - Alarm, vyd. Plettac Security, ročník XI, č.:2/2009, Infodom s.r.o., Slovenská republika , s. 18 ? 21, ISSN 1335 ? 504 X.**
5. **IVANKA, Ján. AUTOMATION SYSTEMS AND SAFETY IN INTELLIGENT BUILDINGS Conference Information: International Conference on Military Technologies, MAY 05-06, 2009 OPROX Inc, Brno, CZECH REPUBLIC Source: ICMT09: INTERNATIONAL CONFERENCE ON MILITARY TECHNOLOGIES Book Series: INTERNATIONAL CONFERENCE ON MILITARY TECHNOLOGIES p: 225-234 , ISBN: 978-80-7231-649-6 Published: 2010**

Vedoucí diplomové práce: **Ing. Ján Ivanka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem diplomové práce je navrhnout zabezpečení multifunkčního domu pomocí elektrického zabezpečovacího systému. Práce se dělí na teoretickou a praktickou část. V teoretické části jsou uvedeny normy týkající se elektrického zabezpečovacího systému a další náležitosti nezbytné k návrhu tohoto systému. V praktické části jsou uvedeny použité prvky k zabezpečení objektu, jejich popis, samotný návrh systému a vše je doplněno obrazovou dokumentací a aktualizací softwarového vybavení systému.

Klíčová slova: Elektrický zabezpečovací systém, norma, WinLoad, návrh

ABSTRACT

The aim of the thesis is to propose a multipurpouse building with an intruder alarm system. The thesis is divided into theoretical and practical part. In the theoretical section provides standards for intruder alarm system and other facilities necessary for the design of this system. In the practical section are mentioned the elements used to secure the building, their description, the actual system design is completed and all documentation and imaging software update system.

Keywords: Intruder Alarm System, norm, WinLoad, design

Tímto bych rád poděkoval svému vedoucímu diplomové práce, panu Ing. Jánu Ivankovi, za jeho ochotu při tvorbě diplomové práce, připomínky, návrhy, odborné vedení a vymezení času na konzultace. A rovněž Ing. Jiřímu Langerovi za cenné rady a možnost spolupráce s firmou, pro kterou pracuje.

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

Za rok 2011 došlo v České republice celkem k 59 672 krádeží vloupáním, z toho ve Zlínském kraji k 1 611 a v hlavním městě Praha k 10 385.[1] V letošním roce od 1.1.2012 do 31.3.2012 k celkovému počtu 14 264, ve Zlínském kraji k 409 a v hlavním městě Praha k 2 434.[2] Možná to nejsou velká čísla, ale hlavním účelem soukromých bezpečnostních služeb je snaha tato čísla ještě snížit. Ať už prevencí, nebo přímým zásahem při narušení našeho soukromí a vlastnictví.

Soukromé bezpečnostní služby se snaží o prevenci – předcházení kriminalitě, hlavně v obchodních domech. Dnes již nenarazíme na obchodní centrum, supermarket či hypermarket, kde by nebyl člen soukromé bezpečnostní služby. Jejich úkolem je již zmíněná prevence, ale i případné zadržení pachatele a jeho následné předání policii. Kromě fyzické ostrahy soukromé bezpečnostní služby instalují i systémy, které mají samy chránit celý objekt, nebo konkrétní předměty, zboží. V dnešní době si jich nelze nevšimnout, ať už právě ve zmiňovaných obchodních řetězcích, nebo třeba firmě, kde pracují atd. Mluvím především o elektrických zabezpečovacích systémech, kterým se bude věnovat i má diplomová práce. Další významnou rolí prvků elektrických zabezpečovacích systémů, konkrétně kamerových systémů, je následná identifikace pachatele a příslušné fotografie a video mohou posloužit i jako důkazy v trestním řízení.

Vzhledem k tomu, že již pátým rokem studuji obor Bezpečnostní technologie, systémy a management na UTB ve Zlíně, rozhodl jsem se vybrat téma zabezpečení objektu pomocí elektrického zabezpečovacího systému. Na toto téma bylo napsáno již mnoho prací, ale technologie jde každým rokem kupředu, tak se nám nabízí stále nové možnosti. Pro svou práci jsem si zvolil víceúčelový objekt, který se nachází právě v Praze. I přes značná omezení ze strany vlastníka jsem se pokusil s montážní firmou, která byla ochotna se mnou spolupracovat, vypracovat návrh zabezpečení a pak daný návrh i realizovat. Nejen, že nás značně omezoval rozpočet, ale taky fakt, že se v daném objektu nemohou provádět žádné stavební práce a z hlediska charakteru objektu byly zamítnuty i lišty, kterými se případně vedlo vedení. Proto jsme zvolili bezdrátový systém a jednotlivé prvky od firmy Paradox.

[1] Policie České republiky: Informační servis. *Statistiky* [online]. 31.12.2011 [cit. 2012-05-03]. Dostupné z: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-mapy-kriminality.aspx
[2] Policie České republiky: Informační servis. *Statistiky* [online]. 31.03.2012 [cit. 2012-05-03]. Dostupné z: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-956215.aspx

Tento systém byl zvolen vzhledem dobrých předešlých zkušeností tímto systémem právě montážní firmou a mým samým a k faktu, že splňoval kritéria, která mi zadal vlastník objektu.

Ve své práci jsem se snažil zúročit všechny poznatky a vědomosti nabyté právě během studia a roční praxe u dané bezpečnostní firmy. Podařilo se mi vypracovat návrh, který byl schválen vlastníkem objektu. K tomu jsem do práce zakomponoval i případné další návrhy, jak danou bezpečnost objektu v budoucnu ještě zvýšit.

V teoretické části diplomové práci se budu věnovat legislativě, základnímu členění ochrany a všem nezbytnostem, které jsou potřeba k návrhu elektrického zabezpečovacího systému, včetně bezpečnostního posouzení objektu. V praktické části se zaměřím na samotný víceúčelový objekt, provedu jeho bezpečnostní posouzení, bezpečnostně-technickou obhlídku objektu, popíši riziková místa a možné způsoby napadení. Dále navrhnu konkrétní způsob zabezpečení daného objektu dle možností a požadavků vlastníka a provede se realizace daného návrhu. Rovněž navrhnu i další možnosti, jak daný objekt zabezpečit, popíši jednotlivé prvky systému, který byl instalován a provedu jeho naprogramování a uvedu ho do provozního stavu.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ PRŮMYSL

Mezi základní činnosti firem, které řadíme do bezpečnostního průmyslu, patří fyzická ostraha majetku a osob, detektivní služby, přeprava peněz a cenností, zpracování peněžní hotovosti, a ochrana informací a dat. Prvotním účelem ochrany v bezpečnostním průmyslu je prevence. A právě při prevenci hrají významnou roli soukromé bezpečnostní služby, ať už při ochraně majetku a osob, při předcházení kriminalitě, tak zamezování škod vzniklých trestnou činností. Služby, které poskytují soukromé bezpečnostní agentury, zvyšují standard zákazníka a rovněž mu umožňují si přesně stanovit v jakém rozsahu a pomocí jakých prostředků bude tento standard navyšován.

Význam soukromých bezpečnostních služeb nastal hlavně po rozpadu sovětského svazu a vzniku samostatné České republiky. V této době nastal i velký rozvoj v podnikání v tomto oboru. Příčin bylo mnoho, mezi hlavní patří uvolnění trhu a otevření hranic. Důsledkem těchto událostí byl nárůst počtu trestných činů, zvyšování objemu soukromého majetku, tak i rozvoj elektroniky a elektronických zabezpečovacích systémů, zvýšila se životní úroveň mnoha obyvatel a rovněž poptávka po ochraně jejich majetku. Rozsah služeb, které nabízejí bezpečnostní agentury je průběžně doplňován, modernizován a měněn dle potřeb a přání zákazníka.

1.1 Ochrana objektu

Soukromé bezpečnostní služby při ochraně majetku - objektu před narušením, vypracovaly různé formy ochrany těchto objektů. Mezi základní formy ochrany patří *klasická ochrana*. Mezi základní prvky klasické ochrany řadíme především mechanické zábranné systémy (dále jen MZS) a zařízení, jejichž primárním úkolem je odrazení pachatele, zamezení a zabránění vniknutí do objektu, znemožnění odcizení nebo poškození objektu, nebo aspoň tuto činnost na dostatečně dlouhou dobu oddálit.

Další formou ochrany jsou *režimová opatření,* která jsou založena na zavedení a uplatňování účinných bezpečnostních směrnic v chráněném objektu. Režimová ochrana představuje organizačně administrativní opatření, která směřují k zajištění předem stanovených a požadovaných podmínek pro správnou a smysluplnou funkci bezpečnostního systému a jeho sladění s provozem v chráněném objektu. Mezi základní opatření patří klíčový režim, režim vstupu a výstupu osob, režim pohybu osob a chráněných informací v objektu, vjezdu a výjezdu vozidel… Režimová opatření se

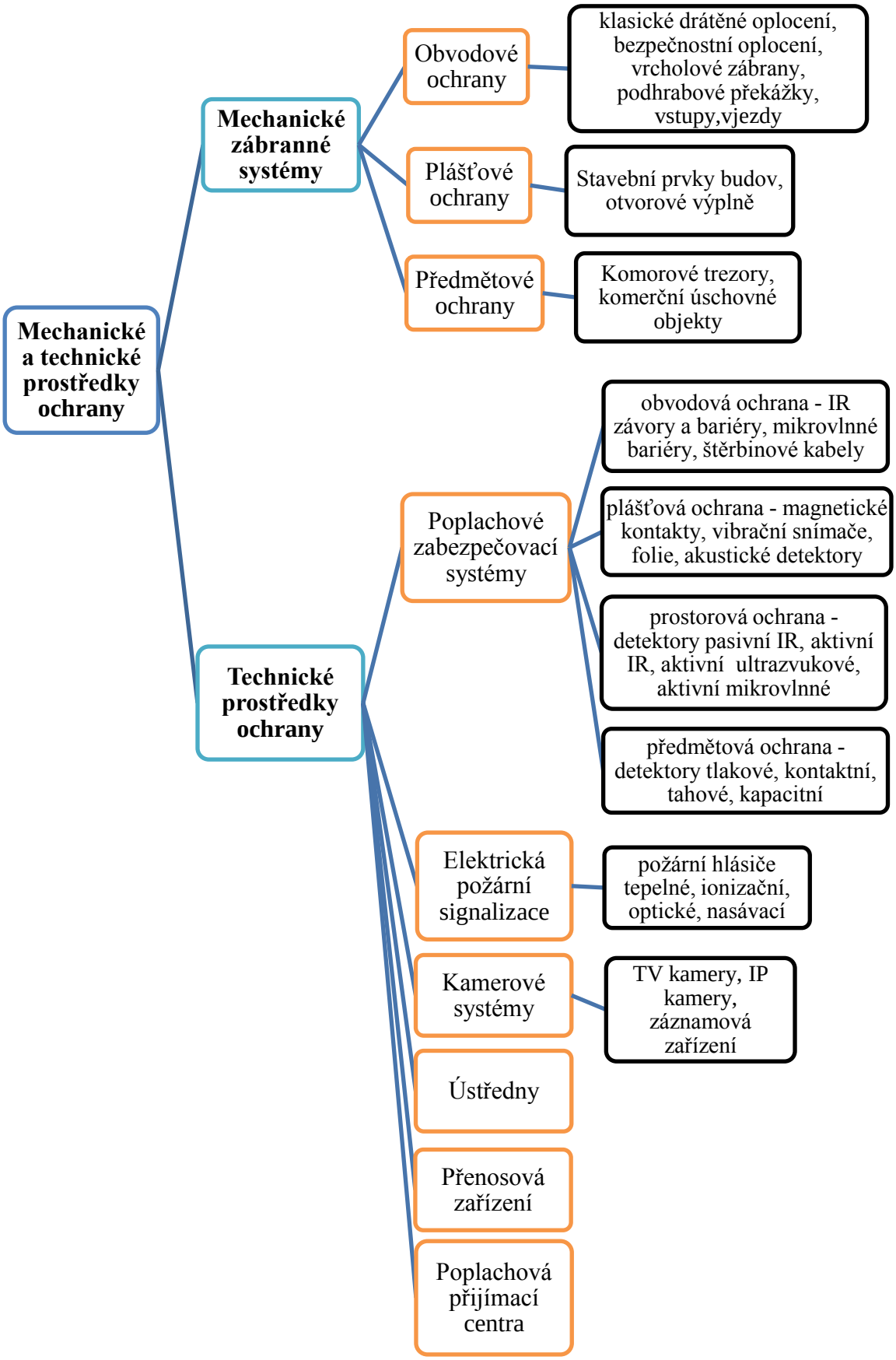
většinou uvádějí v provozním řádu objektu a měli by s nimi být seznámeny všechny pověřené osoby. Může obsahovat i seznam osob, které mají oprávnění vstupovat do objektu, nebo jeho částí. [3]

Dále zde patří *fyzická ochrana,* která je prováděna fyzickou ostrahou v objektu – živou silou. Do fyzické ochrany můžeme zařadit hlídací službu, vrátné, zásahovou jednotku, obsluhu přijímacího poplachového centra (dále jen PPC), policii apod. Aplikujeme-li ji při ochraně objektu, závisí na její úrovni výsledná činnost ostatních druhů ochrany. Ze všech druhů ochran je nejsložitější z hlediska organizace, výběru vhodných osob, jejich zaškolení atd., její režijní náklady jsou vysoké – zejména platy a taky se jedná o lidský faktor, který je zvyklý chybovat a může být zmanipulován. Proto pracovníci působící na úrovni této ochrany musí splňovat určité kvalifikační předpoklady zaměřené na psychickou a fyzickou stránku a znalost vybraných právních předpisů.[4]

A poslední a nejvýznamnější formou ochrany je *technická ochrana*. Do této ochrany spadají jak mechanické, tak elektronické systémy, které zabraňují, monitorují nebo detekují narušení bezpečnosti objektu. Mezi technickou ochranu patří již zmiňované mechanické zábranné systémy, dále elektrické zabezpečovací systémy (dále jen EZS), přístupové systémy, kamerové systémy, tísňové systémy atd. [5]

---

[3] ČANDÍK, Marek. *Objektová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-731-8217-3.
[4] ČANDÍK, Marek. *Objektová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-731-8217-3.
[5] ČANDÍK, Marek. *Objektová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-731-8217-3.



Obrázek 1: Rozdělení prostředků ochrany

1.2 Prostorové členění technické ochrany

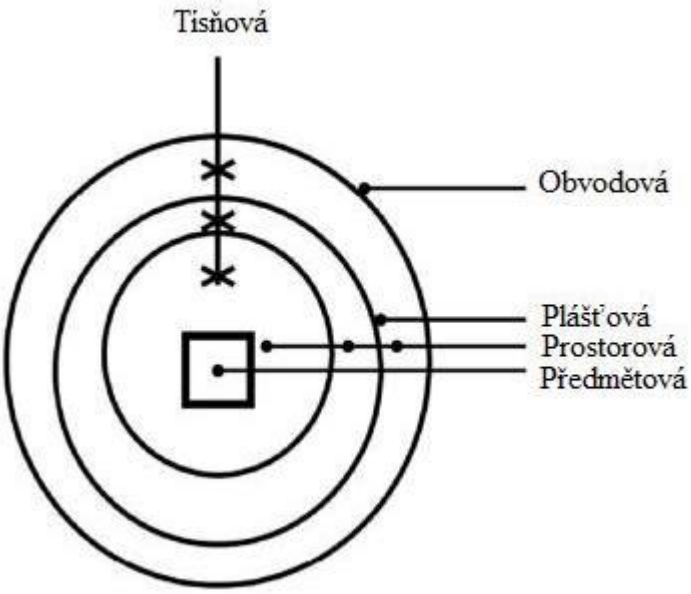
Technická ochrana se rozděluje do pěti základních okruhů ochranných zón:

- *obvodová ochrana:* rovněž se označuje jako perimetrická nebo venkovní. Zajišťuje bezpečnost vyhrazenému území a detekuje případné narušení obvodu objektu. Obvodem objektu máme na mysli jeho katastrální hranice, která je nejčastěji realizována přírodními nebo umělými bariérami (ploty, zdi, vodní toky, příkopy apod.). Při užití prvků poplachového zabezpečovacího systému je kladen důraz hlavně na odolnost těchto prvků proti falešným poplachům,[6]
- *plášťová ochrana:* zabraňuje a pak případně signalizuje narušení pláště budovy, objektu. Jedná se o zabezpečení vstupu do všech stavebních otvorů objektu (okna, dveře, šachty, střešní okna apod.). Plášťová ochrana se obvykle realizuje zevnitř objektu a označuje se rovněž jako objektová ochrana. K zajištění plášťové ochrany se používá převážně kombinace detektorů tříštění skla a magnetických kontaktů, které mohou být doplněny prvky MZS. U objektů s vyšším stupněm zabezpečení se používají i další prvky zabezpečení, jako otřesové detektory, které detekují případné otřesy stěn atd.,[7]
- *prostorová ochrana:* primárním účelem je signalizace změn v chráněném prostoru v objektu. Jedná se hlavně o prostory, kde se předpokládá pohyb pachatele. V případě, že dojde k narušení tohoto okruhu ochranné zóny, pachatel překonal plášť objektu a vnikl do vnitřních prostor objektu. Nejpoužívanější prvky této ochrany jsou pasivní infračervené detektory pohybu, případně jejich kombinace s jinými detektory – duální detektory, nebo doplněním o kamerový systém. Tato ochrana se označuje i jako pohybová ochrana,[8]
- *předmětová ochrana:* zabraňuje nebo detekuje poškozování, znehodnocování nebo neoprávněnou manipulaci s chráněnými předměty. Prvky této ochrany jsou především různá úschovná místa, jako trezory, bezpečnostní skříně apod. a detektory založené na principu detekce změn při manipulaci s chráněným

[6] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-80-7318-554-1 (BROž.).
[7] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-80-7318-554-1 (BROž.).
[8] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-80-7318-554-1 (BROž.).

předmětem – otřesová čidla, čidla na ochranu zavěšených předmětů, kapacitní čidla. Poplach může být vyhlášen pouhým přiblížením se pachatele k chráněnému předmětu, nebo manipulací s ním. Mezi zabezpečované předměty patří cennosti – šperky, vázy, obrazy, ale rovněž automobily, zemědělské stroje atd…,[9]

- *tísňová ochrana:* účelem této ochrany je signalizace ohrožení života napadením, zdravotní problémy nebo působení živlů uvnitř objektu (únik vody, plynu, požár atd.). Mezi prvky tísňové ochrany řadíme veřejné, skryté a osobní tísňové hlásiče.[10]



Obrázek 2: Prostorové členění technické ochrany[11]

[9] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-80-7318-554-1 (BROž.).
[10] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-80-7318-554-1 (BROž.).
[11] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-80-7318-554-1 (BROž.).

1.3 Legislativa a poplachový zabezpečovací systém

Zařízení poplachových zabezpečovacích systémů můžeme definovat jako soubor detektorů, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, zapisovacích zařízení a ovládacích zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru. Zařízení poplachových zabezpečovacích systémů slouží k signalizaci nebezpečí ve střeženém objektu, zejména o nežádoucím vniknutí do objektu. [12]

1.3.1 Normy

Technické normy jsou předpokladem technického pořádku v daném oboru na příslušné úrovni, tedy např. celosvětově, mezinárodně, národně, v rámci určitého sdružení apod. V oboru poplachových systémů začaly v 90. letech 20. Století vznikat na půdě evropských (CENELEC – Evropský výbor pro normalizaci v elektrotechnice) a světových (IEC – Mezinárodní výbor pro elektrotechniku) normalizačních organizací oborové standardy nabízející pro jednotlivé skupiny zařízení z oboru poplachových norem:

- řešení funkčních požadavků na jednotlivá zařízení,
- dále uvádějící metody zkoušení prokazující splnění těchto funkčních požadavků,
- požadavky na vlastnosti vztahující se k vlivům prostředí,
- metody zkoušení prokazující splnění klimatické odolnosti,
- systémové požadavky vztahující se k podmínkám nasazení těchto systémů,
- návody a doporučení na aplikaci poplachových systémů.

Evropské normy jsou produktem evropských normalizačních organizací. V případě poplachových systémů je to konkrétně technická komise CLC/TC79 a její pracovní skupiny. [13]

[12] ČSN EN 50 131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007.
[13] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4.

1.3.2 Změna normy 50 131-1 ed.2

Poplachové zabezpečovací systémy byly a jsou známé spíše pod „starým“ názvem elektronické zabezpečovací systémy (dále jen EZS). Původní norma ČSN EN 50131-1, (vešla v účinnost v roce 1999), byla nahrazena v roce 2009 na ČSN EN 50 131-1 ed.2. Až v této normě se rozlišují systémy pro detekci napadení a pro detekci vniknutí. V normě se vyskytuje zkratka IAS (Intruder Alarm System – poplachový systém pro detekci vniknutí), která byla používána i v předchozím vydání této normy. Další zkratka I&HAS (Intruder and Hold-up Alarm System – poplachový systém pro detekci vniknutí a přepadení. V normě se vyskytuje i zkratka HAS (Hold-up Alarm System – poplachový systém pro detekci přepadení. To jsou důvody, proč se v českém překladu vyskytují originální zkratky - I&HAS „poplachové zabezpečovací a tísňové systémy“, IAS pro „poplachové zabezpečovací systémy“ a HAS pro „poplachové tísňové systémy, místo dříve používaného EZS. Pro české texty byly uvedené zkratky nahrazeny: I&HAS = PZTS, IAS = PZS, HAS = PTS. Ve své práci se budu zabývat návrhem poplachového systému pro detekci vniknutí, tak budu dále ve své práci používat zkratku EZS.

1.3.3 Základní normy

Tabulka 1: Rozdělení norem poplachových systémů[14]

Číslo normy (řada)	Název
EN 50 130-x-y	Poplachové systémy
EN 50 131-x-y	Poplachové systémy – **Poplachové zabezpečovací a tísňové systémy**
EN 50 132-x-y	Poplachové systémy – **CCTV** sledovací systémy pro použití v bezpečnostních aplikacích
EN 50 133-x-y	Poplachové systémy – Systémy kontroly vstupu **(ACS)**
EN 50 134-x-y	Poplachové systémy – Systémy **přivolání pomoci**
EN 50 136-x-y	Poplachové systémy – Poplachové **přenosové systémy** a zařízení
EN 50 137-x-y	Poplachové systémy – Systémy **kombinované nebo integrované** *

*tato norma není v platnosti

Tabulka 2: Jednotlivé části norem[15]

Číslování normy (řada)	Oblast
ČSN EN 50 13x-1	**Systémové požadavky** (funkce, typy, kategorie, definice…)
ČSN EN 50 13x-2-4	Požadavky na **jednotlivé části systému** (např. detektory, ústředny + požadavky na zkoušky)
ČSN EN 50 13x-5	**Komunikace**, propojení
ČSN EN 50 13x-6	**Napájení**
ČSN EN 50 13x-7	**Pokyny pro aplikaci**

[14] ČSN EN 50 131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007.
[15] ČSN EN 50 131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007.

2 POPLACHOVÝ ZABEZPEČOVACÍ SYSTÉMY – SYSTÉMOVÉ POŽADAVKY

2.1 Stupně zabezpečení objektu

Stupeň zabezpečení stanovuje norma ČSN EN 50 131-1 ed.2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy. Stupeň zabezpečení objektu určujeme před samotným návrhem zabezpečení konkrétního objektu. Existují kritéria na výbavu a funkci jednotlivých komponentů, která stanovují stupeň daného zabezpečení a to z hlediska:

- přístupové úrovně,
- provozování,
- vyhodnocení,
- detekci,
- napájení,
- zabezpečení proti sabotáži,
- monitorování,
- propojení,
- záznamu události.

Stupeň zabezpečení jednotlivých komponent nebo celků je dán mírou rizika daného typem narušitele a prostředky, kterými disponuje při útoku na objekt. Stupeň zabezpečení jednotlivých komponentů je stanoven na certifikované zkušebně. Národní bezpečnostní úřad (dále jen NBÚ) pak na základě funkčních zkoušek vystaví certifikát s omezenou dobou platnosti.

Stupeň zabezpečení poplachového zabezpečovacího systému závisí na požadované úrovni zabezpečení, která se z pravidla stanovuje při posouzení objektu, nejlépe při obhlídce na místě. O stanovení rizika a základních požadavků na způsob zabezpečení se pořizuje záznam bezpečnostního posouzení objektu, který je podkladem pro zpracování příslušné dokumentace. Účastníky při pořizování bezpečnostního posouzení objektu jsou všechny zainteresované strany, tzn.: klient, projektant, montážní firma, dále to může být zástupce pojišťovny, člen sboru PČR, provozovatel poplachového přijímacího centra (dále jen PPC).

Tabulka 3: Stupeň zabezpečení objektu[16]

Stupeň zabezpečení	Míra rizika	Předpokládány typ narušitele	Použití
1	Nízké	Narušitel má malou znalost EZS; omezený sortiment snadno dostupných věcí	Rodinné domy, byty, chaty…
2	Nízké až střední	Narušitel má určité znalosti o EZS; omezený sortiment základních přenosných nástrojů	Komerční objekty
3	Střední až vysoké	Narušitel je obeznámen s EZS; úplný sortiment základních přenosných přístrojů a elektronických zařízení	Zbraně, ceniny, informace…
4	Vysoké	Narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí; kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků EZS	Objekty národního a vyššího významu

2.1.1 Volba stupně zabezpečení

Konečný stupeň zabezpečení se provádí několika způsoby a je ovlivněn několika faktory:

- volí si ji zákazník: předpokládá se, že zákazník je laik a hlavní roli zde hrají finanční možnosti zákazníka, s přihlédnutím na hodnotu zabezpečovaného majetku,
- doporučuje instalační firma: navrhuje technik instalační firmy, nebo příslušný projektant. Oba vycházejí hlavně z praktických zkušeností a doporučují nejvhodnější typ zabezpečení pro daný objekt a hodnotu zabezpečovaného majetku. Řídí se ale i požadavky klienta, či pojišťovny,
- stupeň zabezpečení je stanoven třetí stranou: v případě, že objekt má strategické, finanční nebo jiné využití, tak stanovuje příslušný stupeň zabezpečení NBÚ, Policie ČR, pojišťovna, vnitřní směrnice nebo norma.

[16] ČSN EN 50 131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007.

Se vzrůstajícím stupněm zabezpečení se zpřísňují i požadavky na jednotlivé komponenty systému (viz Tabulka 4.).

Tabulka 4: Doporučená ochrana objektu dle stupně zabezpečení

Ochrana objektu	Detekce	Stupeň zabezpečení objektu			
		1	2	3	4
Vstupy – otevření	MG kontakt	ano	ano	ano	ano
Vstupy – průnik	Prostorový detektor	vhodné	vhodné	ano	ano
Vstupy – uzamčení	Elektrický zámek	ne	ne	vhodné	ano
Okna – otevření	MG kontakt	ne	ano	ano	ano
Okna – průraz	Akustický detektor	ne	ano	ano	ano
Prostor chodeb	Prostorový detektor	ano	ano	ano	ano
Prostor místnosti	Prostorový detektor	vhodné	doporuč.	ano	ano
Stěny, stropy, podlahy	Otřesové čidlo	ne	ne	doporuč.	ano

2.2 Klasifikace prostředí

Výše zmiňovaná norma obsahuje ještě jednu důležitou kapitolu, a sice stanovení prostředí. Důležitá je pro zajištění správné činnosti komponentů EZS a každý komponent musí být zařazen do jednoho z následujících prostředí (viz Tabulka 5.). Požadavky na zkoušky vlivu prostředí na jednotlivé komponenty EZS jsou popsány v jednotlivých produktových normách.

Jednotlivé komponenty EZS musí správně pracovat, jsou-li vystaveny působení vlivů prostředí specifikovaným v níže uvedené tabulce. Pro každou z tříd je v tabulce uvedeno typické prostředí.

Tabulka 5: Klasifikace prostředí

Třída	Název	Popis prostředí	Rozsah
I	Vnitřní	Vytápěna obytná nebo obchodní místnost	+5°C až +40°C
II	Vnitřní všeobecné	Přerušovaně vytápěná nebo nevytápěná místnost (chodba, schodiště)	-10°C až +40°C
III	Venkovní chráněné	Prostředí vně budov, kde komponenty nejsou trvale vystaveny vlivům počasí (přístřešek)	-25°C až +50°C
IV	Venkovní všeobecné	Prostředí vně budov, kde komponenty jsou trvale vystaveny vlivům počasí	-25°C až 60°C

2.3 Přístupové úrovně

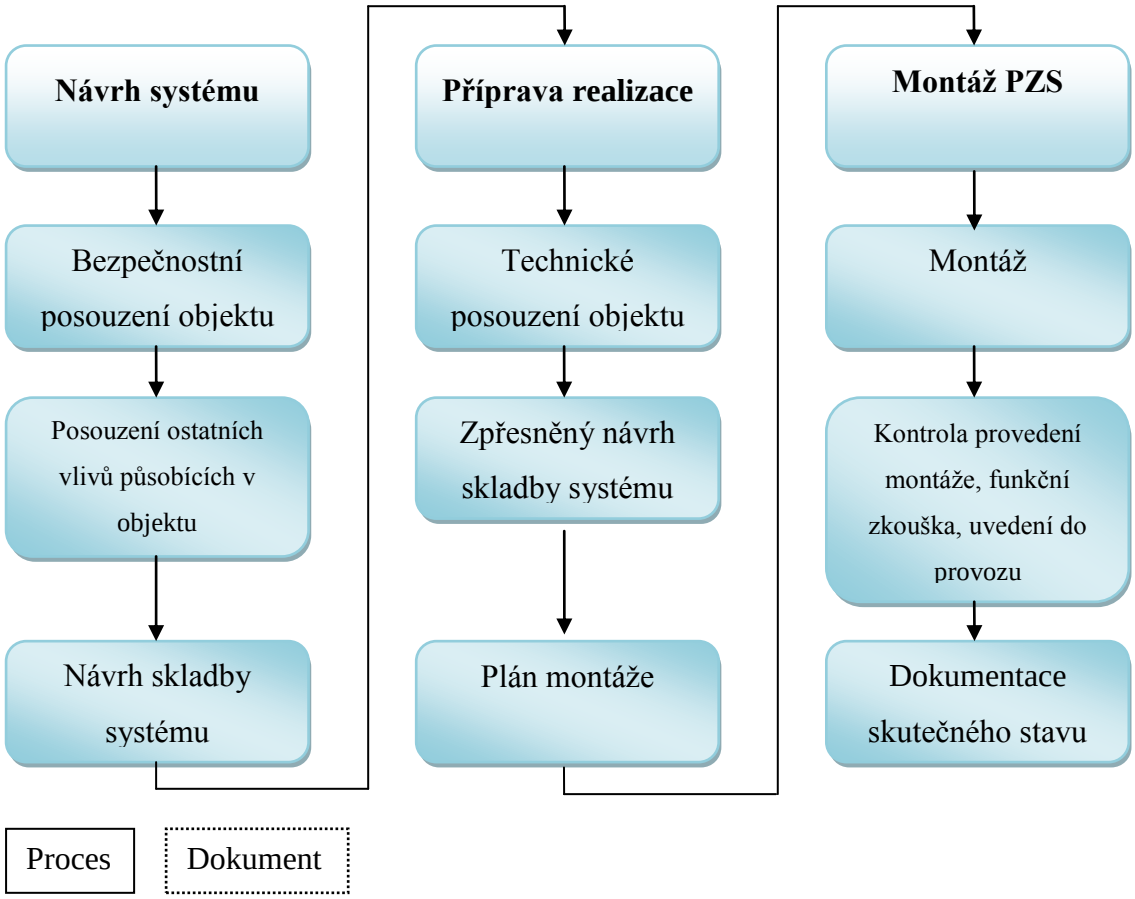
Norma specifikuje čtyři přístupové úrovně pro přístup uživatelů ke komponentům systému:

- úroveň 1: Přístup pro kohokoliv – přístup pro kohokoliv – funkce, u nichž je vyžadován přístup na úrovni 1, který nesmí mít žádná omezení přístupu,
- úroveň 2: Přístup pro uživatele (např. osobu obsluhující systém) – funkce, které ovlivňují provozní stav, aniž by došlo ke změně konfigurace systému. Přístup k funkcím na této úrovni musí být vymezen prostřednictvím klíče nebo kódové klávesnice, nebo zámku nebo dalšího ekvivalentního prostředku,
- úroveň 3: Přístup pro uživatele (např. servisní techniky) – všechny funkce ovlivňující konfiguraci EZS mimo zásahů do konstrukce zařízení,
- úroveň 4: Přístup pro uživatele (např. výrobce zařízení) – přístup k součástkám, které umožňují změnu konstrukce zařízení. Používá se především při výměně operačního systému.[17]

[17] ČSN EN 50 131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007.

3 ZŘIZOVÁNÍ ELEKTRICKÉHO ZABEZPEČOVACÍHO SYSTÉMU

Zřizování EZS a všechny další potřebné úkony vychází z norem ČSN CLC/TC 50 131-7 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – část 7: Pokyny pro aplikace a TNI 33 4591-1 Komentář k CLC/TC 50 131-7 – část 1: Návrh EZS.



Obrázek 3: Zřizování poplachových zabezpečovacích systémů

Norma uvádí tři etapy zřizování EZS:

- návrh systému,
- příprava realizace,
- montáž EZS.

Některé literatury ještě uvádí čtvrtou etapu, a sice trvalý provoz.

3.1 Návrh EZS

Prvním krokem při zřizovaní EZS je návrh systému. Jeho cílem je stanovit rozsah samotného systému EZS, včetně výběru komponentů příslušného stupně zabezpečení a třídy prostředí. Výstupem je dokument, který by měl obsahovat následující informace:

1. údaje o zákazníkovi – jméno, adresa a obchodní jméno + ostatní informace nutné pro identifikaci klienta,
2. údaje o střežených objektech – název a adresa střežených objektů, popis střežených objektů, účel využití objektů,
3. stupeň zabezpečení – stupeň navrženého EZS, stupeň jakýkoliv subsystémů,
4. třída okolního prostředí – třída prostředí každého komponentu,
5. seznam materiálu (přehled komponentů) – seznam typů zařízení, rozmístění všech zařízení (slovně nebo schematicky), stanovení předpokládaného pokrytí detektory pohybu,
6. konfigurace systému – podrobné informace o hlavních funkcích systému, postupy pro uvádění do jednotlivých stavů střežení/klid, postupy pro uvádění stavů střežení/klid v určitých částech systému, údaje o programování okruhů (noc, den, sabotáž),
7. hlášení poplachu – podrobné informace o navržených zařízeních pro ohlašování poplachu, způsob ohlašování poplachu, typ a umístění výstražných zařízení a komunikátorů, typ, umístění a název poplachového přijímacího centra,
8. legislativa – údaje o shodě prvků systému nebo EZS s požadavky místní nebo národní legislativy (zákon o snížení hluku, legislativy v oblasti elektromagnetického vyzařovaní, elektrické bezpečnosti…),
9. normy – údaje o shodě prvků systému nebo celého EZS s požadavky příslušných technických norem,
10. další právní předpisy – podrobné informace o shodě komponentů EZS s jakýmikoliv dalšími předpisy (směrnice pojišťoven, směrnice příslušných inspektorátů…),
11. certifikace – podrobnosti prohlášení o certifikaci komponent, podrobnosti prohlášení o certifikaci EZS,
12. zásah – plánovaná odezva na aktivaci poplachu nebo poruchy (policie, zásahové služby, servisní organizace…),

13. údržba – doporučení pro pravidelnou údržbu EZS nebo jednotlivých komponent, podrobnosti o četnosti servisních prohlídek, seznam prací, které je nutné při každé prohlídce provést,
14. opravy – podrobné údaje o servisní firmě, jména kontaktních osob, denní telefonní čísla, kontakt na 24 hodinový servis.[18]

Pro zpracování takového dokumentu je potřeba znát informace o chráněném objektu včetně vlivů, které na něj působí vevnitř i mimo něj a další faktory, které působí na objekt z hlediska bezpečnosti. Tyto informace získáme pomocí bezpečnostního posouzení objektu, který popisují výše zmiňované normy. Nebo můžeme provést bezpečnostní analýzu, která je rozsáhlejší a zahrnuje více aspektů. Bezpečnostní analýza zahrnuje i metody analýzy rizik, které se používají především pro rozsáhlejší systémy.

3.2 Bezpečnostní posouzení

Bezpečnostní posouzení je prvním krokem etapy samotného návrhu systému zabezpečení daného objektu. Jeho cílem je stanovit rozsah systému, východiska pro volbu komponentů, stupeň zabezpečení, určit pojistnou třídu, třídu prostředí a navrhnout samotné řešení systému.

Účelem bezpečnostního posouzení je odhalit v průběhu přípravy systémového návrhu faktory, které mají vliv na volbu komponentů a jejich umístění. Další faktory mohou být odhaleny v průběhu technického posouzení objektu.

3.2.1 Obecný obsah bezpečnostního posouzení

Při posuzování objektu a volby vhodného stupně zabezpečení jsou důležité tyto aspekty:

1. zabezpečované hodnoty (majetek),
2. stavební dispozice (konstrukce, umístění, osídlení),
3. minimálně úroveň střežení EZS,
4. zpracovatel odhadne očekávaný způsob narušení v jednotlivých místnostech objektu a dle toho stanoví stupeň zabezpečení a skladbu systému,

[18] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.

5. ostatní vlivy – nutno posuzovat stávající a potencionální podmínky ve střežených prostorách
   a) vlivy uvnitř střežených prostor ovlivnitelné uživatelem systému,
   b) vnější vlivy.

Bezpečnostní posouzení provádí buď zástupce dodavatele a to za účastí zákazníka nebo Policie ČR, zástupce pojišťovny či provozovatele PPC. Nebo bezpečnostní posouzení provede třetí nezávislá osoba, kterou může být bezpečnostní konzultant, soudní znalec nebo akreditovaná osoba.

Řada ustanovení ČSN CLC/TS 50131-7 neposkytuje podrobný návod na postup činnosti v rámci etap návrhu sytému a neobsahuje odkazy na národní legislativu. TNI 33 4591-1 doplňuje, upřesňuje možnosti řešení, zejména u rozsáhlejších systémů. Výstupem je Zápis o bezpečnostním posouzení objektu**,** který obsahuje: druh a rozsah majetku, struktura objektu, vlivy na objekt (vnější, vnitřní), stanoveni pojistných tříd, stanoveni stupně zabezpečeni, klasifikace prostředí, stanoveni typu ochrany, způsob předání poplachové informace, speciální požadavky (speciální detektory), zvláštní opatřeni (vzhledem k předcházejícím krádežím).

3.2.2 Bezpečnostní posouzení – zabezpečované hodnoty

Bezpečnostní posouzení (dle *ČSN CLC/TS 50131-7 Poplachové systémy- Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace*. Příloha B).

I. Bezpečnostní posouzení objektu – zabezpečované hodnoty ⇒ Míra rizika vloupáni do střeženého objektu závisí na charakteru střeženého majetku. Bereme v úvahu faktory:

1. druh majetku (Aktivum): snadnost zpeněženi, atraktivita pro pachatele, nebezpečni vloupáni,
2. hodnota majetku: maximální hodnota, přímé ztráty, následné výdaje související se ztrátou, osobni vztah k jednotlivým položkám majetku,
3. objem majetku: snadnost/náročnost odcizeni a přepravy (počítač /turbina), tržní atraktivnost, zpeněženi, snadnost přístupu do střežených prostor (budova, areál, komunikace, vrátnice),

4. historie krádeží (četnost a způsoby předcházejících incidentů),
5. nebezpečí: zneužiti střeženého majetku, nebezpečni majetku pro okolí a pro osoby,
6. poškození (vandalismus, žhářství, reakce postižených osob).[19]

3.2.3 Bezpečnostní posouzení – budova

Bezpečnostní posouzení (dle ČSN CLC/TS 50131-7 Poplachové systémy- Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace. Příloha C).

II. Bezpečnostní posouzení objektu – budova ⇒ V rámci posuzování rizik jednotlivých hrozeb jako podklad ke zpracování systémového návrhu zabezpečeni je podstatným faktorem fyzická struktura objektů. Cílem je identifikace slabých míst v rámci Stavební dispozice objektu.

1. konstrukce (stěny, střecha, podlahy, stropy, sklepy),
2. otvory (okna, dveře, střešní světlíky, ventilační vstupy, další časti pláště budovy jako šachta, vstup výtahu),
3. provozní režim objektu (doba osídlenosti objektu, přítomnost ostrahy, přistup veřejnosti, návštěvy, doprava),
4. držitelé klíčů (přistup, dosažitelnost, evidence, uloženi),
5. lokalita
   - riziko kriminality v oblasti, sousední budovy a jejich vliv (např. vloupání),
   - rychlost reakce na signalizaci poplachu, zásah, vzdálenost (vztah) sousedních obydlených objektů,
6. stávající zabezpečení**:** kvalita a rozsah mechanického zabezpečovací zařízeni a EZS,
7. historie krádeží, loupeží, výhružek (počet předcházejících incidentů, způsob jejich realizace),
8. místní legislativa a předpisy (bezpečnostní požadavky, požární předpisy, požadavky vzhledem ke konstrukci objektu),
9. prostředí střeženého objektu (městská zástavba, venkov, přírodní překážky, nadmořská výška, reliéf krajiny).[20]

---

[19] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.

3.2.4 Bezpečnostní posouzení – vlivy působící na zabezpečovací systém a mající původ ve střeženém objektu

Bezpečnostní posouzení (dle ČSN CLC/TS 50131-7 Poplachové systémy- Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace. Příloha D).

III. Bezpečnostní posouzení objektu – vlivy působící na zabezpečovací systém a mající původ ve střeženém objektu

- faktory ovlivňující výběr, umístěni a nastaveni komponentů (zejména detektorů),
- ovlivnitelné uživatelem,

1. vodovodní potrubí: vliv pohybu vody v plastových potrubích (nasazeni mikrovlnných detektorů),
2. vytápění, vzduchotechnika, klimatizace: vliv turbulence vzduchu (např. nasazeni ultrazvukových detektorů),
3. vývěsní štíty, závěsní předměty: vliv zavěšených předmětů s možnosti pohybu v zorném poli detektorů (záclony, rostliny, lampy, reklama),
4. výtahy: vliv vibraci strojních zařízeni (např. otřesová čidla),
5. zdroje světla
   - kompaktní výbojky, zářivky ⇒ rušeni mikrovlnných detektorů,
   - bodové reflektory ⇒ nasměrované na čočky (zrcadla) PIR detektorů,
   - vliv světlometů vozidel,
6. elektromagnetické rušení,
7. vnější zvuky: v případě nasazeni ultrazvukových detektorů, příklad: telefonní zvonky, vzduchová potrubí (netěsnosti), kompresory,
8. domácí zvířata: vliv na detektory pohybu,
9. průvan: citlivost detektorů na proudění vzduchu
   - ultrazvukové detektory - zvuk jako medium pro přenos energie,
   - PIR – př. rychle změny teploty (tepelný šok - aktivace poplachu),
   - těsnění stavebních otvorů,
   - závěsné, pohybující se předměty jako plakáty, rostliny, závěsy,

---

[20] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.

10. uspořádání skladovaných předmětů ⇒ z hlediska zastínění zorného pole detektoru, možnost uvolněni předmětů a jejich následný pohyb,
11. stavební konstrukce střežených objektů (střechy, stěny, podlahy, sklepy, lehké stavební materiály – vibrace, stav a usazeni dveří, oken),
12. umístění detektorů na zasklení
    - typ - konstrukce skla (ploché, zvýšená pevnost, vrstvené, dvojité zaskleni),
    - možnost vyjmuti skla z rámu,
    - teplotní rozdíly na povrchu skla ⇒ kondenzace vody,
13. riziko planých poplachů u tísňových zařízení - volba umístěni detektorů z hlediska pohybu osob (aktivace dětmi).[21]

3.2.5 Bezpečnostní posouzení – vlivy působící na zabezpečovací systém a mající původ vně střeženém objektu

Bezpečnostní posouzení (dle ČSN CLC/TS 50131-7 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace. Příloha E).

IV. Bezpečnostní posouzení objektu – vlivy působící na zabezpečovací systém a mající původ vně střežených objektů ⇒ obecně faktory bez možnosti ovlivněni uživatelem objektu, volba typů komponent a jejich umístěni.

1. dlouhodobě působící faktory: nepředpokládáme změnu (řadově roky), silnice, železnice, metro, parkoviště, letecky koridor, seizmická rizika – podloží,
2. krátkodobě působící faktory: výstavba,
3. vlivy počasí: převažující a potencionální vlivy počasí, exponovaná místa - vítr, deště, pobřeží, kopce, blesky,
4. vysokofrekvenční rušení: vysilače TV, vysílače rádia, základnové stanice GSM, radary, vliv na bezdrátové komponenty EZS,
5. sousední objekty (vibrace, EM rušeni, průmyslové objekty),
6. vlivy klimatických podmínek: výběr zařízeni odpovídající místnímu klimatu (např. teplota, vlhkost),

[21] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.

7. ostatní vnější vlivy: aktivity v přístupných vnějších částech objektu a aktivity v přilehlých částech rozsáhlejších komplexů budov, hrající si děti, kulturní a sportovní akce.[22]

3.3 Bezpečnostní analýza

Bezpečnostní analýza je metoda, při níž se zavádí dekompozice objektu na základní prvky, vyhledává se a zkoumá vnitřní zranitelnost, vnější hrozby a implementované ochranné mechanismy, působící na jednotlivé prvky ve zvolených vrstvách bezpečnosti: počítačové, komunikační, fyzické, personální, administrativní, organizační.

Cílem bezpečnostní analýzy je identifikovat maximum zranitelností a nedostatků obsažených ve zkoumaném objektu, odhadnout hrozby, rizika a možné negativní dopady na zkoumaný objekt a určit efektivitu a funkčnost stávajících ochranných mechanismů a navrhnout nové tak, aby byla všechna rizika efektivně snížena nebo pokryta na akceptovatelnou úroveň.[23]

3.3.1 Analýza rizik

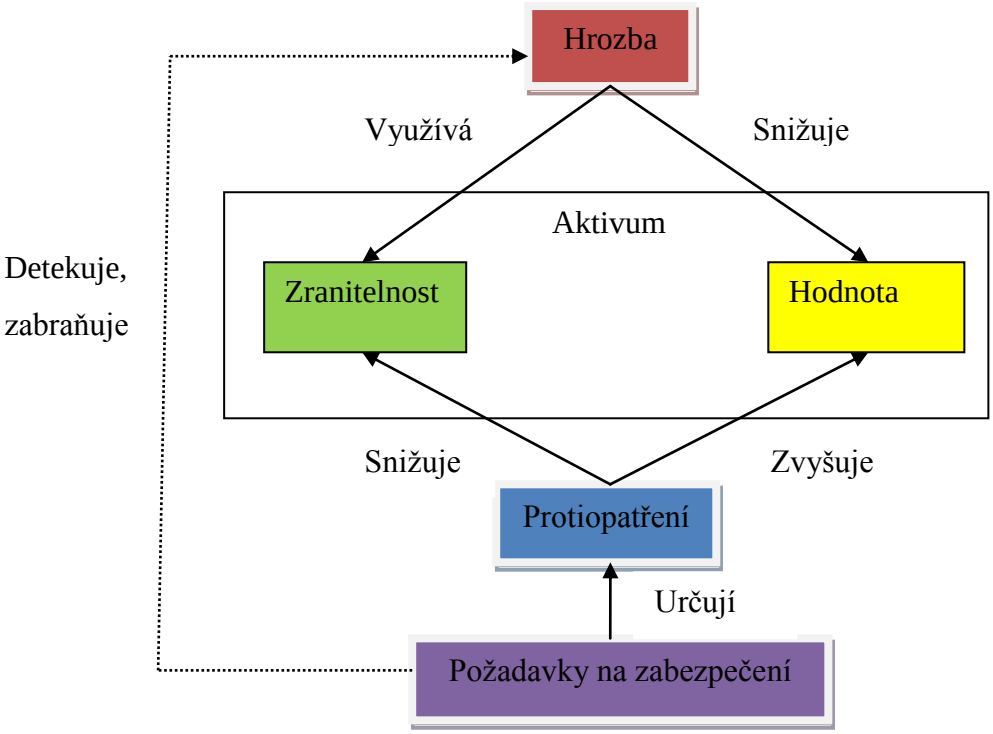
Součástí kvalifikované bezpečnostní analýzy je i analýza rizik. Analýza rizik se chápe jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a jejich dopadu na aktiva, čili stanovení rizik a jejich závažnosti. Při analýze rizik používáme tyto pojmy:

- hrozba: je síla, událost, aktiva nebo osoba, která může způsobit škodu. Hrozba využije zranitelnosti, překoná protiopatření a působí na aktivum, kde způsobí škodu. Hrozba působí jednak přímo na aktivum nebo na protiopatření, s cílem získat přístup k aktivu,
- protiopatření: je postup, proces, technický prostředek, co je nevrženo proti zmírnění působení hrozby, snížení zranitelnosti nebo dopadu hrozby. Protiopatření chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva,
- aktivum: vše, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Aktiva dělíme na hmotná a nehmotná. Vůči působení hrozby se aktivum

[22] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.
[23] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.

vyznačuje určitou zranitelností a je zároveň chráněno protiopatřeními před těmito hrozbami,

- zranitelnost: je nedostatek analyzovaného aktiva, kterým může dojít k naplnění hrozby. Zranitelnost je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby,
- riziko: pravděpodobnost nebo možnost vzniku ztráty. Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby.[24]



Obrázek 4: Vazby v analýze rizik[25]

[24] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.
[25] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.

Hrozba využívá zranitelnosti, překonává protiopatření a působí na aktivum, kde způsobí škodu. Aktivum má určitou hodnotu a tím motivuje člověka – pachatele k aktivaci hrozby. Aktivum se vyznačuje určitou zranitelností vůči působené této hrozby. A naopak, aktivum je chráněné protiopatřeními před hrozbami. Protiopatření pak chrání aktiva, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva. Jejich další úlohou je samotné odrazování od aktivování hrozeb. Hrozba pak působí jednak přímo na aktivum, nebo na protiopatření, s cílem získat přístup k aktivu. Hrozba musí být aktivována, aby mohla působit, a pro svou aktivaci vyžaduje zdroje. Pravděpodobnost, že hrozba přejde v událost, se nazývá rizikem. Pravděpodobnost stanovujeme na základě některé z metod analýzy rizik.

4 ELEKTRICKÉ ZABEZPEČOVACÍ SYSTÉMY

EZS jsou komplexem technických prvků, které slouží k detekci nebo rozpoznání nežádoucí osoby a tuto skutečnost určitým způsobem signalizovali a dále informovali pověřenou osobu o této skutečnosti. Jejich primárním účelem není zabránit nežádoucí osobě ve vstupu do chráněného objektu, jak je tomu u mechanických zábranných systémů, ale na tento vstup upozornit. Proto je vhodné tyto dva systémy kombinovat.

Hlavní částí celého systému je ústředna, která monitoruje a vyhodnocuje stavy příslušných detektorů v objektu a v případě narušení poslala informaci o této události dále a vyhlásila poplach. EZS musí obsahovat:

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

4.1 Jednotlivé komponenty systému

4.1.1 Ústředny EZS

Ústředny jsou jádrem celého systému EZS, jejich základní funkce jsou:

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

Ústředny EZS dělíme do čtyř skupin podle způsobu připojení smyček:

1. analogové ústředny,
2. sběrnicové ústředny (ústředny s přímou adresací čidel),
3. koncentrátorové ústředny,
4. ústředny s bezdrátovým přenosem.

4.1.2 Detektory EZS

Detektory slouží k detekci narušení objektu. Detektory jsou zařízení, která reagují na fyzikální změny tak, že převádí vstupní fyzikální veličiny na jinou výstupní fyzikální veličinu. Dojde-li k narušení objektu, nastane změna vstupního signálu (jejího parametru), která způsobí změnu parametru výstupní fyzikální veličiny a ta je následně zpracována a vyhodnocena.

Základní členění detektorů v systému EZS je podle druhu ochranné zóny, které vychází z prostorového členění technické ochrany.

- Prvky obvodové ochrany:
  - mikrofonické kabely,
  - infračervené závory a bariéry,
  - mikrovlnné bariéry,
  - štěrbinové kabely,
  - zemní tlakové hadice,
  - perimetrické pasivní infračervené detektory.
- Prvky plášťové ochrany:
  - magnetické kontakty,
  - detektory tříštění skla,
  - vibrační detektory,
  - drátový senzor.
- Prvky prostorové ochrany:
  - pasivní infračervený detektor,
  - aktivní infračervený detektor,
  - ultrazvukový detektor,
  - mikrovlnný detektor,
  - kombinované duální detektory.
- Prvky předmětové ochrany:
  - otřesový senzor,
  - senzor na ochranu zavěšených předmětů,
  - kapacitní senzor.

4.1.3 Detektory prostředí

Součástí systémů EZS jsou i detektory, které slouží jako ochrana proti hrozbám pocházející především z prostředí uvnitř objektu. Jedná se o hlásiče požárů, které již jsou povinny zavádět v novostavbách. Dále existuje mnoho druhů prostředí, které jsou určeny pro detekování a snímání různých druhů látek a veličin. Detektory prostředí dělíme na:

- hlásiče požáru:
    - teplotní hlásiče,
    - ionizační hlásiče kouře,
    - optické hlásiče kouře,
    - multisenzorové hlásiče s využitím plynové detekce,
    - optické hlásiče plamene,
    - lineární tepelné detektory,
- detektory úniku plynu,
- detektory teploty,
- detektory vlhkosti,
- detektory zaplavení,
- detektory stavu elektroinstalace atd…

4.1.4 Signalizační zařízení

Mezi výstupní prvky EZS patří signalizační zařízení, které v případě narušení objektu opticky nebo akusticky signalizují toto narušení. Mezi nejběžnější patří akustická signalizace, tzv. siréna, jejíž součástí může být i optická signalizace – maják. Tato zařízení mají spíše psychologický efekt a z toho důvodu by se měly instalovat na viditelná, ale zároveň obtížně dostupná místa.

4.1.5 Poplachové přenosové systémy

V případě narušení objektu a vyhlášení poplachu musí ústředna tuto informaci předat dál a to pověřené osobě, majiteli objektu, nebo přímo na poplachové přijímací centrum. Předání této informace se uskutečňuje právě pomocí poplachových přenosových systémů, které zahrnují sítě a zařízení pro přenos informací. Pro předání informací používáme následující přenosové cesty:

- telefonní linky,
- GSM brány,

- radiové sítě,
- internetová spojení,
- vyhrazené přenosové cesty.

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

4.1.6 Ovládací zařízení

Ovládací zařízení slouží k ovládání celého systému EZS, uvádí systém do stavu střežení a do stavu klidu. Existují nejrůznější provedení ovládacích zařízení, volíme je podle stupně zabezpečení a podle požadavků zákazníka. Jejich základní funkce jsou:

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

Ovládací zařízení se umisťují co nejblíže ke vstupním dveřím, aby uživatel bez problémů a ve vymezeném čase mohl objekt odstřežit nebo zastřežit. Mezi ovládací zařízení patří kódové klávesnice, čtečky identifikačních karet, blokovací zámky či spínací zámky.

4.1.7 Napájecí zdroje

K uvedení systémů do činnosti jsou zapotřebí napájecí zdroje, které napájí celý systém EZS elektrickou energií a to i v případě výpadku napájecího napětí ze sítě. Z tohoto hlediska dělíme napájecí zdroje na základní napájecí zdroje a na náhradní napájecí zdroje. Jedná-li se o rozsáhlý systém EZS, používáme ještě přídavné síťové napájecí zdroje s vlastním náhradím zdrojem napětí.

Základní napájecí zdroj musí být schopen dodávat taková proud, který je součtem proudových odběrů všech prvků v systému včetně ústředny. Základní napájecí zdroj musí být schopen dobíjet připojený akumulátor během doby stanovené v související normě. Náhradní napájecí zdroj musí být schopný překonat nejdelší výpadek základního zdroje dle požadavků normy.

Norma rozlišuje tři typy napájecích zdrojů:

- typ A – základní napájecí zdroj (síťový zdroj) a náhradní napájecí zdroj dobíjený (dobíjený akumulátor),
- typ B – základní napájecí zdroj a náhradní napájecí zdroj nedobíjený (akumulátor nedobíjený),
- typ C – základní zdroj napájení s omezenou kapacitou (baterie).

4.1.8 Kabeláž

V systému EZS se používají následující čtyři druhy vedení:

- napájení AC – jištěný přívod z rozvaděčů o napětí 230V a průřezu 1,5 Cu,
- napájení 12 V – je určeno pro napájení detektorů a ostatních komponentů EZS. Jedná se o napájení z výstupu ústředny nebo pomocného zdroje,
- zóny – jedná se o vedení, na kterém je nízké napětí zpravidla kolem 5 V. Nesmí dojít k souběhu se silovým vedením a umístění s telefonním nebo síťovým kabelem,
- BUS – mezi ústřednou a klávesnicí je přenos dat typu sběrnice. Sběrnice nesmí mít souběh se silovým vedením a nesmí být ve společném kabelu s jiným vedením.

II. PRAKTICKÁ ČÁST

5 VÝBĚR A POPIS OBJEKTU

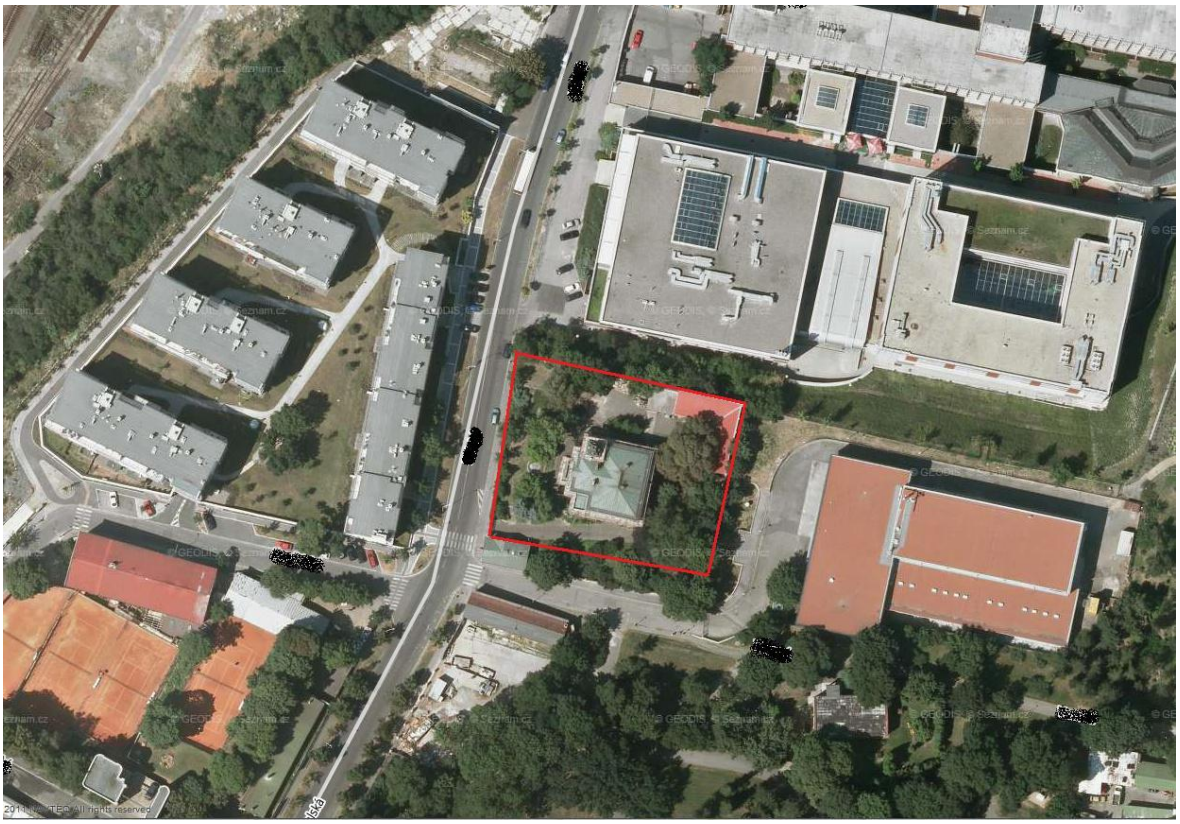
Předmětem diplomové práce je návrh a realizace zabezpečení víceúčelového objektu. Ve své diplomové práci spolupracuji s bezpečnostní firmou, která sama provádí návrhy a instalaci elektrického zabezpečovacího systému, a tato firma byla vybrána na zabezpečení daného objektu. Vzhledem k tomu, že v dané firmě pracuji na částečný úvazek, domluvil jsem se s vedením této firmy a za souhlasu samotného vlastníka, navrhl sám několik možností zabezpečení víceúčelového objektu. Z důvodu bezpečnosti však nebudu uvádět přesnou adresu vybraného objektu, ani přesnou jeho lokalitu. Při návrhu zabezpečení je nutné stanovit stupeň zabezpečení, a proto budu pracovat s konkrétními údaji a reálným stavem daného objektu s tím, že neuvedu ve své práci údaje, které by mohly vést k identifikaci daného objektu. Na výběru stupně zabezpečení měly značný vliv i požadavky vlastníka a předem stanovený rozpočet na zabezpečení objektu.

Daný víceúčelový objekt má dvě patra. V přízemí objektu se nachází prodejna informačních technologií, ať už softwaru či hardwaru. Dále se zde nacházejí kanceláře a reprezentační místnost. Ve druhém patře je zasedačka s balkónem pro různé konference a porady, sekretariát a kancelář pro vedení firmy a navíc pokoj na spaní. Hlavním přáním zákazníka bylo zabezpečit daný objekt, aniž by byly prováděny jakékoliv stavební práce, které by umožnili skrýt případnou kabeláž EZS – objekt je starý a řadí se mezi památky, čili bylo nutné zvolit bezdrátové zabezpečení. Dalším požadavkem zákazníka bylo, aby bylo možné zakódovat celý objekt, popřípadě celý objekt bez pokoje na spaní, koupelny a záchodu, čili v zásadě horní patro rozdělit na půlky. V objektu totiž často přespávají jak zaměstnanci z jiných poboček, nebo důležité návštěvy a je nutné, aby objekt byl zabezpečen a nocležník se nedostal do kanceláří či prodejny.

5.1 Umístění objektu

Vybraný objekt se nachází v hlavním městě Praha, v městské části Žižkov. Přímo naproti objektu přes ulici se nachází nové luxusní byty, z jedné strany objektu se nachází restaurace a vysoká škola, z druhé strany objektu se nachází sady. Vedle objektu, ze strany sadů, se nachází slepá ulice, která vede k jedné firmě, která sídlí za naším objektem. V blízkosti objektu, cca 1km je poliklinika. Velikou výhodou je, že 700m od objektu se nachází oddělení hlídkové služby Policie ČR a 1,1km obvodní ředitelství městské policie. Hasičská stanice 1,2km. Dojezdnost těchto složek je v řádu minut.

Obrázek 5: Obecná mapa objektu



Obrázek 6: Letecká mapa objektu

5.2 Popis objektu

Jak jsem již zmínil výše, jedná se o víceúčelový objekt o dvou patrech. Objekt je zabezpečen obvodovou ochrannou, na jižní a západní části areálu je vybudována vysoká zeď, na které se nachází obvodové oplocení, s betonovými sloupy a mřížemi. Východní a severní část je zabezpečená jen obvodovou zdí, která slouží jako oplocení. Jako vstup do areálu slouží velká železná brána, která má na svém vrcholu „ostny“. Vedle této brány, která je určena pro vjezd aut, je i malá vstupní železná branka podobných rozměrů. V areálu objektu se nachází mnoho vegetace, která roste i po plotě, čímž je zhoršena viditelnost jak do areálu, tak i z areálu a případnému narušitele dává možnost se skrýt, nebo pomocí této vegetace se do areálu dostat, případně i do objektu.

Plot je v dobrém stavu a nenachází se v něm žádná skulinka, kterou by šlo nepozorovaně vniknout do objektu. Skrz tento plot se do objektu nedostane ani žádné zvíře, jediná možnost překonání plotu je ho přelézt. Z hlediska mechanického obvodového zabezpečení je vše na dostatečné úrovni.

Obrázek 7: Vysoká zeď s plotem

Obrázek 8: Plot

Obrázek 9: Vstupní brána

Samotný objekt je postaven z cihel a má spoustu oken. Jak již bylo několikrát zmíněno, je dvoupatrový a má i balkón.

Obrázek 10: Pohled na objekt

Obrázek 11: Boční pohled na objekt

Z důvodu, že je objekt starý a řadí se mezi památkově chráněné budovy hlavního města Prahy, nelze jej zrekonstruovat tak, aby byly splněny všechny bezpečnostní požadavky. Hlavní slabinou objektu jsou staré dřevěné dveře, které vidíme na obrázku níže. V objektu není nainstalován žádný bezpečnostní systém.

5.3 Bezpečnostní posouzení objektu

I. Bezpečnostní posouzení objektu – zabezpečované hodnoty ⇒ Míra rizika vloupáni do střeženého objektu závisí na charakteru střeženého majetku. Bereme v úvahu faktory:

1. druh majetku:
   - IT technologie (počítače, notebooky, multifunkční tiskárny, projektor),
   - software,
   - lednička, televize, telefony, rádio, vybavení kuchyně (kávovar, mikrovlnná trouba...).
2. hodnota majetku: bráno mimo nábytek
   - prodejna: do 500 000 Kč,
   - kanceláře: do 450 000Kč,
   - kuchyně: do 40 000 Kč,
   - ostatní: do 70 000 Kč.
3. objem majetku:
   - snadnost/náročnost odcizeni a přepravy: ano – vesměs malé až střední věci, lehké,
   - tržní atraktivnost, snadnost zpeněžení: ano.
4. historie krádeží:
   - nízká kriminalita v okolí, žádná předchozí loupež ani vloupání do objektu.
5. nebezpečí zneužiti střeženého majetku:
   - ano: software, osobní údaje o zákaznících.
6. poškození (vandalismus):
   - hrozí hlavně na perimetru – poškození zdi a plotu.

II. Bezpečnostní posouzení objektu – budova ⇒ V rámci posuzování rizik jednotlivých hrozeb jako podklad ke zpracování systémového návrhu zabezpečeni je podstatným faktorem fyzická struktura objektů. Cílem je identifikace slabých míst v rámci stavební dispozice objektu:

1. konstrukce:
   - venkovní a vnitřní zdivo,
   - podlahy betonové,
   - střecha plechová,
   - sklepy: ano – mříže na oknech,
2. otvory:
   - dveře: staré, dřevěné, dvoukřídlé s okenními tabulemi,
     - vstup do sklepa: velké, kovové dveře se zámkem a petlicí,
     - jedny balkónové dveře – dřevěné,
   - okna: staré, dřevěné, nad nimi ještě malé – všechny otvíratelné,
     - sklepní: malé s mřížemi,
     - střešní světlík: ne,
3. provozní režim objektu:
   - doba osídlenosti: pracovní doba od 7 do 17 hod,
     - možnost přespání,
   - přítomnost ostrahy: ne,
   - přístup veřejnosti, návštěvy: ano – do prodejny, zasedačky,
4. držitelé klíčů (přistup, dosažitelnost, evidence, uloženi):
   - jen zaměstnanci a vedení, od bytu v sekretariátu,
5. lokalita:
   - častý pohyb osob,
   - v blízkosti Policie ČR i městská policie (dojezdní doba krátká, vzdálenost kolem 1km),
   - při stupu do areálu luxusní nové byty – velké osvětlení, dobrá viditelnost,
6. stávající zabezpečení**:**
   - mechanické zábranné systémy:
     - kvalitní obvodová ochrana – dostatečně velký a pevný plot – nelze podhrabat, těžko přelézt bez žebříku atd.,
     - zámky ve dveřích a petlice na dveřích do sklepa,
     - mříže na sklepních oknech,
   - doposud žádné prvky EZS,
7. prostředí střeženého objektu:
   - v blízkosti nové luxusní byty, vysoká škola, restaurace, park,

- možnost zpozorování neoprávněného vniknutí do střeženého objektu ze sousedních objektů: z velké části ano,
- riziko kriminality v lokalitě objektu: malé,
- možnost usnadnění vloupání ze sousedních objektů: ne.

III. Bezpečnostní posouzení objektu – vlivy působící na zabezpečovací systém a mající původ ve střeženém objektu:

1. vodovodní potrubí: kovové,
2. vytápění, vzduchotechnika, klimatizace:
   - plynový kotel,
   - topení v každé místnosti,
   - bez pevné, zabudované klimatizace,
3. vývěsní štíty, závěsní předměty: záclony a rostliny,
4. výtahy: ne,
5. zdroje světla:
   - zářivky,
   - vliv světlometů vozidel: ne – vysoký plot, velká vzdálenost objektu od cesty,
6. elektromagnetické rušení: ne,
7. domácí zvířata: ne,
8. průvan: ne,
9. skladování hořlavých nebo výbušných materiálů: ne.

IV. Stanovení stupně zabezpečení:

- vzhledem účelu objektu, výše a druh zabezpečovaných hodnot, lokalitě a blízkosti bezpečnostních sborů, byl stanoven stupeň zabezpečení 2 – nízké až střední riziko.

V. Klasifikace prostředí:

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

VI. Stanovení typu ochrany:

- na ochranu objektu bude aplikována plášťová a prostorová ochrana.

VII. Způsoby předání poplachové informace:

- na PPC,
- na mobil vlastníka a správce budovy.

VIII. Speciální požadavky:

- bezdrátový systém

IX. Požadavky majitele objektu:

- možnost případného dalšího rozšíření EZS, např. o kamerový systém.

5.4 Možné způsoby napadení a vniknutí do objektu

5.4.1 Z hlediska obvodové ochrany

Objekt je zabezpečen obvodovou ochrannou, na jižní a západní části areálu je vybudována vysoká zeď, na které se nachází obvodové oplocení, s betonovými sloupy a mřížemi (viz obrázek níže). Aby pachatel dokázal tuto zeď s plotem překonat, potřeboval by hodně vysoký žebřík, který používají hasiči při záchraně osob, anebo hašení požárů ve výškových budovách, anebo by musel být velice zdatný horolezec. V jednom místě je možnost využít vegetace, která se kolem zdi a na ní nachází, ale vzhledem k charakteru objektu a hodnotě majetku v něm, toto považuji za krajně nepravděpodobné, jelikož by to stálo hodně úsilí a času.

Obrázek 12: Zeď s plotem kolem objektu

Mnohem pravděpodobnější způsob vniknutí je přes bránu, která lze překonat i bez větší pomoci. Ovšem brána je u hlavní cesty, dobře osvětlená a přímo naproti se nacházejí nově postavené luxusní byty.

Obrázek 13: Slabá místa

Za nejpravděpodobnější a zcela zjevně nejslabší část se jeví pravá strana objektu, jak můžeme vidět zakreslené na horním obrázku červenou čarou. Jedná se o úzkou uličku mezi objektem a blízkým parkem. Cesta vede jen k objektu firmy za naším chráněným objektem a v noci je zcela nevyužívána. Silnice je sice osvětlena pouličními lampami, ale není celá viditelná z konkrétního objektu. Zmiňovaná firma je zcela skryta za naším objektem, a jelikož se jedná o křižovatku, nenachází se žádný objekt ani přímo naproti této cesty. V této části je náš objekt chráněn jen zdí, která lze snadno překonat, pokud je daný jedinec zdatný, za pomoci dalšího pachatele, či stoličky, žebříku (viz Obrázek 14).

Obrázek 14: Nejzranitelnější místo objektu

5.4.2 Z hlediska plášťové ochrany

Z hlediska plášťové ochrany považuji za nejslabší část hlavní vchodové dveře. Jedná se o staré, dvouramenné, dřevěné dveře, které navíc mají skleněnou výplň. Dveře jsou opatřeny západkou nahoře i dole, ale vzhledem k tomu, z jakého jsou materiálu, lze předpokládat jejich vykopnutí nebo vypáčení. Vynecháme-li možnost překonání zámku, může pachatel rozbít skleněnou výplň a pak si buď otevřít dveře, nebo se protáhnout rozbitou výplní. Vniknutí skrz sklepní okna je sice možné, ale je to méně pravděpodobné, jelikož by pachatel musel překonat mříže a nemůže vědět, zda sklep není ještě nějak zabezpečen zevnitř. Vchodové dveře do sklepa jsou ocelové a zabezpečené petlicí. Zde nepřipadá v úvahu jejich vykopnutí, ale lze odstranit visací zámek, který je sice skrytý, ale i přesto při zručnosti a zkušenosti pachatele je to možné, ale pak je nutné ještě překonat zámek ve dveřích.

Dalším způsobem, jak neoprávněně vniknout do objektu je skrz okna v prvním patře. Jedná se o stará, dřevěná okna, které mají dvě vrstvy a nad nimi jsou ještě menší okýnka. Pro pachatele nebude velký problém tato okna vypáčit.

Obrázek 15: Vstupní dveře do objektu a okna

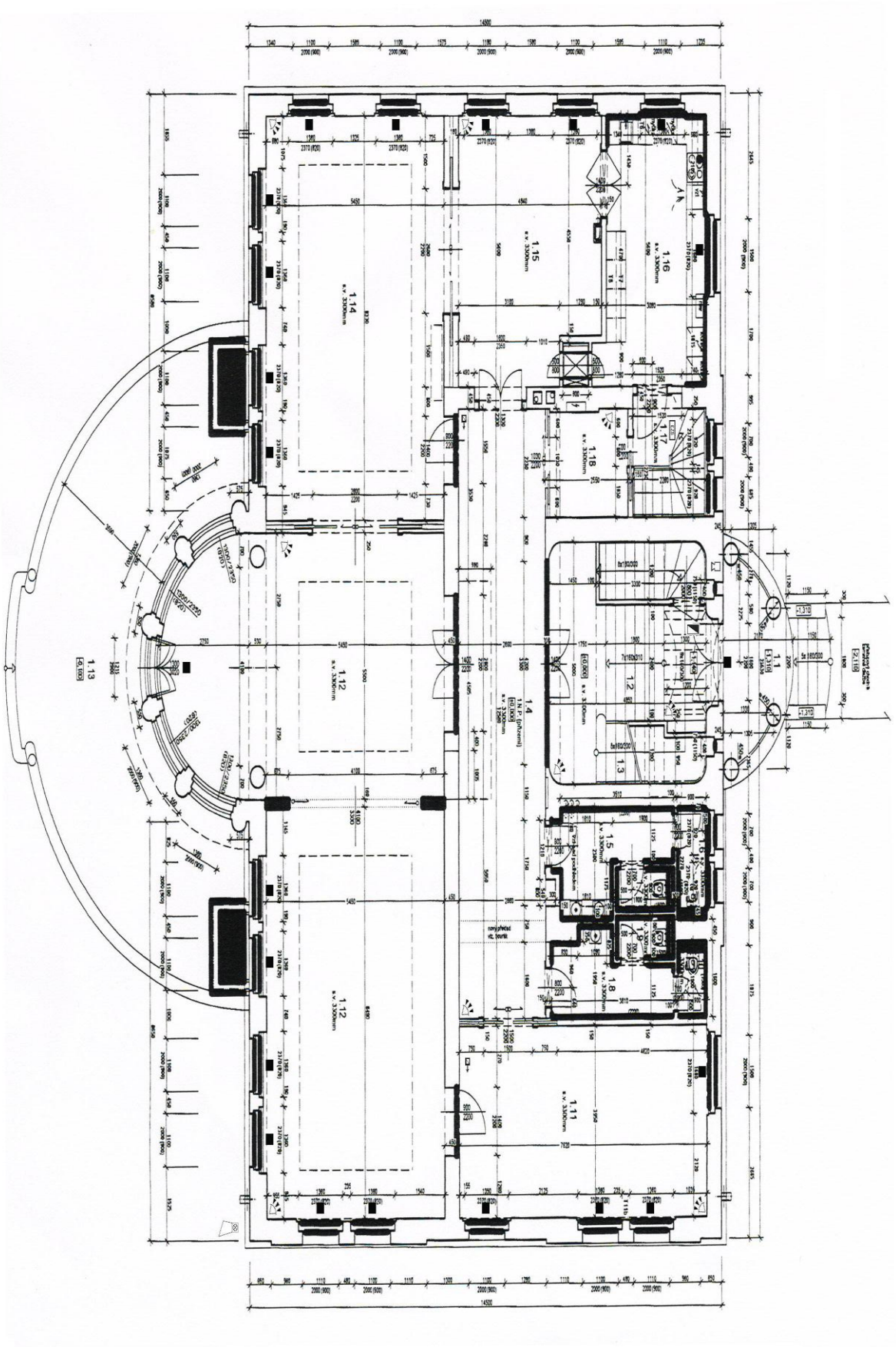
6 NÁVRH ZABEZPEČENÍ OBJEKTU POMOCÍ EZS

Při samotném návrhu zabezpečení daného víceúčelového objektu jsem vycházel hlavně s požadavků klienta, ať už co se týká zabezpečení, tak financí. Zákazník si systém zabezpečení postupem času přeje dále rozšiřovat a zvyšovat tak kvalitu zabezpečení objektu. Proto jsem v první fázi zabezpečení navrhl a provedl jen nezbytná opatření, abych splnil všechny klientovy požadavky, a dále ve své práci uvedu další návrhy zabezpečení, ať už režimová opatření, nebo mechanické či elektronické zabezpečení, které by šly nadále realizovat.

6.1 První patro objektu

První patro objektu má přibližně 380 m^2 a nachází se v něm vstup, který je zabezpečen magnetickým kontaktem a ve vstupní hale je PIR detektor. Oba tyto prvky mají definovanou zpožděnou zónu, aby přicházející oprávněná osoba mohla v klidu, v přesně definovaném časovém rozmezí, odstřežit celý objekt. Dále se zde nacházejí tři kanceláře, prodejna, reprezentativní místnost, kuchyň a toalety. V prvním patře, v úklidové místnosti je umístěna ústředna. Do prvního patra byly nainstalovány dva RTX 3 moduly pro bezdrátovou komunikaci s detektory. Jejich umístění jsem zvolil z estetického hlediska a rovněž, aby bylo první patro pomyslně rozděleno na dvě části a v každé části právě jeden modul.

Každé okno je opatřené magnetickým kontaktem a v každé místnosti je umístěn PIR detektor, naproti vstupních dveří tak, aby nebylo oslňováno slunečným svitem přes okno a umístění odpovídalo dle dané normě. U všech těchto prvků je nadefinována okamžitá zóna, čili při její narušení bude ihned vyhlášen poplach. Jediné nestřežené místnosti jsou toalety a úklidová místnost, jelikož vstup do nich vede jen přes střežené místnosti a okny se do nich nelze dostat – jsou příliš malá a opatřena mřížemi. Další možný vstup do objektu je skrz terasu, zde jsou dveře opatřeny magnetickým kontaktem a mříží a slouží pouze jako nouzový východ.



Obrázek 16: Půdorys 1. patra

Tabulka 6: Legenda místnosti 1.N.P.

Číslo místnosti	Název místnosti	Plocha
1.1	Závětří	8,60 m^2
1.2	Vstupní schodiště	16,30 m^2
1.3	Schodiště	11,74 m^2
1.4	Hala	34,08 m^2
1.5	Umývárna - ženy	5,16 m^2
1.6	WC - ženy	2,17 m^2
1.7	WC - ženy	1,62 m^2
1.8	Umývárna - muži	5,57 m^2
1.9	WC - muži	1,62 m^2
1.10	WC - muži	1,44 m^2
1.11	Kancelář	30,10 m^2
1.12	Společenská místnost a prodejna	83,62 m^2
1.13	Terasa	82,39 m^2
1.14	Kancelář	46,60 m^2
1.15	Jídelna	24,06 m^2
1.16	Kuchyň	17,54 m^2
1.17	Úklidová místnost	2,13 m^2
1.18	Šatna	5,27 m^2
CELKEM		**380 m^2**

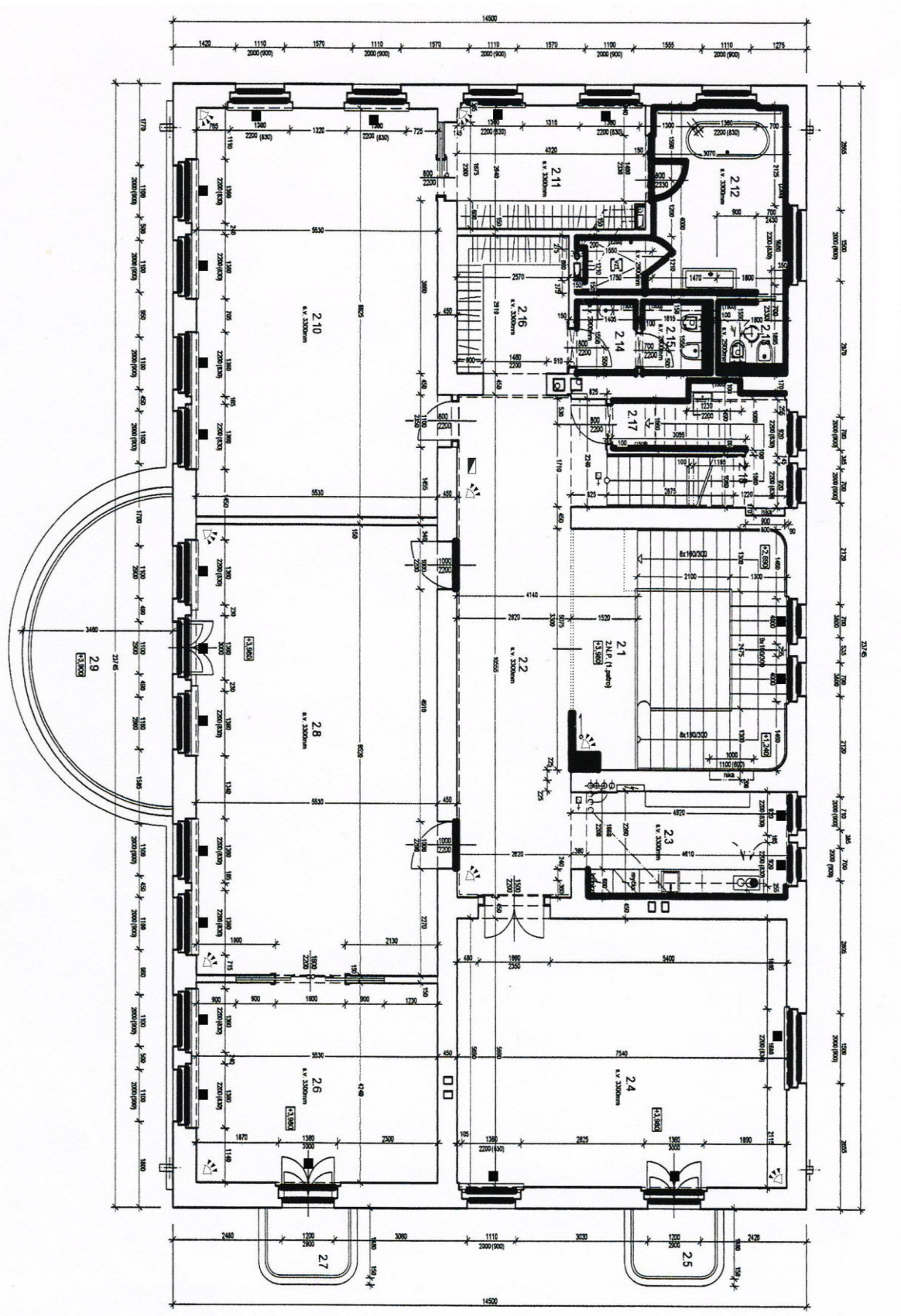
6.2 Návrh dalšího možného zabezpečení prvního patra

Vzhledem k charakteru a stáří objektu, kdy je nutné zachovávat jeho rysy, nelze provést zásadní rekonstrukci ať už z hlediska plášťové ochrany – okna, dveře, tak prostorové s tím, že by bylo možné schovat kabeláž do zdí. Hlavním nedostatkem jsou vchodové dveře, které by se snad daly nahradit vhodnými bezpečnostními dveřmi, vyráběné třeba na zakázku, a byly by věrnou replikou těch stávajících. Cena by byla asi vyšší, ale zaručena by se zvýšila i bezpečnost. Objekt má spousty oken, které by šly asi taky nahradit nějakými bezpečnějšími replikami těch původních. Co se týká zvýšení bezpečnosti pomocí EZS, přichází v úvahu určitě detektory tříštění skla. Ty byly obsaženy i v původním návrhu, ale pro tuto etapy byly zamítnuty a neuspěl jsem ani s návrhem duálních detektorů – PIR s detektorem tříštění skla. Z hlediska mechanického zabezpečení nepřicházeli do úvahy

mříže, ať už hlediska estetického, tak z důvodu zásahu do fasády domu. Možným řešením by byly bezpečnostní fólie.

6.3 Druhé patro objektu

Druhé patro má necelých 300 m^2 a nachází se v něm kancelář pro vedení firmy, sekretariát, velká zasedačka s balkónem, místnost na spaní, dvě šatny, koupelna, kuchyň, toalety a sklad. I ve druhém patře byly, ze stejného důvodu jako v prvním, nainstalovány dva RTX 3 moduly. V každém okně a balkónových dveří je magnetický kontakt a v každé místnosti umístěn PIR detektor. Všechny tyto prvky jsou rovněž v okamžité zóně. Nezabezpečeny zůstaly pouze koupelna a sklad, do nichž se lze dostat pouze přes zabezpečené prostory. Oknem je to nemožné, ať už z důvodu, že se místnosti nacházejí ve druhém patře, tak hlavně proto, že okna jsou velice malá a ještě opatřena mřížemi. Druhé patro si můžeme pomyslně rozdělit na dvě části, kdy pomyslná hranice je u konce schodiště se zasedací místností. V první půlce se nachází kancelář pro vedení, sekretariát, zasedací místnost a kuchyň. Ve druhé pomyslné půlce se nachází místnost na spaní, šatna, koupelna a toaleta. V případě, že zde nějaká osoba bude nocovat, nepotřebuje vůbec vycházet na chodbu, natož do ostatních místností. Před místnosti na spaní je umístěná druhá klávesnice a v pomyslné chodbě i PIR detektor ve zpožděné zóně, aby v případě odchodu, zde přespávajícího, a ještě neodkódovaného objektu, mohl sám oprávněný uživatel, který zde přespával, zbytek objektu odstřežit a případně objekt opustit. A naopak, v případě, kdy již všichni budovu opustili a daná osoba se chystá spát, zastřeží celý zbytek objektu, aby se do něj nedostala žádná neoprávněná osoba. Jedinou možnou komplikací daného systému je, že poslední odcházející osoba zapomene na přítomnost osoby, která zde nocuje a zakóduje celý objekt. Tím pádem by vznikl poplach, a pokud dotyčná osoba nezná příslušný kód, nemůže tento poplach zrušit. Jednoduchou možností, jak tomuto předejít je buďto celý objekt před odchodem projít, dobrá komunikace s ostatními zaměstnanci anebo umístění tabule u hlavního vchodu, kde by se vkládali kartičky osob, které se nacházejí ještě v objektu.



Obrázek 17: Půdorys 2. patra

Tabulka 7: Legenda místnosti 2.N.P.

Číslo místnosti	Název místnosti	Plocha
2.1	Hala – schodiště	7,71 m^2
2.2	Hala	30,16 m^2
2.3	Kuchyň	10,87 m^2
2.4	Kancelář – vedení	43,41 m^2
2.5	Balkón	3,58 m^2
2.6	Sekretariát	23,45 m^2
2.7	Balkón	3,58 m^2
2.8	Zasedačka	52,65 m^2
2.9	Terasa	16,63 m^2
2.10	Pokoj na spaní	48,08 m^2
2.11	Šatna	11,90 m^2
2.12	Koupelna	14,27 m^2
2.13	WC, bidet	2,40 m^2
2.14	Předsíňka	2,18 m^2
2.15	WC, bidet	2,50 m^2
2.16	Šatna	7,48 m^2
2.17	Sklad	17,79 m^2
CELKEM		**299 m^2**

6.4 Návrh dalšího možného zabezpečení druhého patra

Ve druhém patře se nabízí stejná opatření jako v patře prvním. A sice výměna oken a balkónových dveří a instalace detektorů tříštění skla. Rovněž je možné zavést příslušná režimová opatření, aby nedošlo k situaci, že zakódujeme objekt, v němž se v pokoji na spaní někdo nachází. Jak tomu předejít jsem již popsal v předešlé kapitole.

6.5 Návrh dalšího možného zabezpečení perimetru a zahrady

Ve své diplomové práci jsem měl za úkol navrhnout a realizovat plášťovou a prostorou ochranu, ale vzhledem k požadavku a přání zákazníka v budoucnu dále zvyšovat bezpečnost objektu a rozšiřovat dané zabezpečení, podíváme se i na možnosti zabezpečení obvodové ochrany a zahrady.

Jak jsem již popsal v předchozích kapitolách, kolem objektu je vysoká zeď s plotem, nebo samotná zeď. Za nejslabší místo může být považována vstupní braná. Snížit riziko vstupu do objektu právě přes tuto bránu je nainstalovat zde kameru. Ať už systémem, že se nám brána bude automaticky zavírat a my ji případně otevřeme na dálku po zazvonění návštěvníka a prohlednutí kamery, anebo že se nám případné překonání zaznamená. Daná kamera může být rozšířena i o software automatické detekce narušení a případně nám rovnou vyhlásit poplach. Rovněž je možné, ale méně praktické, zřídit zde vrátnici. Přímo vedle brány se nachází starý objekt, který by lze snadno přestavět.

Pravou stranu areálu chrání jen vysoká zeď. Lze na ní přidat nějakou bariéru s ostny, nebo rovněž podél zdi nainstalovat kamerový systém. Možnosti zabezpečení zdi z hlediska mechanického zabezpečovacího systému je více, hlavním cílem je znemožnit, nebo ztížit přelezení právě této obvodové zdi.

Celá zahrada je hojně prorostlá vegetací, ať už vysokými okrasnými stromy, nebo keři. To nám ztěžuje přehled po pozemku a naskytuje možnost pro ukrytí případného narušitele. Na zahradě lze instalovat halogenová světla, která se rozsvítí v případě jakéhokoliv pohybu nebo by svítili permanentně, což by mělo i jistý estetický efekt. Vzhledem k tomu, že je celý objekt obehnán vysokým plotem – zdí, naskytuje se zde možnost si pořídit hlídacího psa.

6.6 Součet jednotlivých prvků

Hlavní rozhodují faktor, jaké zvolíme zabezpečení a v jakém rozsahu, jsou peníze a ochota je investovat právě do zabezpečení. V našem případě jsem měl ještě omezené možnosti s nutností použít bezdrátový systém. Majitel objektu si přál v první etapě jen to nejnutnější, ovšem na druhou stranu ne to nejlevnější. Celkový rozpočet se měl pohybovat mezi 100 000 až 120 000 Kč a to se mi podařilo splnit.

Tabulka 8: Součet prvků EZS

Prvek EZS	Model	Počet	Cena za kus/Kč	Cena celkem vč.DPH
Ústředna EZS	Digiplex EVO-192	1	2 969,-	2 969,-
Bezdrátová nadstavba	Modul RTX3	4	2 179,-	8 716,-
Komunikační modul	PCS200	1	5 829,-	5 829,-
PIR detektor	PMD1P	18	1 539,-	27 702,-
Magnetický kontakt	DCT10-433/868	45	1 099,-	49 455,-
Klávesnice	K641	2	2 859,-	5 718,-
Vnitřní siréna	SA-87R	2	260,-	520,-
Venkovní siréna	TEKNIM - 720WR	1	1 099,-	1099,-
Box	BOX VT	1	1 099,-	1099,-
Akumulátor	AKKU 7Ah	1	359,-	359,-
Převodník rozhraní	INTERFACE 307	1	989,-	989,-
modul LAN/INTERNET	IP 100	1	3 669,-	3 669,-
CELKEM				**108 124,-**

7 VÝBĚR A POPIS POUŽITÝCH KOMPONENTŮ EZS

7.1 Ústředna Digiplex EVO-192

Ústředna Digiplex EVO-192 je největší dodávanou ústřednou z nabídky PARADOX. Lze u ní nastavit až 192 zón a je určena až pro 999 uživatelů. Je vhodná i pro velké objekty, se zabudovaným systémem kontroly přístupu. Ústředna Digiplex EVO-192 je kompatibilní s bezdrátovou nadstavbou MAGELLAN MG-RTX3, internetovým modulem IP100, hlasovou nadstavbou LISTEN-IN a všemi moduly DIGIPLEX.

Obrázek 18: Digiplex EVO-192[26]

7.1.1 Parametry a funkce ústředny Digiplex EVO-192

- 192 zón, 8 podsystémů (společný prostor rovněž obsadí 1 podsystém),
- 8 vstupů s ATZ = až 16 zón na základní desce,
- rozšiřování zón = expandéry, bezdrátová nadstavba, sběrnicové detektory,
- 999 uživatelských kódů, 999 bezdrátových klíčenek, 999 karet PROXIMITY ,
- libovolná délka každého kódu od 1 do 6 čísel - volitelná uživatelem,
- až 256 modulů na sběrnici,
- až 32 drátových klávesnic.[27]

[26] STASANET.cz: bezpečnostní technologie. *Digiplex EVO-192* [online]. 27.10.2006 [cit. 2012-04-19]. Dostupné z: http://www.stasanet.cz/paradox-digiplex/paradox-digiplex-ustredny/digiplex-evo-192-3.html

7.1.2 Ostatní parametry a funkce ústředny Digiplex EVO-192

- možnost zablokování klávesnic při pokusech o zadání neplatných kódů,
- programovatelná doba zablokování i počet zadání neplatných kódů,
- 2048 událostí v paměti s datem a časem, archiv přístupný z LCD klávesnice nebo pomocí instalačního programu WinLoadem,
- digitální komunikátor pro spojení s monitorovacími stanicemi včetně použití moderních DTMF formátů a formátu na PAGER použitelného i pro volání na občanský telefon, monitorování telefonické linky, 4 telefonní čísla pro PPC,
- různé způsoby zapínání - automatické zapnutí, zapnutí STAY, FORCE, zapínání dle klidu, okamžité zapnutí atd.,
- ovládání systému pomocí tlačítka - "KEYSWITCH", včetně možnosti ovládat i přímo výstupy PGM,
- omezení falešných poplachů pomocí časově závislých zón "INTELLIZONE", automatické vyřazení zón nebo podsystémů při opakovaných poplaších,
- kompatibilní s radiovou nadstavbou MG-RTX3, až 32 bezdrátových zón k 1 modulu,
- nadstavba pro kontrolu přístupu na desce - ovládání vstupu do 32 dveří - až 16 skupin dveří a 16 skupin času,
- lze připojit hlasovou nadstavbu LISTEN-IN,
- lze připojit internetový modul IP100,
- délka sběrnice: 900m; možnost prodloužení pomocí APR3-HUB2.[28]

---

[27] STASANET.cz: bezpečnostní technologie. *Digiplex EVO-192* [online]. 27.10.2006 [cit. 2012-04-19]. Dostupné z: http://www.stasanet.cz/paradox-digiplex/paradox-digiplex-ustredny/digiplex-evo-192-3.html

[28] STASANET.cz: bezpečnostní technologie. *Digiplex EVO-192* [online]. 27.10.2006 [cit. 2012-04-19]. Dostupné z: http://www.stasanet.cz/paradox-digiplex/paradox-digiplex-ustredny/digiplex-evo-192-3.html

Tabulka 9: Technické parametry ústředny

Střídavé napájení	16 V, 20 / 40 VA, 50 – 60 Hz
Zálohovací akumulátor	12 Vss minimálně 4 Ah
Napájecí výstup	12 Vss, 600 mA trvale, 700 mA maximálně, elektronická pojistka 1,1 A
Výstup na sirénu	1 A, elektronická pojistka 3 A
Všechny výstupy pro provoz	10,8 – 12,1 ss

7.2 Bezdrátová nadstavba RTX-3

Bezdrátový obousměrně komunikující modul (na frekvenci 433MHz) kompatibilní se systémy ESPRIT (lze použít jenom klíčenky), SPECTRA SP a DIGIPLEX EVO (pro tyto systémy použitelný kompletní sortiment vysílačů). K modulu jsou připojitelné výhradně vysílače řady MAGELLAN. Modul může být použit i samostatně (tj. bez připojení k ústředně). Modul MG-RTX3 je dodáván ve dvou provedeních, s jedním či dvěma relé 5A.

Obrázek 19: Bezdrátová nadstavba RTX-3[29]

[29] STASANET.cz: bezpečnostní technologie. *RTX3-433/868* [online]. 27.10.2006 [cit. 2012-04-19]. Dostupné z: http://www.stasanet.cz/paradox-spectra/bezdratova-nadstavba-magellan/rtx3-433-868-2.html

7.2.1 Parametry a funkce nadstavby RTX-3

- napájení: 11-16V=, odběr:max. 140mA,
- obousměrná komunikace po sběrnici na frekvenci 433MHz,
- plovoucí kód, kódovaný přenos,
- detekce rušení signálu, a měření síly signálu,
- až 4 PGM výstupy,
- MG-RTX3: 2x tranzistor s otevřeným kolektorem 50mA + 1x relé 5A, 28V,
- MG-RTX3/2Rx relé 5A, 28V + 1 další relé 5A, 28V (pro verzi MG-RTX3/R2),
- do vnitřního prostředí, teplota: 0°-40C°, vlhkost do 95%, bez kondenzace,
- rozměry desky: v150 x š170 x h30mm,
- rozměry plastového krytu: v100 x š95 x h30mm.

7.2.2 Kompatibilita modulu v aplikacích

S ústřednami EVO 48, EVO 96, EVO 192:

- zapnutí / vypnutí systému, ovládání PGM 1, 2, 3 a volitelně PGM4,
- libovolná aktivace z tabulky událostí pro ústředny EVO,
- inteligentní komunikace po BUS,
- 1 modul MG-RTX3 = 32 bezdrátových zón,
- pro EVO 96 lze 1 modulu připojit až 32 klíčenek,
- pro EVO 48/EVO 192 96 lze 1 modulu připojit až 96/999 klíčenek,
- (při použití klávesnice EVO-641LCD, jinak pouze 32 klíčenek),
- počet modulů MG-RTX3 omezen pouze povoleným počtem modulů na BUS,
- k modulu lze připojit všechny bezdrátové vysílače (viz dole) s výjimkou bezdrátové klávesnice MG-32LRF.

7.3 Komunikační modul PCS 200

Komunikační modul PCS200 poskytuje EZS ústřednám Paradox možnost bezdrátové komunikace, přenos systémových událostí prostřednictvím GPRS nebo GSM sítě na monitorovací přijímač IPR512. Modul PCS200 lze nakonfigurovat tak, aby posílal události koncovému uživateli prostřednictvím SMS a vzdáleně komunikoval (upload / download) se softwarem Winload přes GPRS. To vše je dosaženo pomocí jednoduchého 4vodičové sériové spojení mezi ústřednou a modulem PCS200. Modul PCS200 lze instalovat až 2m

od EZS ústředny. Anténu na modulu lze nainstalovat až do vzdálenosti 18m od zařízení, pomocí volitelného anténní prodloužení v závislosti na síle signálu.

Obrázek 20: Komunikační modul PCS 200[30]

7.3.1 Parametry a funkce komunikačního modulu PCS 200

- přenos událostí na PPC IPR512 přes GPRS nebo přes GSM,
- rychlý upload / download se softwarem WinLoad nebo NEware přes GPRS,
- firmware upgrade přes GPRS nebo Přímým spojením,
- přenos zpráv prostřednictvím textových zpráv (až 16 telefonních čísel)
- dohled komunikace modulu s ústřednou. Pokud ústředna nedetekuje modu, l potom ústředna přenese tuto ztrátu, jako přenosový kód na PCO po pevné lince,
- konečný uživatel může zastřežit či odstřežit systému zasláním textové SMS zprávy na PCS200 - GSM režim,

[30] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *PCS200 - GSM/GPRS KOMUNIKÁTOR* [online]. [cit. 2012-04-19]. Dostupné z: http://www.eurosat.cz/4022-pcs200-gsm-gprs-komunikator.html

- poslat před-nahrané hlasové zprávy o poplachu na 8 tel. čísel pomocí hlasového modul VDMP3 - GSM režimu,
- jednoduchá instalace pomocí 4-vodičového sériové spojení,
- modul antény lze nainstalovat až 18m od modulu PCS200 pomocí volitelného prodloužení anténní kabelu v závislosti na síle signál,
- 128-bit (MD5) a 256-bit (AES) šifrování - GPRS režim.

Tabulka 10: Technické parametry komunikačního modulu PCS 200[31]

typ modulu	GSM brána
napájení	12-16V
proudový odběr	400mA, při vysílání max. 1A
odběr	80 mA, max. 600 mA při GPRS / GSM přenosu
antenna	Zisk 3dBi, impedance 50 Ohm, příkon 2W max
výstupní výkon	Class 4 (2W) @ 850 / 900 MHz Class 2 (1W) @ 1800 / 1900 MHz
počet tel. čísel pro vysílání SMS zpráv	16
výstupy	8x na ústředně přes modul VDMP3
ovládání výstupů	pomocí tónové volby
SIM karta	ano, 1 libovolný operátor
SMS protokol	8-bit (IRA: ITU-T.50) nebo 16-bit (UCS2 ISO/IEC10646)
jazykové prostředí pro SMS zprávy	český jazyk
software pro nastavení modulu	WinLoad
anténa	součást dodávky (70/80/140/170MHz)
optické signalizace	LED diody, GSM a GPRS komunikace, síla signálu, status error, RX, TX, RF
uložení modulu	plechový box, bílá barva

[31] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *PCS200 - GSM/GPRS KOMUNIKÁTOR* [online]. [cit. 2012-04-19]. Dostupné z: http://www.eurosat.cz/4022-pcs200-gsm-gprs-komunikator.html

Příslušenství:

- CVT485 - převodník seriál/RS485
    - připojení na ústřednu: konektor EBUS a DIALER nebo VDMP3 - kon. EBUS,
    - způsob připojení k PCS100: svorkovnice +/-12V=, +/-RS485,
    - propojení GSM komunikátoru a ústředny: 4 dráty,
    - max. vzdálenost PCS100 od ústředny: 300m.
- EXT2 - prodlužovací kabel s kovovým držákem na přichycení ke zdi
    - typ kabelu: RG174,
    - délka kabelu: 2m,
    - barva kabelu: černá.

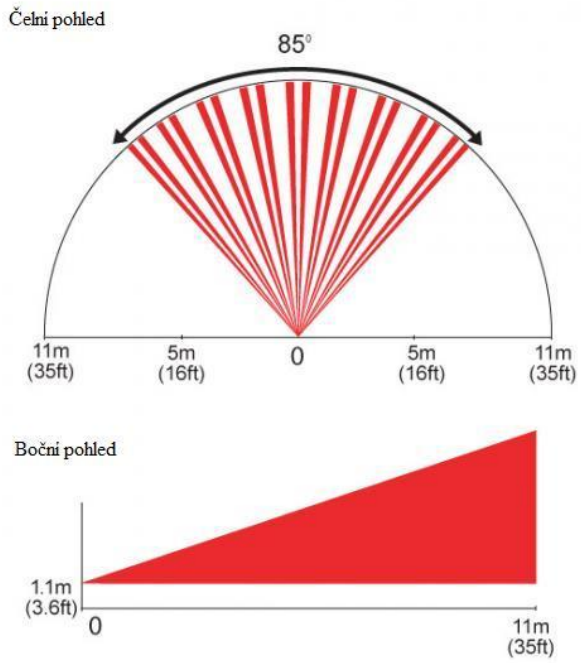
7.4 PIR detektor MG-PMD1P

Analogový bezdrátový PIR detektor s imunitou proti zvířatům do 18 kg. Slouží k detekci pohybu pro systém Magellan a v součinnosti s bezdrátovým rozšířením MG-RCV3 i s ostatními drátovými systémy. Díky softwaru " Alive " je čidlo schopné více šetřit baterie, než jiné systémy. Pokud detektor přenese dva signály o narušení zóny v pěti minutách, přepne se do režimu šetření baterií. Po uplynutí pěti minut dojde opět k přepnutí do klasického pracovního režimu. Napájení tohoto čidla probíhá třemi " AA " alkalickými bateriemi.

7.4.1 Parametry a funkce PIR detektoru MG-PMD1P

- Typ senzoru: dvojitý obdélníkový prvek,
- Pokrytí: 88,5°standardně, 11m x 11m, střed paprsku 15m,
- Pracovní teplota 0°C až +50°C,
- LED indikace – poplach / slabá baterie,
- přenos informace o slabé baterii,
- 433 MHz nebo 868 MHz,
- Automatická teplotní kompenzace,
- Patentovaný systém zpracování signálu (Auto Pulse Signal Processing),
- Tamper kontakt,
- napájení: 3x tužkové AA alkalické baterie (součást dodávky),
- životnost baterií cca 4 roky,

- režim "usnutí" pro úsporu baterií,
- dosah v budově: 35m (MAGELLAN 60-60), 50m (SPC1759MG), 70m (MGRCV3),
- záběr: 11x11m / 88,5° - standardní Fresnelova čočka (možnost výměny čočky)
    - 2. generace Fresnelových čoček LODIFF, PET Imunite,
- doporučená výška instalace: 1,8-2,7m,
- rozměry: 125x65x57mm.[32]



Obrázek 21: Detekční pole[33]

[32] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *MG-PMD1P* [online]. [cit. 2012-04-19]. Dostupné z: http://www.eurosat.cz/415-mg-pmd1p.html

[33] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *MG-PMD1P* [online]. [cit. 2012-04-19]. Dostupné z: http://www.eurosat.cz/415-mg-pmd1p.html

7.5 Bezdrátový magnetický kontakt DCT10-433/868

Bezdrátový magnetický kontakt s dvěma jazýčkovými relé a s jedním externím vstupem. Při přenosu signálu z magnetického kontaktu jsou rozlišeny v ústředně dvě zóny, jazýčkové relé a univerzální vstup. Pro napájení detektoru slouží tři AAA alkalické baterie.

Obrázek 22: Bezdrátový magnetický kontakt[34]

Tabulka 11: Technické parametry magnetického kontaktu DCT10-433/868[35]

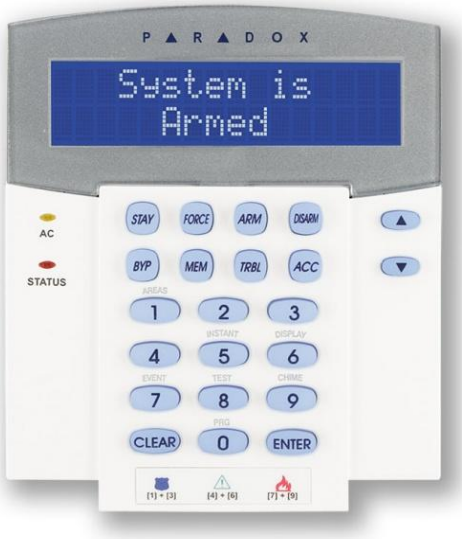
Typ detektoru	bezdrátový magnetický kontakt, povrchový
Senzor	2 x jazýčkové relé, horizontální/vertikální
Externí vstup	ano, 1 x univerzální, NC/NO
Adresace detektoru	jedinečné číslo detektoru (2x)
Napájení	3 x AAA alkalické baterie
Životnost baterie	cca 3 roky
Tamper krytu	ano
Frekvence	433/868 MHz
Bezdrátový systém	MAGELLAN/OMNIA
Přenos signálu	technologie plovoucího kódu
Dosah	70 metrů s MG-RTX3
	70 metrů s MG5000/MG5050
	35 metrů s ústřednou MG-6160
Optická signalizace	červená LED dioda - uvnitř krytu
Barva krytu	bílá
Rozměry	š 125 x v 46 x h 25 mm
Pracovní teplota	vnitřní: 0 až 50°C

[34] STASANET.cz: bezpečnostní technologie. *DCT10-433/868* [online]. 27.10.2006 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/paradox-magellan/bezdratova-nadstavba/dct10-433-868.html

[35] STASANET.cz: bezpečnostní technologie. *DCT10-433/868* [online]. 27.10.2006 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/paradox-magellan/bezdratova-nadstavba/dct10-433-868.html

7.6 LCD klávesnice K641

Elegantní a snadno ovladatelná LCD klávesnice Digiplex K641 umožňuje snadný přístup ke všem bezpečnostním funkcím systému. Pomocí této klávesnice lze systém jednoduše a rychle ovládat, přehledně zobrazovat informace o stavu systému a modifikovat parametry a funkce systému. Displej se 32 znaky zobrazuje všechny základní stavy a napovídá postupy ovládání systému. Každou klávesnici v systému lze modifikovat dle aktuálních požadavků, vyplívajících z umístění klávesnice v objektu. Jeden systém může být tak ovládán z více klávesnic, kde každá klávesnice může mít umožněny odlišné možnosti ovládání (přidělení skupinám, možnost zobrazení).



Obrázek 23: LCD klávesnice K641[36]

7.6.1 Vlastnosti klávesnice K641

- 32 znaků pro popis jednotlivých parametrů,
- plné programování ústředen,
- prohlížení historie událostí,
- modrý podsvit LCD,
- česká i anglická verze,
- možnost přiřazení jedné, nebo více skupinám,

[36] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *LCD KLÁVESNICE K641 (DGP2-641BL)* [online]. [cit. 2012-04-20]. Dostupné z: http://www.eurosat.cz/217-k641-dgp2-641bl.html

- 1 zóna a jedno PGM,
- nezávislé nastavení zvonkohry pro každou zónu,
- 14 jednodotykových tlačítek,
- 3 vestavěné panické poplachy,
- dvouřádkový LCD displej s nastavitelným podsvětlením, kontrast a rychlost přepínání zobrazení.

Tabulka 12: Technické parametry klávesnice K641[37]

Napájení	9 až 16 V ss
Proudová spotřeba	110 mA
Proudové omezení PGM	50 mA
Počet vstupů	K641 --1, K641R -- 2
Indikace napájení	žlutá LED svítí
Indikace umístění	zelená a žlutá LED blikají společně
Indikace chyby komunikace	červená a žlutá blikají střídavě
LCD	2 řádkový displej, 2 x 16 znaků

7.7 Vnitřní siréna SA-87R

Vysokovýkonná siréna s piezoelektrickou membránou pro použití jako akustické zařízení v interiéru ale i exteriéru hlídaného objektu. Při poplachu vytvářejí v hlídaném prostoru nesnesitelnou hlukovou hladinu, která případnému pachateli účinně ztěžuje činnost. V uzavřeném prostoru je obtížné lokalizovat umístění sirény a tím ji rychle vyřadit z činnosti.

Obrázek 24: Vnitřní siréna SA-87R[38]

[37] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *LCD KLÁVESNICE K641* [online]. [cit. 2012-04-20]. Dostupné z: http://www.eurosat.cz/217-k641-dgp2-641bl.html

7.7.1 Parametry a funkce sirény SA-87R

- možno spustit jen blikač,
- 8 až 14 V DC,
- odběr: 220 mA (100 mA jen blikač),
- hlasitost: 122 dB/1 m.

7.8 Venkovní siréna TEKNIM -720WR

Kvalitní venkovní siréna s akustickou i optickou signalizací s možností oddělené aktivace. Použitím piezoměniče pro část akustickou a stroboskopu pro část optickou je snížen na minimum odběr tak, že je možné použít pro zálohování malý Ni-MH akumulátor (konstantní kapacita i při nízkých teplotách). Sirénu lze nastavit v režimu SAB (odběr proudu při poplachu z AUX, baterie pouze záloha) nebo SCB (odběr z baterie, zátěž pro AUX pouze 30mA) a nastavení volit podle parametrů AUX ústředny. Siréna je zařazena do nejvyšší bezpečnostní kategorie. Pod červeným plastem majáku jsou umístěny dvě LED, které blikáním signalizují přítomnost napájecího napětí v siréně a dobíjení jejího akumulátoru. Vnitřní plechový kryt elektroniky zvyšuje odolnost sirény proti mechanickému poškození.

Obrázek 25: Venkovní siréna TEKNIM[39]

[38] STASANET.cz: bezpečnostní technologie. *Vnitřní sirény* [online]. 03.07.2008 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/zabezpecovaci-systemy/vnitrni-sireny/2.html

[39] STASANET.cz: bezpečnostní technologie. *Venkovní sirény* [online]. 03.07.2008 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/zabezpecovaci-systemy/venkovni-sireny/ teknim-720wr-2.html

7.8.1 Parametry a funkce sirény TEKNIM

- venkovní zálohovaná siréna s blikačem (stroboskop 1Hz),
- dvojitý kryt – vnější nárazuvzdorný plastový a vnitřní ocelový kryt,
- dvojitý TAMPER – ochrana proti vniknutí do sirény i jejímu odstranění ze zdi,
- napájení 9-16V=,
- odběr v režimu SAB: max. 450mA,
- odběr v režimu SCB: max. 30mA,
- max. dobíjecí proud baterie: 25mA / baterie: Ni-MH,
- akustický tlak: 118dB,
- pracovní teplota -40° až +80°C, krytí IP 46,
- certifikace: 4. třída = vyšší rizika,
- rozměry 300x215x60mm (výška x šířka x hloubka), hmotnost 1,2kg.[40]

7.9 BOX VT (BOX V-40, BOX V-80)

Ústředny vhodné pro střední a velké objekty s možností instalace rozsáhlejší sběrnice. Počet podsystémů 4/8, počet zón 48/192 a nadstavba přístupu ACCESS předurčuje ústředny pro větší rodinné domy a sídla, střední a velké komerční objekty, sklady, případně i továrny a výrobní haly. Jde o plně adresovatelný sběrnicový systém, do kterého lze zařadit až 127/254 sběrnicových modulů (klávesnice, bezdrátová nadstavba, expandéry, PGM výstupy, doplňkové zdroje, posilovače sběrnice, komunikační moduly IP, GSM, GPRS,…) i samostatné sběrnicové detektory BUS.

[40] STASANET.cz: bezpečnostní technologie. *Venkovní sirény* [online]. 03.07.2008 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/zabezpecovaci-systemy/venkovni-sireny/ teknim-720wr-2.html

Obrázek 26: Box VT[41]

7.10 Akumulátor

Zálohovací, olověné, hermeticky uzavřené akumulátory různé kapacity pro použití v instalacích EZS. Všechny dodávané akumulátory jsou o napětí 12V. Pro akumulátory AKKU 7Ah, 18Ah, 26Ah, 40Ah a 65Ah jsou k dispozici speciální krabice s TAMPERem.

Obrázek 27: Záložní akumulátor[42]

AKKU 18Ah: max. dobíjecí proud: 6,5A; rozměry: 181x76x167mm; hmotnost: 6,50kg.

[41] STASANET.cz: bezpečnostní technologie. *BOX VT (BOX V-40, BOX V-80)* [online]. 01.07.2008 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/zabezpecovaci-systemy/boxy-a-prislusenstvi2/box-vt-box-v-40-box-v-80.html

[42] STASANET.cz: bezpečnostní technologie. *Akumulátory* [online]. 30.06.2008 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/zabezpecovaci-systemy/akumulatory/akumulatory-2.html

7.11 INTERFACE 307

Převodník INTERFACE 307 USB slouží k přímému spojení software WinLoad a ústředen SPECTRA SP/MAGELLAN/DIGIPLEX EVO. Adaptér je možné připojit do PC přes SERIAL RS 232 nebo USB port. Na modulu jsou signalizační LED PC link (USB) pro indikaci připojení k PC, PRODUCT link pro indikaci připojení k zařízení a Rx/Tx pro indikaci přenosu dat.

Obrázek 28: Interface 307[43]

7.11.1 Základní vlastnosti převodníku Interface 307

- rychlá komunikace - přenos programu z PC za 8s,
- provedení: porty USB i COM,
- LED signalizace (připojení k ústředně a PC; přenos dat),
- plastový kryt,
- jako příslušenství se dodává kabel pro připojení k PC (délka 5 m, oboustranný USB konektor).

7.12 IP 100 – modul LAN/INTERNET

Tento modul se používá pro komunikaci s ústřednami přes LAN/INTERNET. Modul IP100 obsahuje web server a lze jej využít pro základní uživatelské ovládání, monitorování

[43] STASANET.cz: bezpečnostní technologie. *INTERFACE 307* [online]. 01.07.2008 [cit. 2012-04-20]. Dostupné z: http://www.stasanet.cz/paradox-magellan/moduly-magellan/interface-307.html

ústředny z libovolného PC právě v těchto sítích nebo k posílání emailů z ústředny při zapnutí/vypnutí, poplachu, poruše atd. Modul můžeme využít i k plnému programování instalační firmou a to i dílkově pomocí softwaru WinLoad.

Obrázek 29: modul IP100

abulka 13: Technické parametry modulu IP100[44]

Typ modulu:	komunikační modul LAN/internet
Kompatibilita:	SP4000/SP65/SP5500/SP6000/SP7000 MG5000/MG5050 EVO192 WinLoad/NEWARE/Explorer 6 a vyšší/Mozilla 1.5 a vyšší
Napájení:	11 - 16 V=
Dokumentace:	Instalační manuál - IP100
Proudový odběr:	min.90 mA, max. 110 mA
Firmware:	uložen v EEPROM paměti
Software pro nastavení modulu:	vyhledávač IP100
Software pro spojení:	WinLoad, NEWARE
Jazykové prostředí:	čeština, angličtina
Připojení k ústředně:	4 pinovým kabelem na SERIÁL, konektor ústředny
Způsob připojení do LAN/internet:	veřejná pevná IP adresa, dynamická IP
Optická signalizace:	LED diody ERROR, RX, TX, LINK, LAN

[44] Safepower: Elektronické zabezpečovací systémy. *IP100 - modul LAN/INTERNET* [online]. [cit. 2012-04-29]. Dostupné z: http://www.safepower-shop.cz/elektronicke-zabezpecovaci-systemy-/paradox/digiplex-evo/moduly/8342/ip100---modul-laninternet--81215.htm

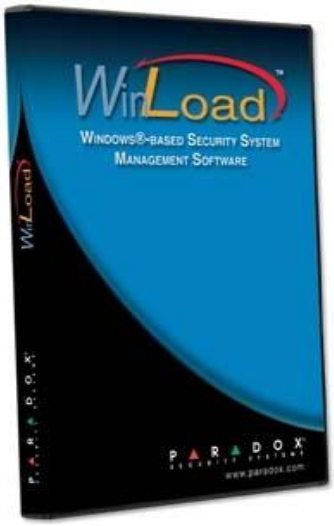
8 PROGRAM WINLOAD

Program Winload je určen pro dálkové nebo místní spojení s ústřednami SPECTRA, MAGELLAN a DIGIPLEX EVO včetně všech jejich modulů. Tento program je výhradně určen pro instalační firmy a slouží jim k programování, sledování, vyhodnocení a archivaci všech událostí ústředen PARADOX. Spojení s ústřednami probíhá buď přes modem po telefonní lince, nebo přímo na místě s ústřednou pomocí adaptéru INTERFACE 307USB. Právě spojení přes LAN/INTERNET je zajištěno pomocí již výše zmiňovaného modulu IP100.

Tabulka 14: Technické parametry pro program WinLoad[45]

Kompatibilita:	ESPRIT E SPECTRA SP MAGELLAN DIGIPLEX I307/CONV4/IP100
Typ software:	programovací, sledovací,
Dokumentace:	Návod - WinLoad
Typ software:	vyhodnocovací
Jazyková verze:	česká
PC minimum:	Pentium 1 GHz, 512 MB, HD 1 GB
Operační systém:	Windows 98, 2000, XP, Vista
Programování ústředny:	ano, je možné nastavit/měnit všechny parametry
Stahování archivu ústředen:	ano
Monitorování, ovládání ústředen:	ano
Typ spojení s ústřednou:	telefonní linka - modem přímo - adaptér I307 USB/CONV4 USB (do 300 m) LAN/internet - IP100, GPRS - PCS200

[45] VARIANTplus: Komplexní řešení elektronických systémů budov. *WinLoad (8888-001) - programovací SW pro E/SP/MG/EVO* [online]. [cit. 2012-04-29]. Dostupné z: http://www.variant.cz/zbozi/8888-001-winload



Obrázek 30: Program Winload[46]

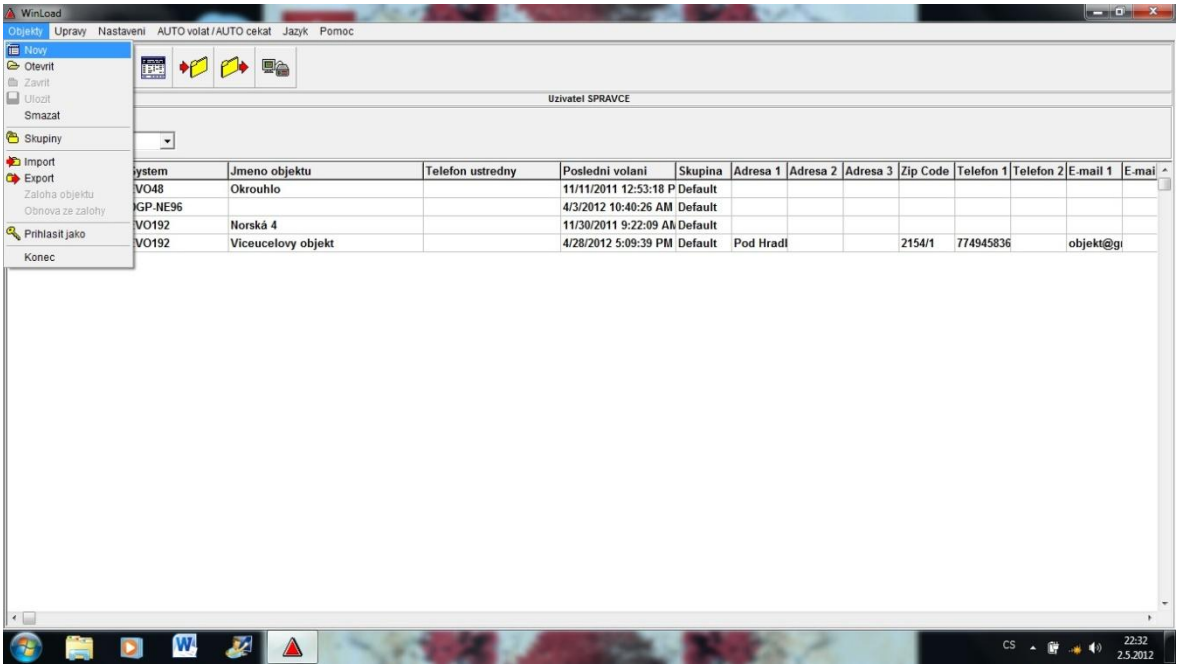
8.1 Programování a nastavení ústředny

Jak již bylo výše zmíněno, pomocí programu Winload dokážeme ovládat a programovat celý systém zabezpečení. Ať už na dálku, nebo po připojení k ústředně fyzicky, můžeme nastavovat jednotlivé zóny a podsystémy. Na začátku je ale nutné do programu zadat příslušné údaje, čím si dále sami usnadníme práci. Program po připojení je schopný sám si načíst údaje o zabezpečení daného objektu. Jedná se převážně o to, že je schopný rozpoznat počet zón, jejich rozdělení a taky počet detektorů. Díky tomu pak snadno skrze tento program ponastavujeme jednotlivé zóny či detektory.

8.1.1 První kroky po spuštění

První krok, který jsem musel provést, bylo propojení PC a desky ústředny pomocí kabelu. Jednotlivé prvky, které jsou k tomu potřeba, jsem již popsal v předešlé kapitole. Pro propojení jsem použil port „Seriál“ na desce ústředny. Poté jsem spustil samotný program WinLoad, kde je potřeba si vytvořit nový objekt.

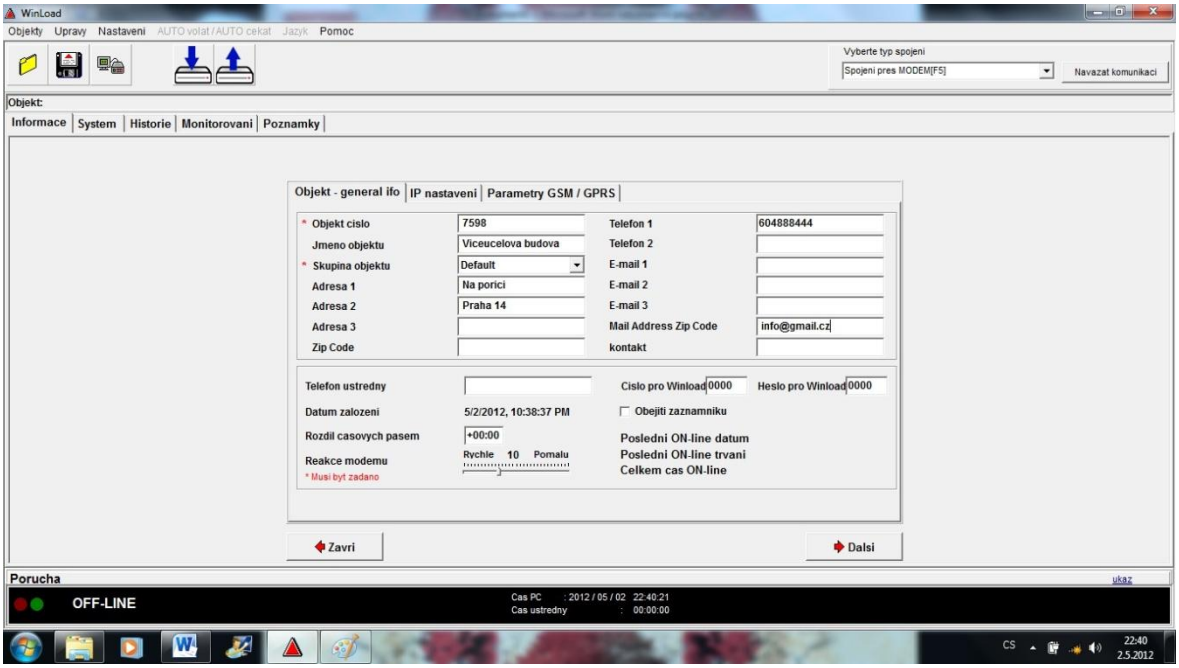
[46] SECTRON: Security & Communication Systems. *WinLoad* [online]. [cit. 2012-04-29]. Dostupné z: http://en.sectron.com/products/alarms/9/163



Obrázek 31: Založení nového objektu

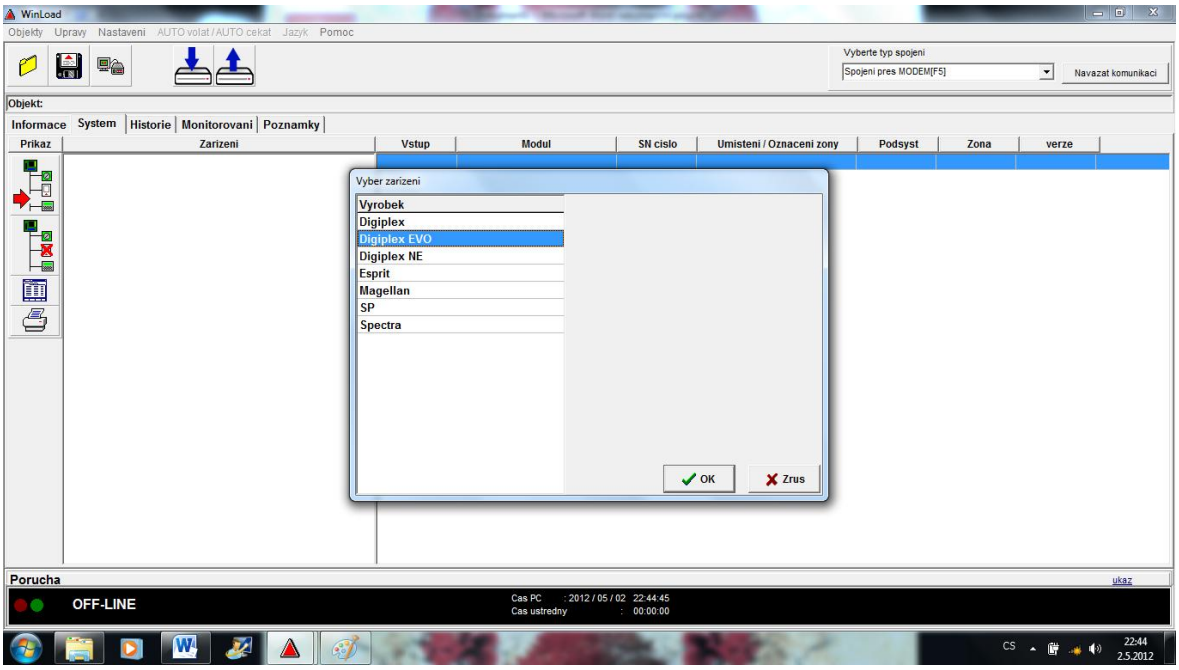
Po vytvoření nového objektu v programu, si zadáme všechny potřebné informace, které nám slouží pro přehlednější komunikaci při další manipulaci s ústřednou. Povinně musíme vyplnit číslo objektu a přiřadit daný objekt do příslušné skupiny objektu. Tyto skupiny si můžeme sami vytvářet. Jedná se hlavně o to, že máme např. jednu firmu, která má více poboček, které zabezpečujeme, a tak si celou skupinu pojmenujeme právě názvem této firmy a do této skupiny pak přidáváme jednotlivé objekty. To nám v budoucnu ušetří spoustu času a ihned víme, kde máme daný objekt hledat. Není to povinné, ale slouží to pro větší přehlednost.

Další údaje, které máme možnost vyplnit, jsou jméno objektu, adresa, telefon na kontaktní osobu – majitele/správce objektu, jeho email.



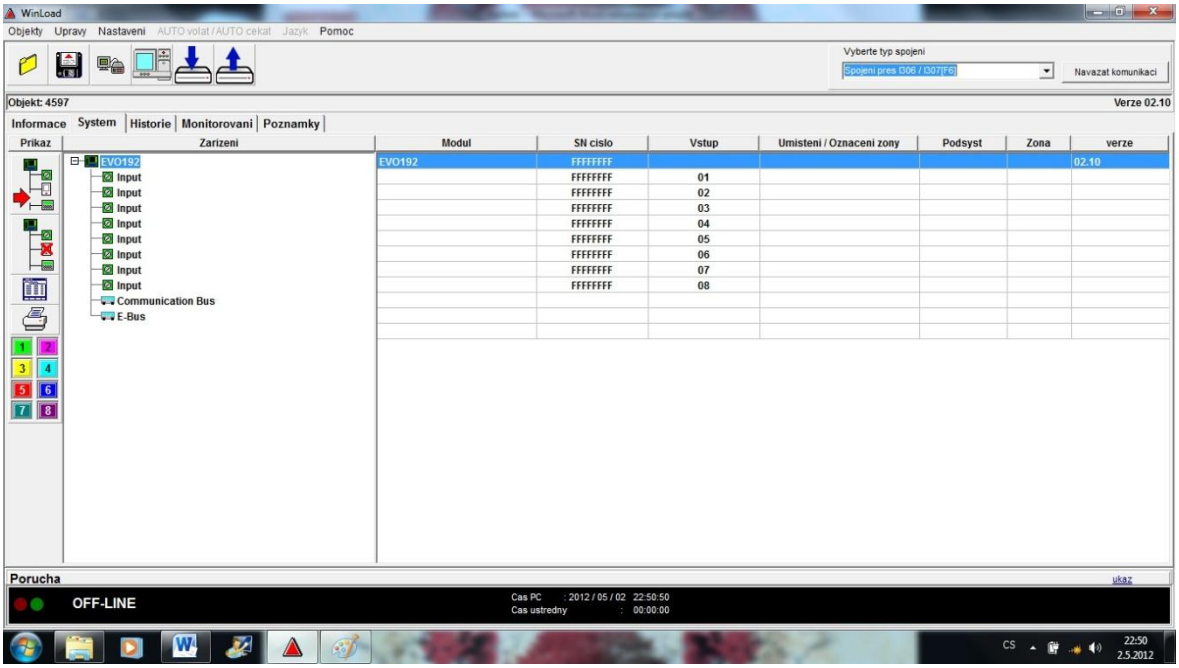
Obrázek 32: Vyplnění informací o objektu

Stisknutím tlačítka „další“ se zobrazí typy ústředen. Musíme vybrat správný typ ústředny, který máme nainstalovaný, jinak nedojde ke komunikaci ústředny s PC. Já jsem nainstaloval ústřednu PARADOX EVO 192, a proto jsem zvolil možnost Digiplex EVO.



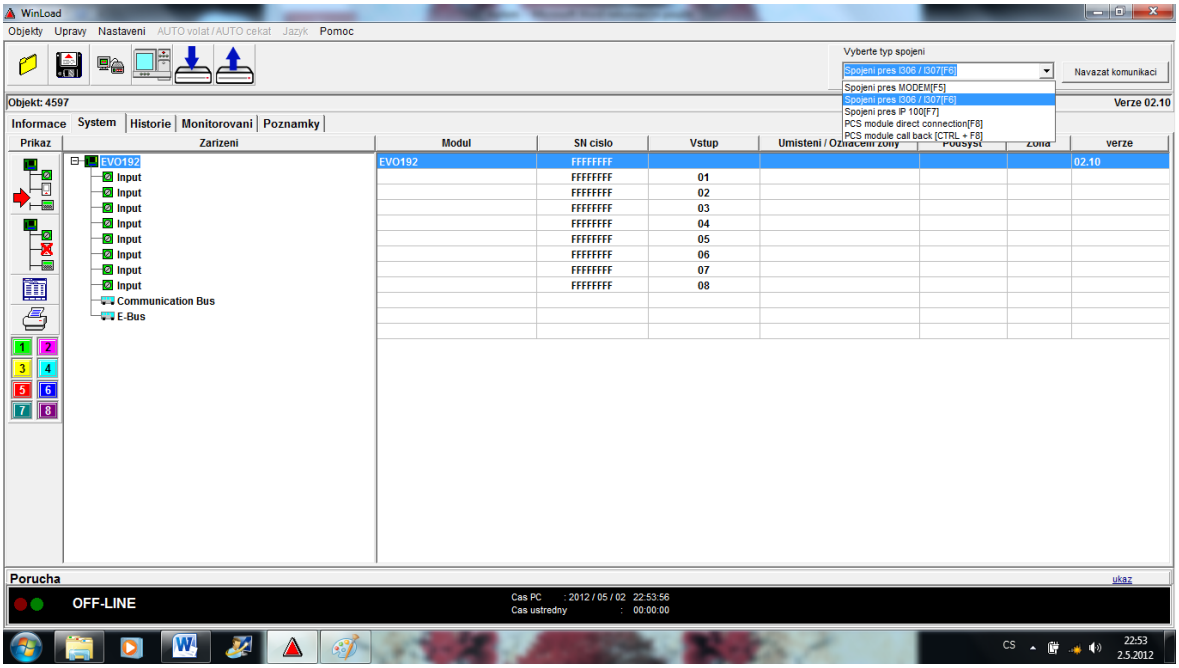
Obrázek 33: Výběr typu ústředny

Pokračujeme tlačítkem „OK“. Ústředna se načte do obecného nastavení. Zatím jsme s ústřednou spojeni jen v režimu off-line.



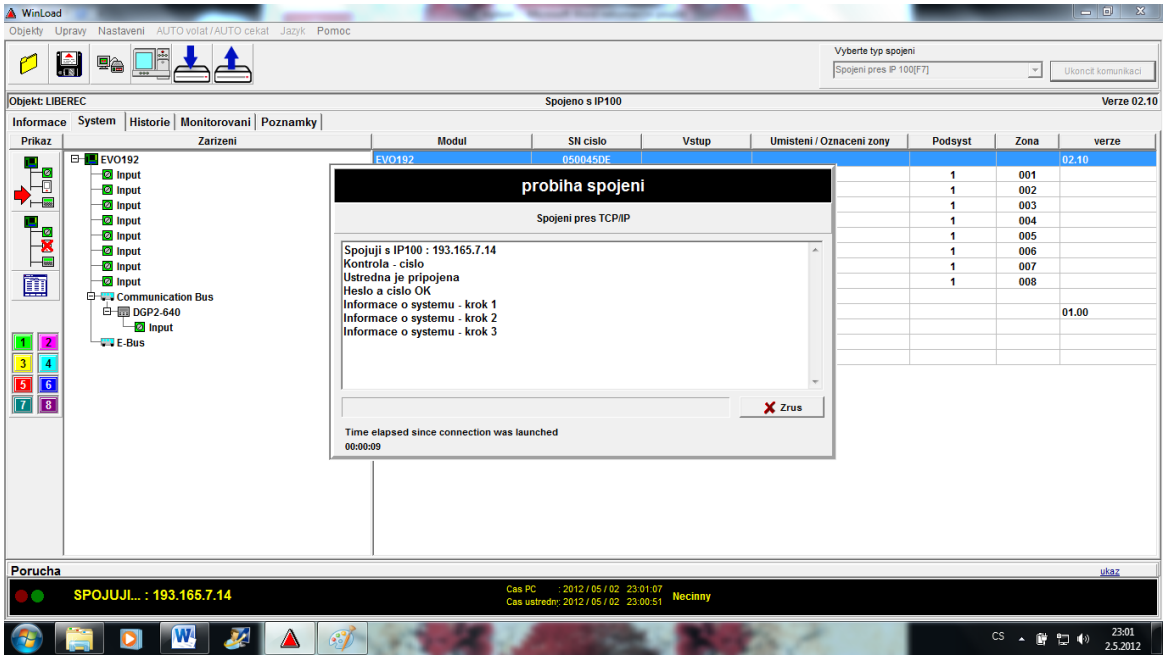
Obrázek 34: Obecné nastavení ústředny

Pro přímou komunikaci s ústřednou si vybereme typ spojení. Pokud se fyzicky nacházíme v objektu, tak použijeme spojení přes I306/I307. Pro spojení na dálku, např. když se nacházíme v kanceláři, nebo kdekoliv jinde, vybereme si typ spojení přes záložku „IP100“. Nutné je mít přístup na internet.



Obrázek 35: Výběr typu spojení s ústřednou

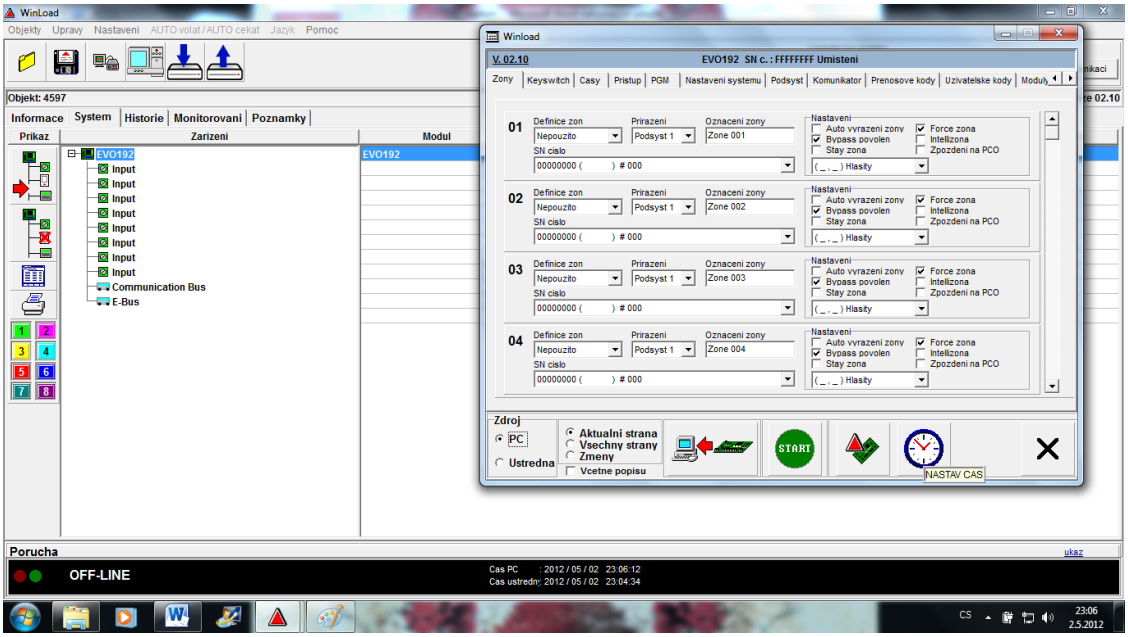
Abychom přešli do režimu on-line, tak musíme po výběru typu spojení, kliknout na záložku „Navázat spojení“. Tímto krokem dojde k propojení ústředny a PC a nyní můžeme nastavit jednotlivé parametry celého systému dle přání zákazníka.



Obrázek 36: Navazování spojení s ústřednou

8.1.2 Programování ústředny

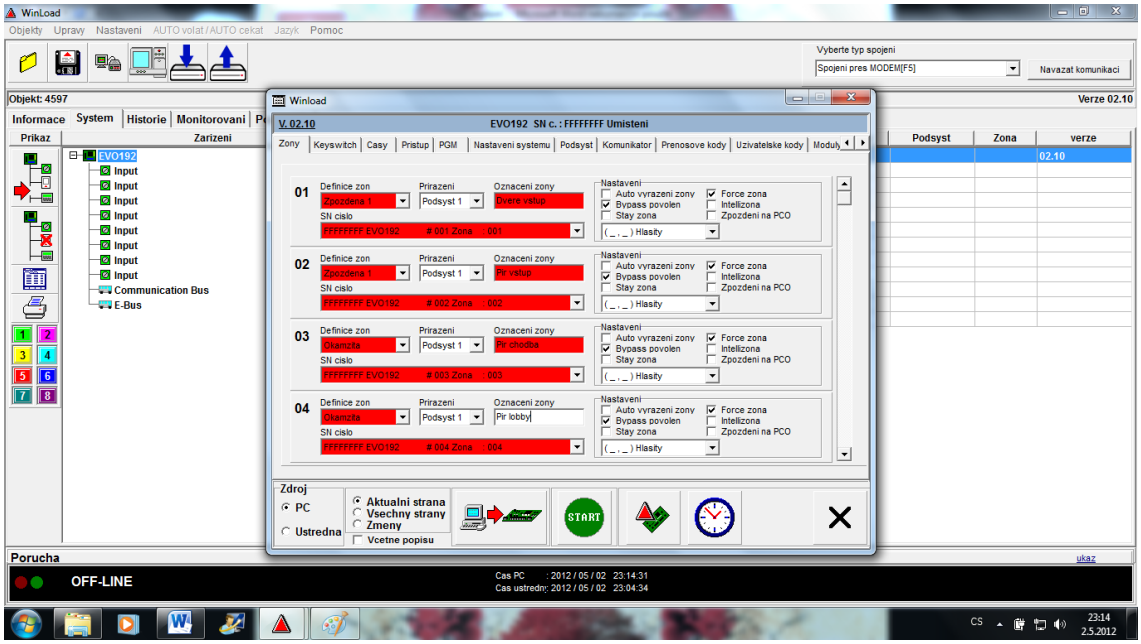
Po navázání spojení můžeme celý systém naprogramovat dle přání a požadavků zákazníka. Po kliknutí na záložku „EVO192“ se nám otevře celé programovací menu ústředny. Nejdříve si srovnáme datum a čas. Srovnání data a času provedeme jednoduchým kliknutím na symbol hodin.



Obrázek 37: Srovnání data a času

Nyní přichází na řadu asi nejdůležitější část programování, a sice nastavení a definice jednotlivých zón. V záložce „Zóny“ definujeme jednotlivé prvky systému EZS a jejich pojmenování. Pro náš případ jsem zvolil rozdělení systému na „Podsystém 1“ a „Podsystém 2“, vzhledem k požadavku zákazníka, který si přál mít možnost zakódovat buďto celý objekt, nebo objekt mimo části s pokojem na spaní.

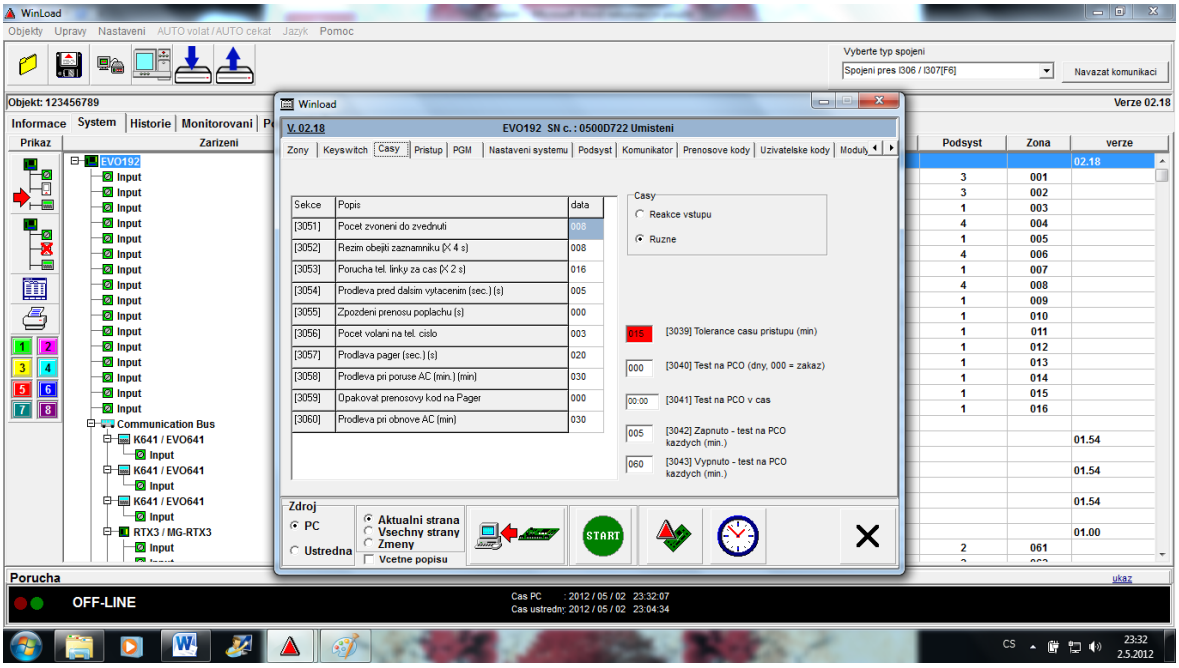
Podsystém 1 pojmenuji jako „Global“, jde o to, že jedním kódem zakódujeme celou budovu.



Obrázek 38: Nastavení Podsystému 1

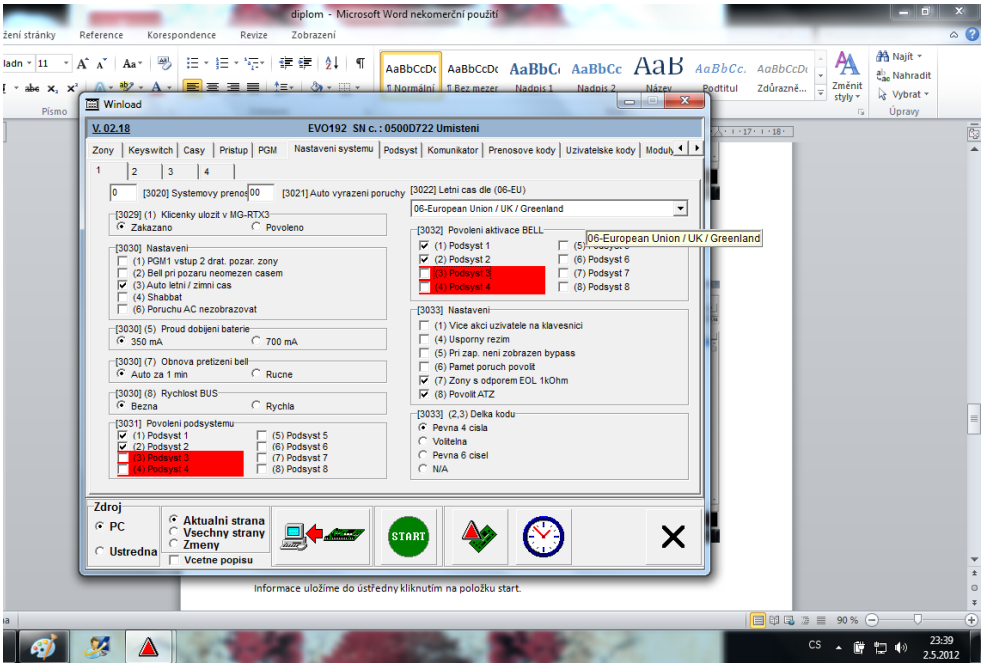
U vstupních dveří jsem umístil klávesnici, proto jsem nastavil magnetický kontakt (01) a PIR detektor (02) umístěné ve vstupní chodbě, jako zpožděná 1 (definice zóny). Tím pádem máme po otevření vstupních dveří 30 vteřin na odkódování objektu, aniž by byl vyvolán poplach. Všechny ostatní prvky v „Podsystému 1“ jsem definoval a nastavil jako okamžité. Rovněž necháme zaznačenou položku Force zone a Bypass, jedná se o funkci, kdy můžeme zakódovat objekt při poruše jednoho prvku systému EZS. Jedná se o nouzové řešení, kdy potřebujeme objekt zakódovat a nemáme čas zjišťovat, který prvek nefunguje.

V záložce „Časy“ nastavujeme prodlevy pro jednotlivé funkce systému.



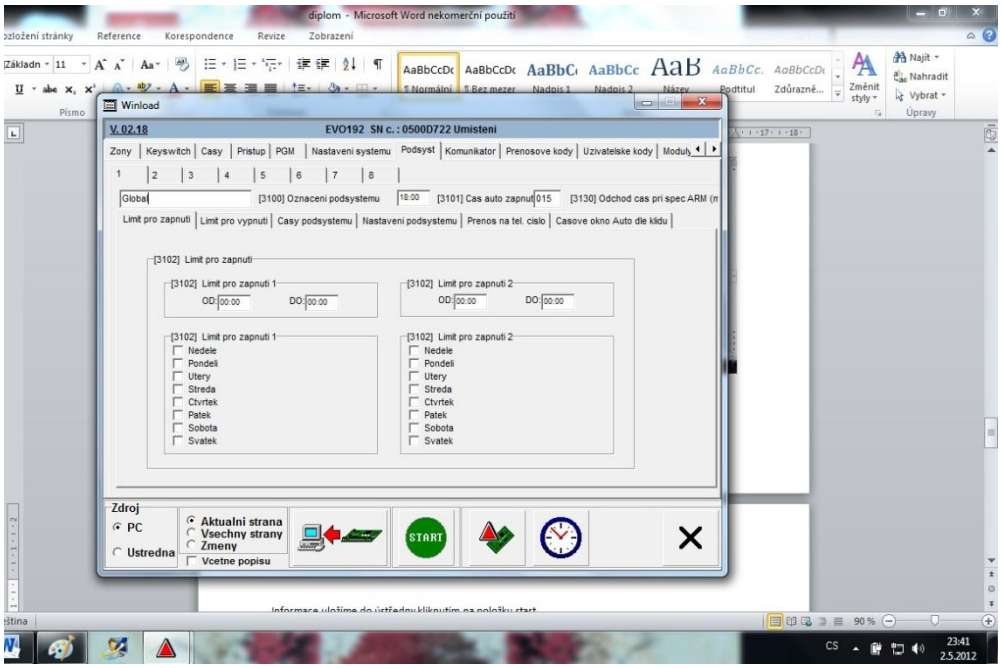
Obrázek 39: Nastavení prodlev (časů) systému

Záložka „Nastavení systému“ nám slouží k zadání dobíjecího proudu. V našem případě, kdy máme dva podsystémy, tak jsem povolil právě „Podsystém 1“ a „Podsystém 2“ a povolil ATZ, jelikož máme větší počet PIR detektorů a magnetických kontaktů než devět.



Obrázek 40: Nastavení systému

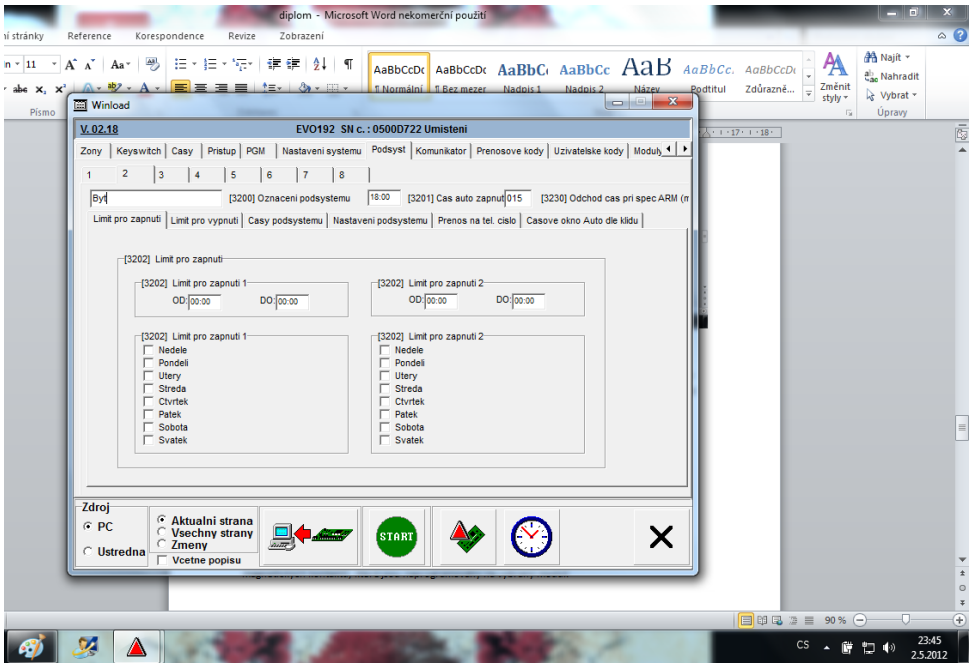
V záložce „Podsystém“ si rozdělíme daný systém na dva podsystémy, jak jsem již zmínil výše, a každému podsystému dáme jiné parametry pro uživatelské účely.



Obrázek 41: Podsystém 1 – Global

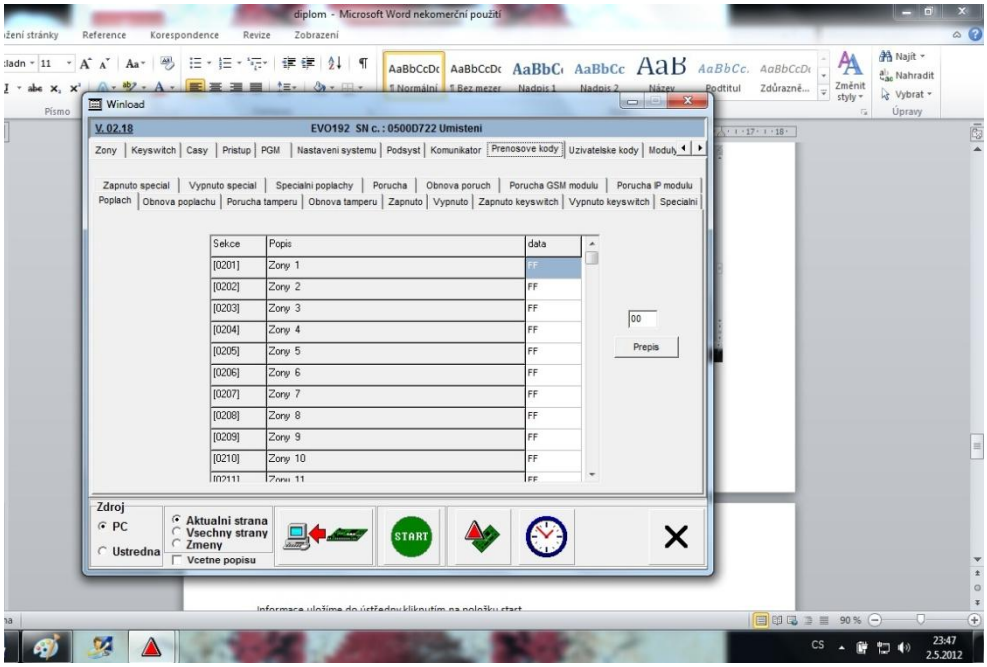
Podsystém 2 bude sloužit jen pro obytnou část objektu ve druhém patře. Jedná se o pokoj na spaní, šatnu, koupelnu a WC. Jedním kódem poté zakódujeme pouze ty místnosti, ve kterých se již nadále nebudeme pohybovat, nebo není přípustné, aby se v nich někdo pohyboval poté, co budovu opustí zaměstnanci. Zbylá část objektu zůstane odkódována,

abychom se mohli volně pohybovat v příslušných místnostech – v částech budovy, bez vyvolání poplachu.



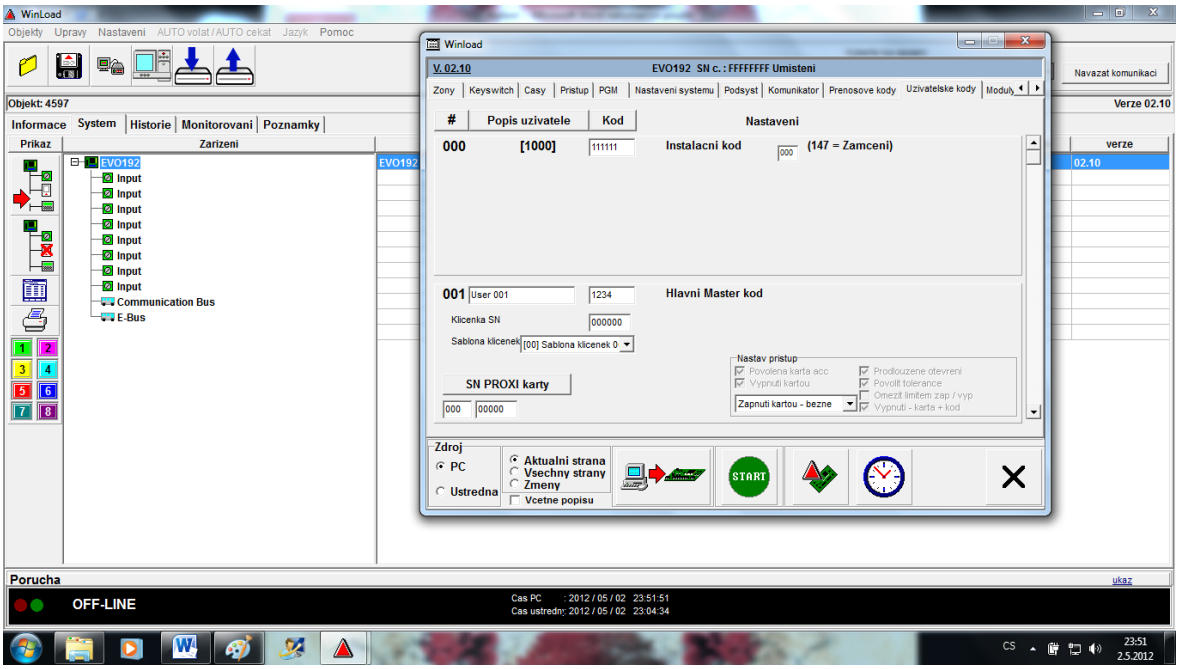
Obrázek 42: Podsystém 2 – Byt

Dalším krokem při nastavování systému, který nemůžeme vynechat je záložka „Přenosové kódy“, která slouží pro hlídání převážně poruch. U položky porucha musím u všech zón do záhlaví data vyplnit dvě nuly, naopak u položky obnova poruch dvě velká písmena F. Tím zajistím, že budou hlídány poruchy a zároveň dojde k jejich obnově a systém nezůstane zablokován.

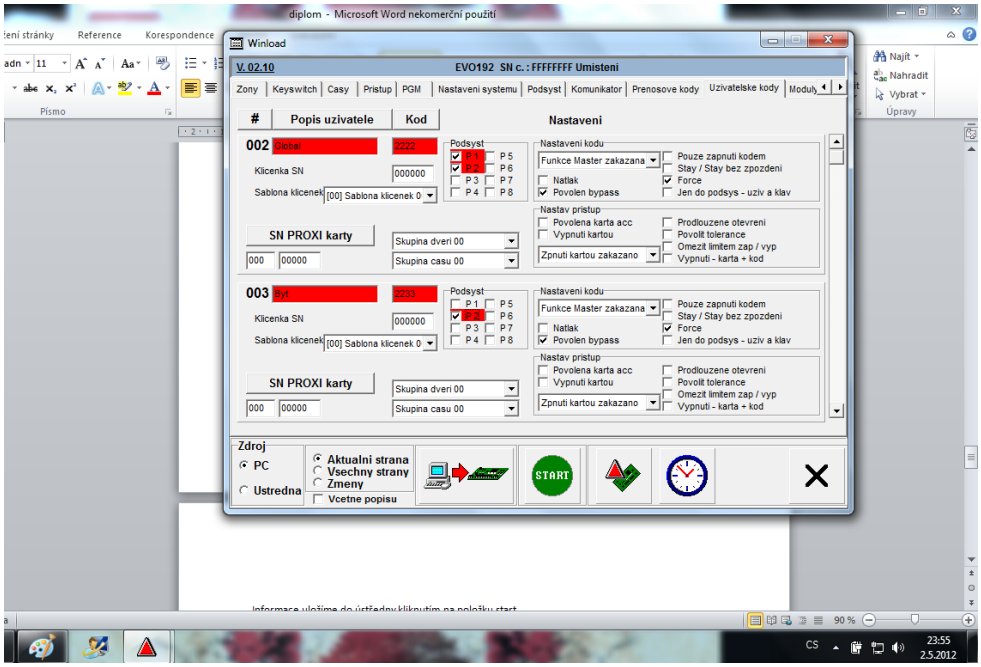


Obrázek 43: Přenosové kódy

V záložce „Uživatelské kódy“ si nastavíme a zadáme „Instalační kód“ a „Master kód“, který slouží servisní firmě pro úpravu celého systému. Kód pro „Global“ a kód pro „Byt“ jsou pak určeny jen pro uživatelské účely. Tím zamezíme i tomu, aby mohl být systém přeprogramován kýmkoliv, kdo vlastní daný program, nebo má přístup k našemu PC.



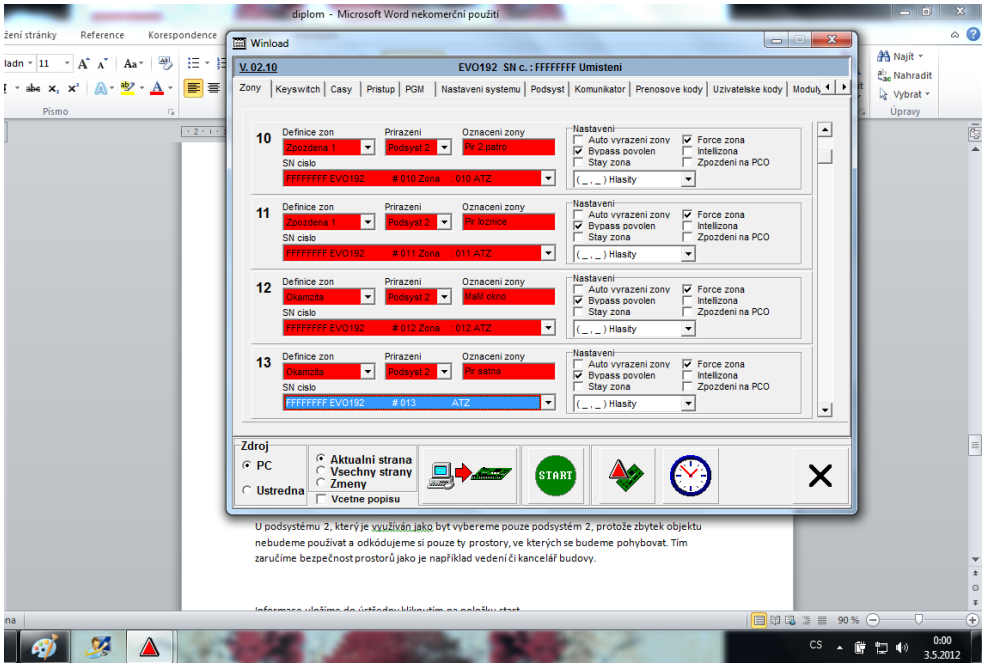
Obrázek 44: Kódy pro servis



Obrázek 45: Uživatelské kódy

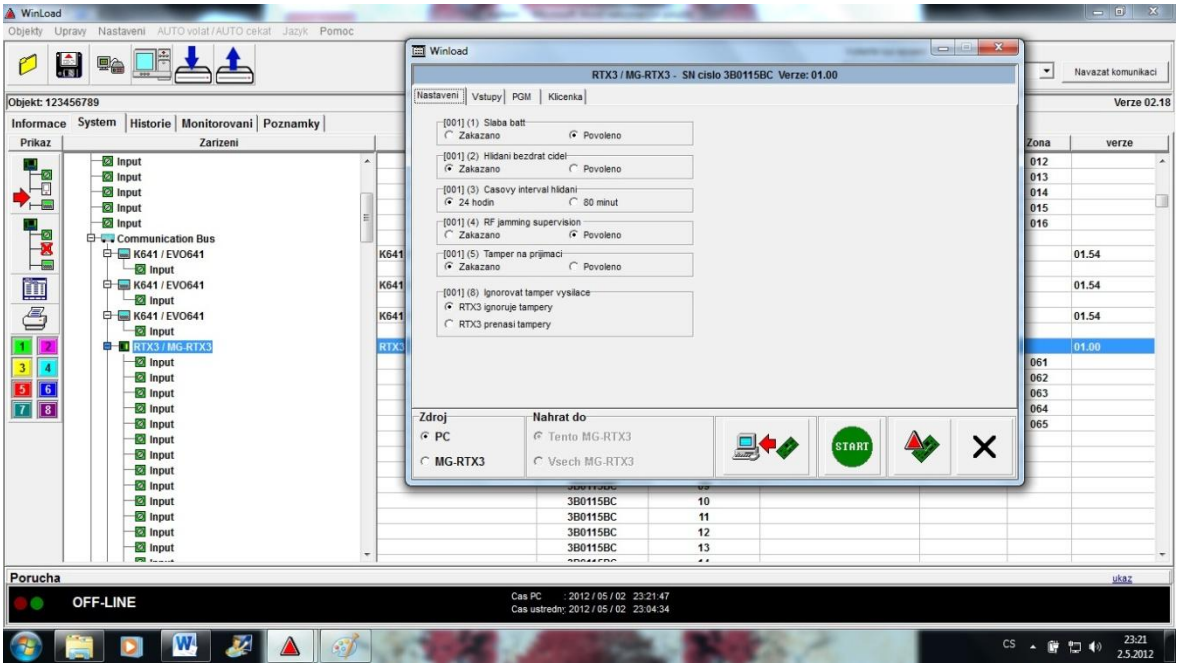
Vzhledem k požadavkům zákazníka je nutné u „Podsystému 1“, který jsem si nazval „Global“, vybrat i „Podsystém 2“ a to z důvodu, aby bylo možné zakódovat celý objekt a to zadáním kódu 2222.

U „Podsystému 2“, který je využíván jako byt, vybereme pouze přiřazení do „Podsystému 2“, jelikož ostatní části objektu nebudeme používat, ani se v nich pohybovat. Tím jsem zaručil bezpečnost ostatních prostorů, nebo detekci při vstupu do nich, jak si přál zákazník.



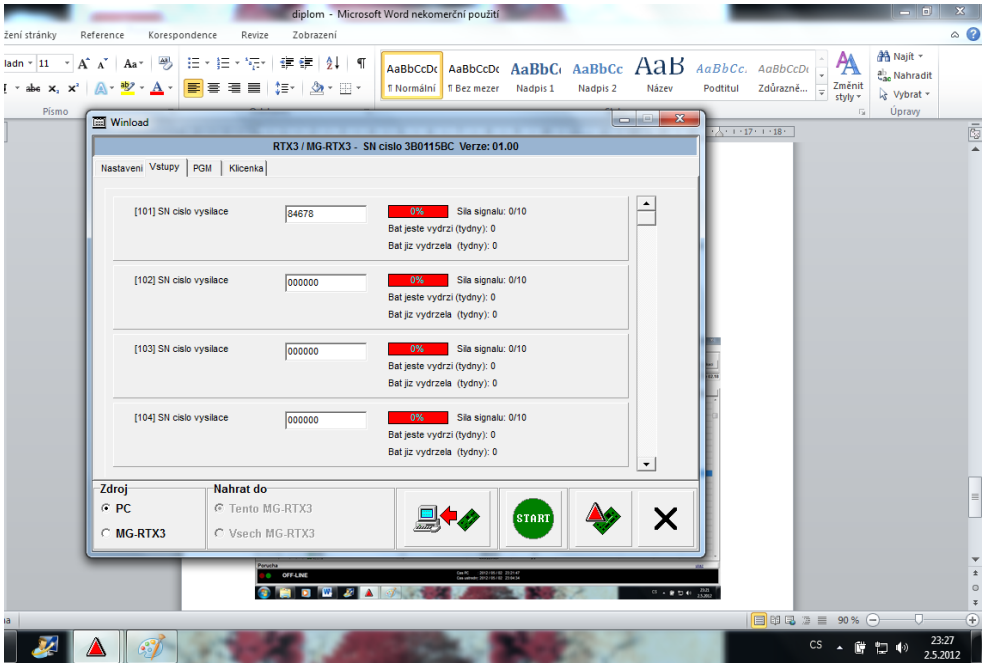
Obrázek 46: Podsystém 2

V prvním i druhém patře jsem musel nainstalovat modul RTX 3, do každého patra po dvou kusech. Modul RTX 3 nám slouží pro bezdrátovou komunikaci a každý modul dokáže komunikovat až s 32 prvky. Každé patro jsem si v podstatě rozdělil na půlky a v každé půlce nainstaloval právě modul RTX 3. I u těchto modulů je nutné nadefinovat funkce. U záložky „Nastavení“ je důležité povolit hlídání baterií, aby systém při jejich vybití vyhlásil poruchu, což zajistí včasnou výměnu baterií jak u PIR detektorů, tak u magnetických kontaktů, které jsou naprogramovány na vybraný modul.



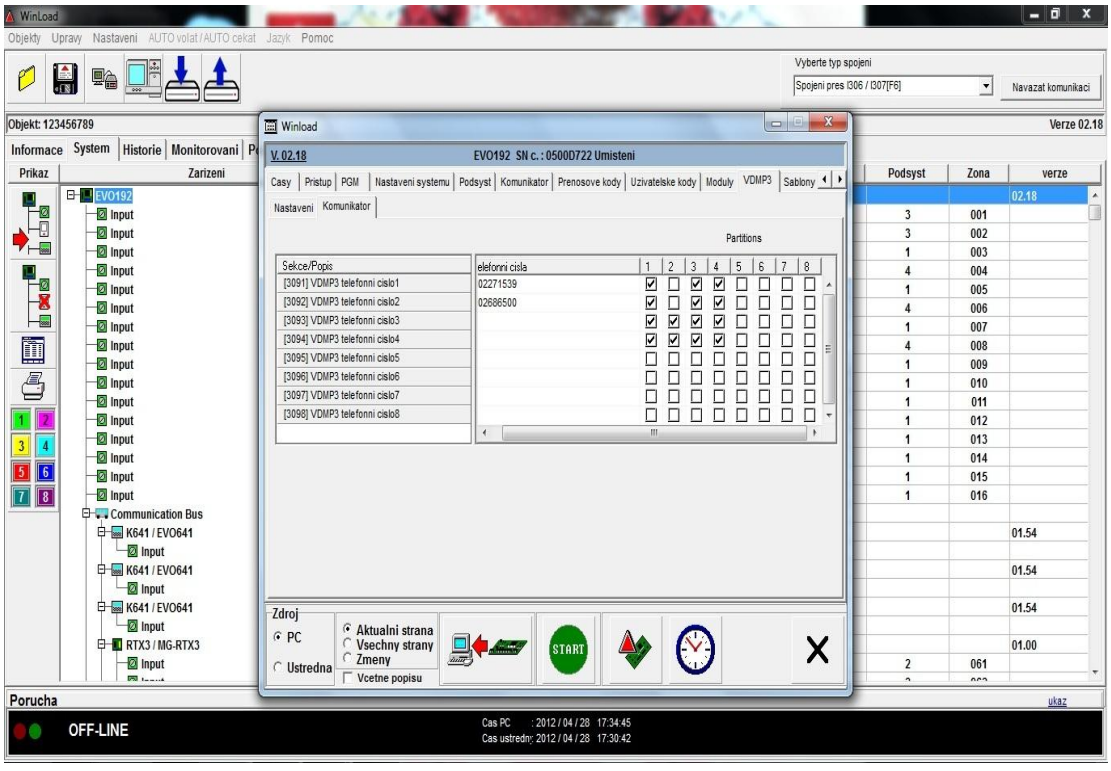
Obrázek 47: Nastavení modulu RTX 3

V záložce „Vstupy“ jsem pak musel zadat jednotlivá sériová čísla PIR detektorů a magnetických kontaktů, které si pak modul RTX 3 sám načte a zajistí jejich správnou funkci. Při přesném pojmenování jednotlivých detektorů, pak snáze poznáme, kde je vyhlášen poplach, nebo který z detektorů hlásí poruchu. V režimu on-line vidíme kvalitu signálu daného prvku a podle něj můžeme případně přeprogramovat vybraný prvek k jinému modulu RTX 3 pro zlepšení dosahu a kvality jeho signálu.



Obrázek 48: Zadávání sériových čísel

Pro přenos zpráv na telefon je k ústředně připojen komunikátor, u kterého nastavíme telefonní čísla, na která budou chodit zprávy o objektu. Zpravidla se jedná o kódování, odkódování, poplachy a poruchy. V našem systému jsem zadal čísla mobilních telefonů na majitele objektu a ředitele místní pobočky.



Obrázek 49: Nastavení komunikátoru

8.1.3 Zobrazení systému EZS v programu WinLoad

Všechny zadané informace a parametry je potřeba uložit do ústředny a to provedeme kliknutím na položku „Start“. Ústředna si pak načte všechny nastavené parametry a kliknutím na položku „Monitorování“ již sledujeme aktivní prvky.

Obrázek 50: Přehled prvků

V tomto programu „Zobrazení“ se nám objeví jakákoliv změna systému. Sledujeme především otevření a zavření dveří – reakce magnetického kontaktu, dále reakci PIR detektorů. Tyto změny se nám objevují žlutě. V případě vyvolání poplachu červeně. Dále je možné sledovat dobíjecí proud záložního zdroje a poruchy.

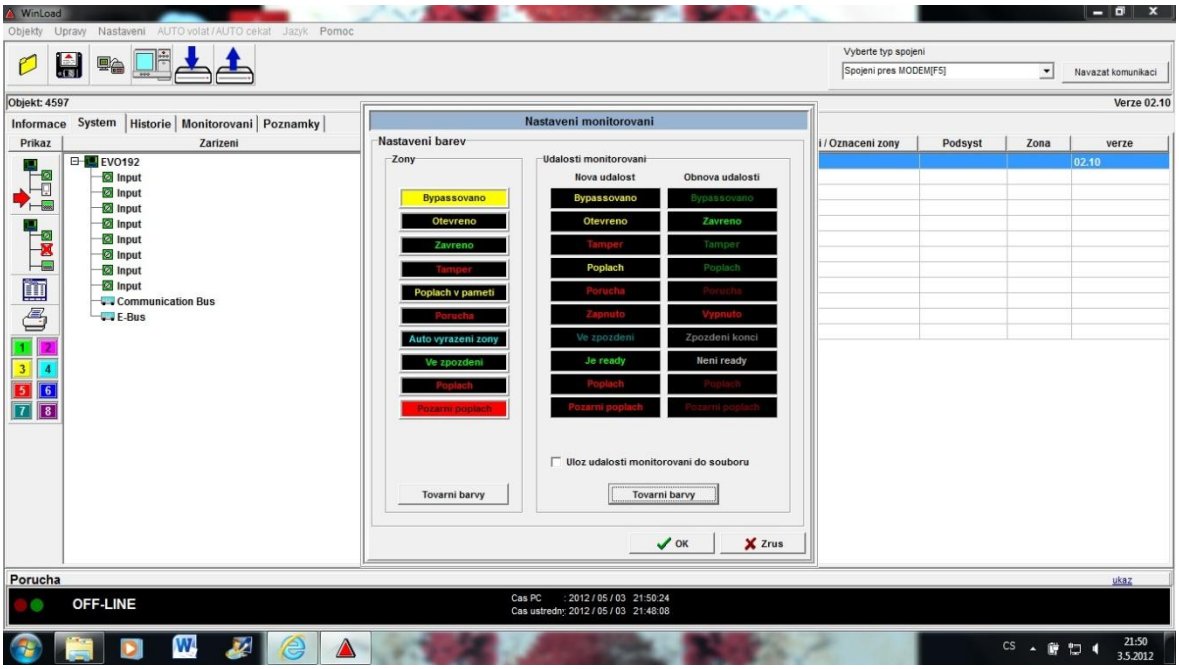
V případě, že je PIR detektor, nebo magnetický kontakt „bypassován“, což znamená, že ho systém při poruše ignoruje, aby došlo k bezproblémovému zakódování objektu, je daná situace v monitorování vybarvena žlutě a doplněna nápisem bypassováno.

Je-li v daném odkódovaném objektu zaznamenám pohyb, při příslušném prvku se v monitorování okno vybarví žlutě s nápisem otevřeno.

Pokud je prvek v klidu – bez pohybu, nebo je objekt zakódován, zabarví se zeleně – zavřeno.

Program WinLoad dokáže detekovat i otevření krytu např. PIR detektoru, tento zásah se nám v monitorování zobrazí u daného prvku „Tamper“ červenou barvou.

Máme-li zakódovaný objekt a dojde k jeho narušení, tak se okno zabarví červenou barvou s nápisem poplach. Poplach se zobrazí u daného prvku, kde došlo k narušení.

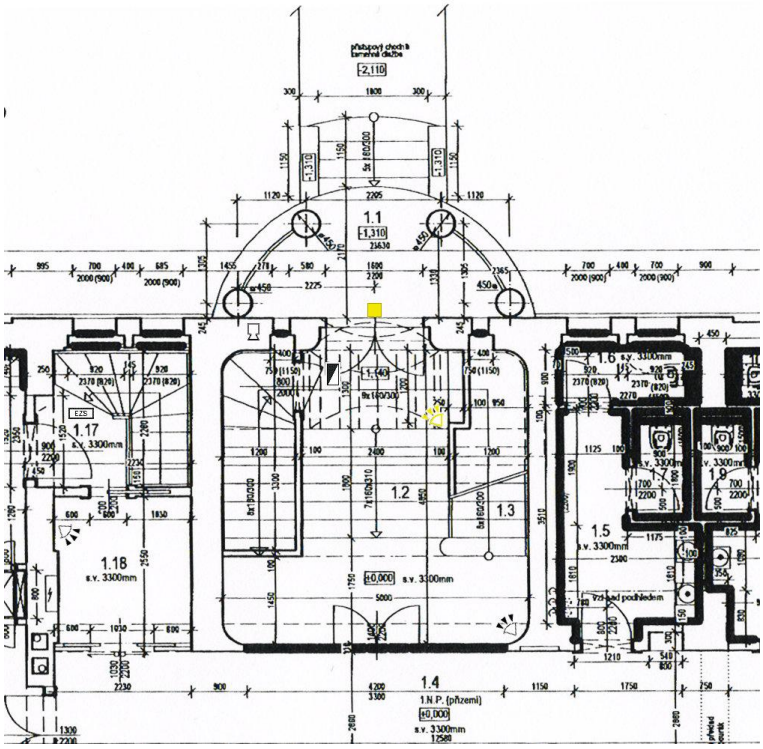


Obrázek 51: Barevné možnosti zobrazení systému

Do programu lze uložit i plánky objektu, kde se nám zobrazí všechny výše popsané události na konkrétním detektoru či kontaktu. V simulaci jsem otevřel vstupní dveře a při odkódovaném objektu se nám daná změna objeví žlutě, viz obrázek níže.

Obrázek 52: Signalizace otevření vstupních dveří

Na daném plánku objektu pak příslušnou změnu vidíme taky.

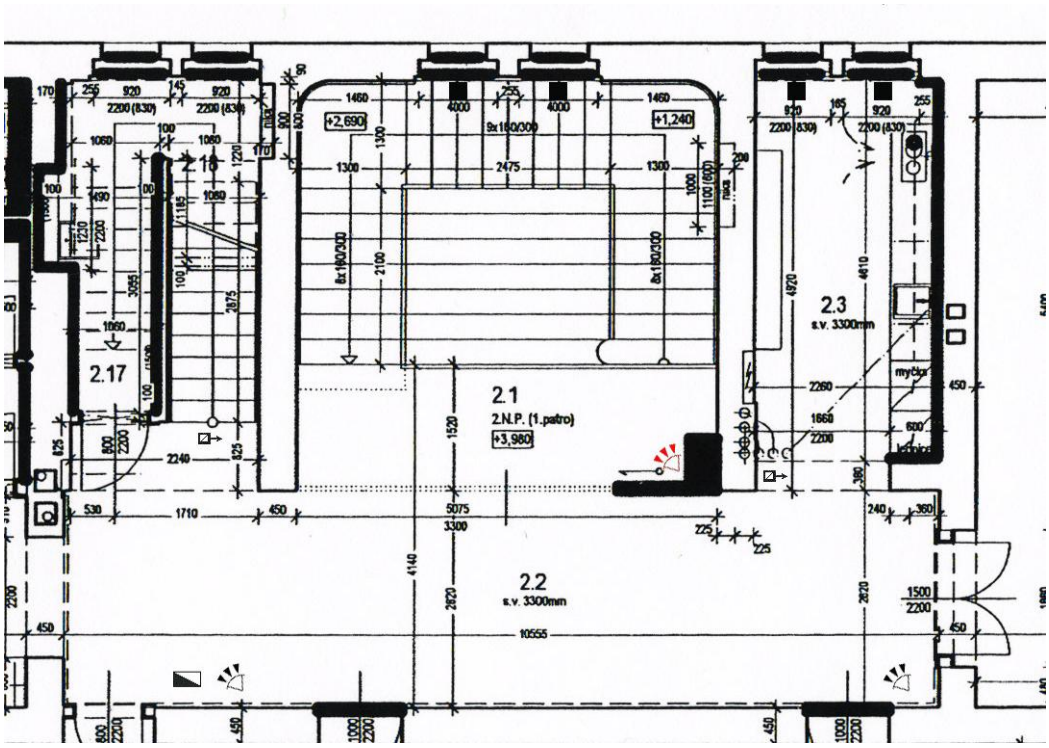


Obrázek 53: Změna stavu – výřez z plánu objektu

Při otevření okna/dveří, když máme objekt zakódován, se nám v případě okamžité zóny ihned vyhlásí poplach a daná událost se nám v přehledu objeví červeně.

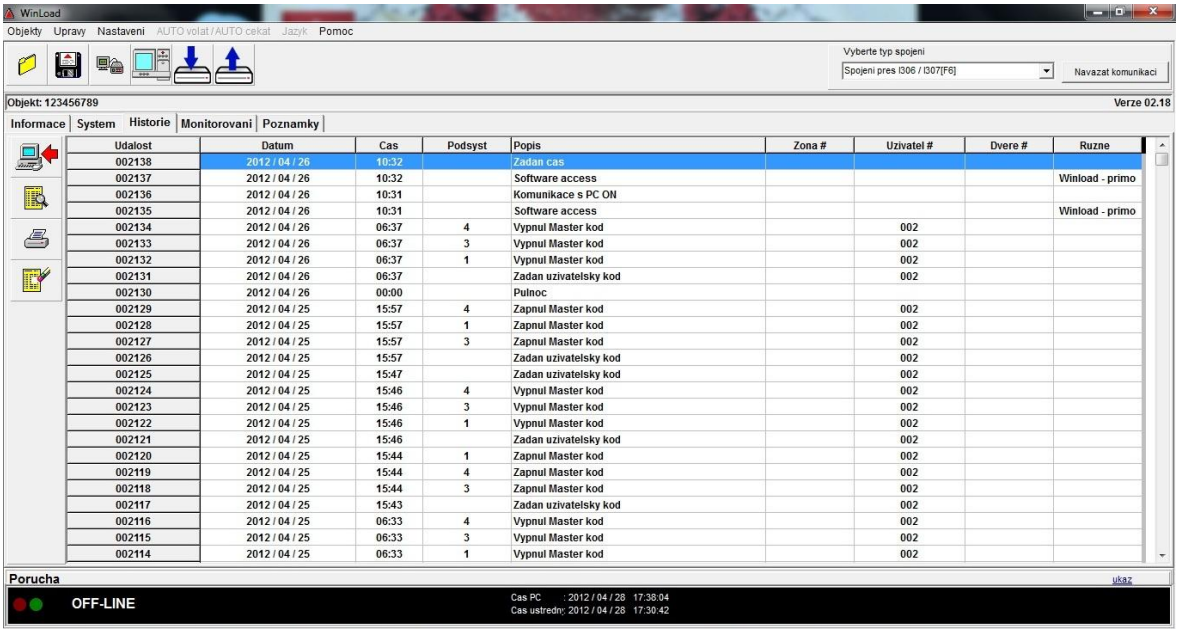
Obrázek 54: Zobrazení narušení objektu

Tato událost se nám samozřejmě zobrazí i na plánku objektu.



Obrázek 55: Narušení zóny v objektu

V položce „Historie“ si můžeme zobrazit všechny zaznamenané informace týkající se ústředny a objektu. Zaznamenává se např. spojení s ústřednou, jaký poplach a na jakém detektoru byl vyvolán, ztráta komunikace se systémem, kódování a odkódování objektu atd.



Obrázek 56: Historie událostí

8.1.4 Shrnutí

Celý objekt jsem zabezpečil pomocí plášťové a prostorové ochrany. Vzhledem k požadavkům zákazníka a to jak po stránce finanční, tak na zabezpečení, jsem zvolil základní zabezpečení pomocí magnetických kontaktů a PIR detektorů. Celý objekt jsem rozdělil, na přání zákazníka, na dva podsystémy, „Podsystém 1 – Global“ a „Podsystém 2 – Byt“. V případě, že budeme opouštět objekt a už v něm nikdo nebude zůstávat, použijeme kód pro „Podsystém 1 – Global“, který jsme si nastavili. V případě, že v pokoji na spaní někdo zůstává, může on sám, nebo my sami použít kód pro „Podsystém 2 – Byt“, čímž se zastřeží celý objekt, kromě části, kde se daná osoba může a bude pohybovat. Konkrétně se jedná o pokoj pro spaní, šatnu, koupelnu, WC.

Pro zakódování „Podsystému 1 – Global“, stiskneme na klávesnici kód 2222 a zadáme ARM. Pro odkódování zase zadáme kód 2222 a stiskneme DISARM. Pro „Podsystém 2 – Byt“, stiskneme 2233 a ARM a pro odkódování 2233 DISARM. Daný objekt můžeme zakódovat i odkódovat i na dálku přes program WinLoad na našem PC.

Výše zmíněné kódy mají jen informativní charakter, pro lepší vysvětlení fungovaní daného systému zabezpečení.

ZÁVĚR

Tématem mé diplomové práce bylo navrhnout a následně realizovat zabezpečení víceúčelového objektu pomocí elektrického zabezpečovacího systému. Před samotným začátkem psaní této práce jsem se domluvil s firmou, která provádí návrh zabezpečení a následně jeho montáž a u které již druhým rokem jsem na brigádě, zda by byla ochotna se mnou spolupracovat a já sám mohl navrhnout a dohlížet na realizace zabezpečení daného objektu. S tímto souhlasil i majitel výše popsaného objektu, se kterým jsem se několikrát osobně setkal a jednotlivé kroky s ním diskutoval.

Na samotném začátku praktické části své diplomové práce jsem popsal daný objekt a jeho okolí, zjistil příjezdové časy a vzdálenost jednotek integrovaného záchranného systému. Následně jsem provedl bezpečnostní posouzení objektu a bezpečnostně technickou obhlídku objektu a jeho okolí, zjistil jeho riziková místa a určil možné způsoby napadení a vniknutí do objektu. Popsal jsem a zhodnotil dosavadní obvodovou ochranu areálu.

V potaz, při stanovení stupně zabezpečení, jsem bral hlavně zabezpečované hodnoty a druh majetku, který se v objektu nachází, jeho atraktivnost pro pachatele a obtížnost jeho krádeže. Významným ovlivňujícím faktorem byly i požadavky vlastníka objektu, který předem jasně stanovil rozpočet, při našich schůzkách mi sdělil své požadavky na zabezpečení, a jak by si ho představoval. Vzhledem ke všem těmto okolnostem jsem zvolil stupeň zabezpečení 2. V objektu se nenacházel žádný elektrický zabezpečovací systém, byly zde jen určité mechanické zábranné systémy a relativně kvalitní obvodové oplocení.

Při samotném návrhu zabezpečovacího systému jsem bral ohled na požadavky vlastníka objektu a na finanční rozpočet, který byl předen zadán. Hlavním přáním bylo jen základní zabezpečení, které se bude nadále rozšiřovat, bezdrátový systém a možnost zakódovat celý objekt, nebo jeho část. Samotný návrh jsem konzultoval s montážní firmou a vlastníkem objektu. Vlastníkovi objektu jsem předložil celkem tři návrhy na zabezpečení objektu pomocí EZS v různých finančních mezích, pod i nad limitem, který byl zadán předem. Všechny tři návrhy musely být pro bezdrátový systém, přičemž třetí návrh obsahoval celkové zabezpečení objektu, bez nutnosti dalšího rozšiřování systému. Po schválení návrhu přišla realizace daného systému. Celou montáž prováděla již zmíněná firma, přičemž jsem osobně dohlížel na průběh montáže a po celou dobu konzultoval umístění jednotlivých prvků tak, aby odpovídaly požadavkům normy a nebyla narušena funkčnost celého systému.

Dále jsem ve své práci, pro větší přehlednost systému, popsal jednotlivé použité prvky, jejich parametry a vlastnosti. Vzhledem k výběru jednoho z mých návrhů vlastníkem objektu, kdy se jedná o základní zabezpečení plášťové a prostorové ochrany, v práci uvádím i další návrhy a možnosti zabezpečení zmíněného objektu.

Aby byly splněny všechny požadavky vlastníka objektu, provedl jsem naprogramování systému pomocí programu WinLoad. Systém jsem rozdělil do dvou podsystémů tak, aby bylo možné zakódovat celý objekt, případně většinu objektu kromě bytové části. K daným podsystémům jsem přidělil příslušné kódy, které byly samozřejmě poté změněny. Celý systém jsem předvedl vlastníkovi objektu a řediteli příslušné pobočky, seznámil je s ovládáním systému a předal veškerou potřebnou dokumentaci a základní manuál pro práci s daným systémem. Celý systém byl následně odzkoušen.

Ke své práci přikládán příslušnou fotodokumentaci objektu, mapové podklady jeho okolí a grafickou dokumentaci, která byla provedena v programu AutoCad, ve kterých je rozmístění jednotlivých prvků. V práci jsou obsaženy i snímky a popisy z jednotlivých kroků při programování pomocí programu WinLoad. V tabulkách jsem uvedl rozměry a popis jednotlivých místností a nakonec i celkový součet prvků a jejich ceny.

ZÁVĚR V ANGLIČTINĚ

The topic of my thesis was to design and subsequently implement an electric alarm system for the multipurpose building. I had a part time job for two years in the company which I chosen and before the start of writing this thesis, I arranged co-operation with a company that performs security design and its assembly to design and oversee the implementation of the security of the object. I gained owner´s agreement with whom I have personally met several times and discussed the steps with him.

At the beginning of the practical part of my thesis I described the object and its surroundings, found out the distance of the Integrated Rescue System units and their arrival times. Then I conducted security assessments and security-building technical tour of the building and its surroundings, he found his place of risk and determine possible methods of attack and intrusion into the building. I have described and evaluated existing circuit protection of area.

When i was setting the security level, I took particular values and ensured the kind of property that is located in the building, its attractiveness for the offender and the difficulty of theft. An important influencing factors were the requirements of the owner of the building, who previously set budget at our meetings and told me his security requirements and how he had imagined that. Taking all these factors, I chosen the second level of security. There was not located any electric security system in the building, there were only a mechanical barrier systems and perimeter fencing is relatively good.

When I was arranging the security system, I took into account the requirements of the owner and the financial budget, which has been previously specified. The main wish was just a basic security, which will continue to expand wireless and the ability to encode the entire object or part. The proposal itself, I consulted with the installation company and the owner of the building. I presented three proposals for building security to the area owner with intrusion in certain financial limits below and above the limit that was specified in advance. All three proposals had to be wireless, and third proposal included the overall security of the building, without the need for another system expansion. When was proposal approved, we came to the realization of the system. The entire installation carried out the aforementioned company and I personally supervised the installation process and consulted throughout the placement of individual elements to fulfill the requirements of functionality and not disturb the whole system.

Furthermore I described in my thesis the various elements which was used, thein characteristics and properties.

I have made programming using Winload system in order to fulfill all requirements of the owner. I have divided the system into two subsystems, so that it can encode the entire object, or a majority of the residential building addition. The subsystems by the relevant codes assigned to I, which were then changed of course. I performed the entire system to the owner and director of the branch, made them familiar with control system and forwarded all necessary documentation and a basic manual for working with given system. The whole system was subsequently tested.

I attach to the corresponding photographs of the building, its surroundings maps and graphic documentation that was done in AutoCad program in which the distribution of individual elements. The paper also contains photos and descriptions of individual programming steps using Winload. I mentioned in the tables dimensions and description of each room and finally the total elements and their prices.

SEZNAM POUŽITÉ LITERATURY

[1] ČANDÍK, Marek. *Objektová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 80-731-8217-3.

[2] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. Učební texty vysokých škol (Univerzita Tomáše Bati ve Zlíně). ISBN 978-80-7318-554-1 (BROž.).

[3] ČSN EN 50 131-1. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007.

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

[5] VALOUCH, PH.D., Ing. Jan. *Projektování integrovaných systémů*: *Bezpečnostní analýza*. Přednáška. Zlín, 2011.

[6] STASANET.cz: bezpečnostní technologie. *Digiplex EVO-192* [online]. 27.10.2006 [cit. 2012-04-19]. Dostupné z: <http://www.stasanet.cz/paradox-digiplex/paradox-digiplex-ustredny/digiplex-evo-192-3.html>

[7] STASANET.cz: bezpečnostní technologie. *RTX3-433/868* [online]. 27.10.2006 [cit. 2012-04-19]. Dostupné z: <http://www.stasanet.cz/paradox-spectra/bezdratova-nadstavba-magellan/rtx3-433-868-2.html>

[8] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *PCS200 - GSM/GPRS KOMUNIKÁTOR* [online]. [cit. 2012-04-19]. Dostupné z: <http://www.eurosat.cz/4022-pcs200-gsm-gprs-komunikator.html>

[9] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *MG-PMD1P* [online]. [cit. 2012-04-19]. Dostupné z: <http://www.eurosat.cz/415-mg-pmd1p.html>

[10] STASANET.cz: bezpečnostní technologie. *DCT10-433/868* [online]. 27.10.2006 [cit. 2012-04-20]. Dostupné z: <http://www.stasanet.cz/paradox-magellan/bezdratova-nadstavba/dct10-433-868.html>

[11] EUROSAT cs: Specializovaný velkoobchod na zabezpečovací technologii. *LCD KLÁVESNICE K641 (DGP2-641BL)* [online]. [cit. 2012-04-20]. Dostupné z: <http://www.eurosat.cz/217-k641-dgp2-641bl.html>

[12] STASANET.cz: bezpečnostní technologie. *Vnitřní sirény* [online]. 03.07.2008 [cit. 2012-04-20]. Dostupné z: <http://www.stasanet.cz/zabezpecovaci-systemy/vnitrni-sireny/2.html>

[13] STASANET.cz: bezpečnostní technologie. *BOX VT (BOX V-40, BOX V-80)* [online]. 01.07.2008 [cit. 2012-04-20]. Dostupné z: <http://www.stasanet.cz/zabezpecovaci-systemy/boxy-a-prislusenstvi2/box-vt-box-v-40-box-v-80.html>

[14] STASANET.cz: bezpečnostní technologie. *Akumulátory* [online]. 30.06.2008 [cit. 2012-04-20]. Dostupné z: <http://www.stasanet.cz/zabezpecovaci-systemy/akumulatory/akumulatory-2.html>

[15] STASANET.cz: bezpečnostní technologie. *INTERFACE 307* [online]. 01.07.2008 [cit. 2012-04-20]. Dostupné z: <http://www.stasanet.cz/paradox-magellan/moduly-magellan/interface-307.html>

[16] UHLÁŘ, Jan. *Technická ochrana objektů*. 1. vyd. Praha: Policejní akademie České republiky, 2001, 205 s. ISBN 80-725-1076-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

MZS	Mechanické zábranné systémy.
PPC	Přijímací poplachové centrum.
EZS	Elektrické zabezpečovací systémy.
IAS	Intruder Alarm System.
I&HAS	Intruder And Hold-Up Alarm System.
HAS	Hold-Up Alarm System.
CENELEC	Evropská komise pro normalizace v elektrotechnice.
IEC	Mezinárodní výbor pro elektrotechniku.
NBÚ	Národní bezpečnostní úřad.
PČR	Policie České republiky.
PIR	Pasivní infračervený senzor.
ČSN	Česká státní norma.
LED	Light-Emitting Diode.
USB	Universal Serial Bus.
COM	Component Object Model.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK