Návrh a realizace komplexního zabezpečení prodejny a zázemí zahradnické firmy Acris

Design and realization of complete security of Acris company

Bc. Radovan Václavek

Diplomová práce

2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky
akademický rok: **2009/2010**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Radovan Václavek**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh a realizace komplexního zabezpečení prodejny a zázemí zahradnické firmy Acris**

Zásady pro vypracování:

1. **Proveďte zhodnocení rizik proti negativním vlivům na areál**
2. **Navrhněte optimální řešení ostrahy a ochrany objektu.**
3. **Vyberte jednotlivé prvky zabezpečení a popište jejich činnost**
4. **Zhodnoťte možnost na pojení na PCO bezpečnostní agentury.**
5. **Ověřte funkci a nastavení jednotlivých prvků po instalaci.**
6. **Proveďte testování systému formou narušení a vyhodnoťte účinnost jednotlivých prostředků**
7. **Vyhodnoťte systém ochrany a navrhněte případné změny technického zabezpečení**
8. **Práci doplňte grafickou a obrazovou dokumentací**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. KINDL, Jiří. Projektování bezpečnostních systémů. I, Zlín : Univerzita Tomáše Bati ve Zlíně, 2.vydání 2007. 134 s. ISBN 978-80-7318-554-1

2. KŘEČEK, Stanislav. Příručka zabezpečovací techniky, Praha, Cricetus, 4.vydání 2002. 350 s. ISBN 80-902938-2-4

3. UHLÁŘ, Jan. Technická ochrana objektů II. díl - Elektrické zabezpečovací systémy. Praha: PA ČR, 2001. 208 s. ISBN 80-7251-076-2.

4. ČERNÝ, Josef, IVANKA, Ján. Systemizace bezpečnostního průmyslu. 1. vyd. Zlín: UTB, 2006. 135 s. ISBN 80-7318-402-8

5. ČANDÍK, Marek. Objektová bezpečnost II. 1. vyd. Zlín: Univerzita Tomáše Bati, 2004. 100 s. ISBN 80-7318-217-3

6. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. 1. vyd. Zlín: Univerzita Tomáše Bati, 2003. 64 s. ISBN 80-7318-119-3.

7. VLČEK, Jiří. Bezpečnost elektrických zařízení: příručka pro konstruktéry. 1. vyd. Praha : BEN - technická literatura, 2007. 109 s. ISBN 978-80-7300-222-0

Vedoucí diplomové práce: **Ing. Jiří Pálka**
Ústav elektroniky a měření

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.
①

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Má diplomová práce je komplexním řešením zabezpečení firmy s využitím současných bezpečnostních prvků a prostředků dostupných na trhu a zároveň odpovídající finančním požadavkům investora s ohledem na materiální hodnoty v chráněném areálu. Součástí je také fotodokumentace a několik příloh, které dokumentují samotnou instalaci, která je také součástí projektu a samozřejmě i finální podoba zabezpečeného areálu.

Klíčová slova: zabezpečení areálu, zabezpečovací technika, kamerový systém, optické závory, bezpečnostní systémy

ABSTRACT

This diploma work is complete solution of design and realization of electronic security system of the ACRIS Company. I designed it by the latest technology with using of hi-tech safety elements in accordance with investor financial needs. We also take into consideration values of secure goods, buildings and other areas.

There are some pictures in attachments which show installation process and final accomplishment of whole security system.

Keywords: Electronic security signalisation, detectors, cctv, opto-electronic sensor,

Na tomto místě bych rád poděkoval vedoucímu mé bakalářské práce Ing. Jiřímu Pálkovi, za odborné vedení, rady a připomínky, které mi poskytoval během vzniku této práce.

Dále vedoucímu servisního střediska firmy System plus panu Romanu Nábělkovi za úzkou spolupráci při návrhu a realizaci praktické části projektu.

A v neposlední řadě firmě ACRIS zahrady s.r.o, za umožnění návrhu a realizace tohoto projektu.

Ve Zlíně, 13.6.2010 .....

podpis diplomanta

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

V této diplomové práci chci na základě nabitých znalostí ze studia mého oboru a současně s využitím mých praktických zkušeností, navrhnout celkový koncept zabezpečení areálu zahradního centra ACRIS, v souladu s trendy v zabezpečovací technice a s požadavky investora.

Po nastudování tohoto materiálu bychom měli získat odpovědi na řadu otázek, které nás v oblasti zabezpečování průmyslových areálů či prodejen mohou napadnout. Postupně informuji o jednotlivých prostředcích, které navrhuji použít pro daný úsek a zároveň vždy stručně popisuji, na jakých základních principech jednotlivé prvky pracují. Dále také zdůvodňuji volbu jednotlivých prvků a nastiňuji další možné varianty. Další část je pak věnována realizaci a samotnému odzkoušení jednotlivých prvků. Následně popisuji různé způsoby simulovaného narušení objektu. Toto narušení pak vyhodnocuji a navrhuji případné opatření nebo řešení. Jako přílohy jsou nafoceny jednotlivé zabezpečovací prvky po jejich nainstalování, průběh samotné instalace, dále mapa areálu a fotodokumentace objektu.

Mojí snahou bylo napsat práci tak, aby byla srozumitelná nejen odborníkům z řad pracovníků zabezpečovacích firem, ale i studentům nebo laikům. Tento text může v budoucnu posloužit jako návod pro navržení zabezpečení podobného typu průmyslového areálu nebo prodejny a také dokumentuje praktické využití zabezpečovací techniky.

I. TEORETICKÁ ČÁST

1. ZHODNOCENÍ RIZIK PROTI NEGATIVNÍM VLIVŮM NA AREÁL

Firma ACRIS zahrady s.r.o. byla založena na počátku roku 2007 jako nástupnická organizace firmy Ing. Martin Přibyl. Zkušenosti v oblasti sadových úprav sahají až do roku 2001, kdy po ukončení studia zakladatele firmy na MZLU v Brně, Zahradnické fakultě v Lednici na Moravě, firma vznikla. Činností firmy je projekce, realizace a údržba zeleně, závlahových systémů a přírodních koupacích biotopů. Zpracovává komplexní řešení a engineering stavby. Hlavní myšlenkou firmy je udržení vysoké kvality prováděných prací s důrazem na individuální, odborný přístup k jednotlivým zadáním a dodržování vhodných technologických postupů. V duchu této myšlenky se chtějí i nadále odlišovat od konkurence. Spolupracují s předními odborníky v oboru. Projektovou část zajišťují renomovaní zahradní architekti, kteří zpracovávají kompletní projekt okolí stavby či domu včetně návrhu použitých materiálů, tvarů a sortimentu rostlin. V návaznosti na zpracovaný projekt zajišťuje firma realizaci vč. terénních úprav a modelací terénu.

Další oblastí jsou automatické závlahové systémy a přírodní koupací biotopy (koupací jezírka). U již realizovaných projektů zajišťují celkovou údržbu. Zde zdůrazňují, že je nutné mít na paměti, zahrada je živý celek, který se neustále vyvíjí a roste. Proto je potřeba s okrasnou zahradou neustále pracovat a pečovat o ni.

Další činností firmy je malo i velkoobchodní prodej mulčovací kůry, zahradního materiálu a rostlin. V zajímavém industriálním prostředí zlínské části Rybníky pro zákazníky 20. března otevřeno zahradní centrum. Zde najdeme jedinečný sortiment rostlin a zahradního materiálu. K dispozici a konzultacím je pro zákazníky odborný personál, který bude řešit jejich požadavky na místě. V případě zájmu zpracují zadání zákazníka včetně projekce, cenové kalkulace a realizace.

Prodejní areál a zázemí se nachází v centru Zlína v jeho průmyslové části, bývalé společnosti Svit, část Rybníky. Jedná se o otevřenou plochu mezi dalším průmyslovými budovami a plochami. Plocha, kterou máme zabezpečit je souvisle obklopena ze dvou stran budovami. Tento areál je v současné době v postupné restrukturalizaci a jde o pozůstatek bývalého gigantu obuvnického závodu Svit, který zkrachoval. Areál v mnohých částech chátral a stával se často vyhledávanou lokalitou sběračů kovů a podobně. Nyní probíhá jeho postupná oprava a získává nové využití i z důvodu, že se jedná o relativně atraktivní lokalitu blízko samotného centra města Zlína.

Přední a zadní přístupové části námi zabezpečovaného prostoru jsou oplocené a opatřené vjezdovými bránami a vstupní brankou. Na samotné ploše se pak nachází kontejnery a stoly s okrasnými dřevinami a jiným prodejním sortimentem a také zde budou v jednotlivých okrajích parkovat vozidla a další zemědělské mechanismy firmy. Vprostřed levé části areálu je umístěna garáž s pracovním nářadím. V čelní přístupové části pak prodejna a kanceláře s šatnami pracovníků. Vše je podrobně rozkresleno ve výkresové části příloh a zobrazeno v příloze.

Abychom mohli navrhnout odpovídající zabezpečení, je třeba se pokusit co nejlépe analyzovat jednotlivé rizika a zvolit odpovídající stupeň zabezpečení. To je třeba provést nejen na základě zjištěných skutečností, ale také s ohledem na požadavky investora. Dále jsou definovány jednotlivé stupně zabezpečení, tak jak je uvádí norma ČSN EN.

1.1. Stupně zabezpečení

Pro poplachové systémy se jedná o skupiny norem rady ČSN EN 5013x, jejichž části jsou postupně zpracovávány a vydávány z evropských norem rady EN 5013x. U těchto norem se problematikou montáží zabývá vždy část 7 tedy ČSN EN 5013x-7 nazvaná aplikační směrnice.

Poplachové systémy dělíme do následujících skupin norem:

- ČSN EN 50130 Poplachové systémy: Všeobecně;
- ČSN EN 50131 (334590) Poplachové systémy: Elektronické zabezpečovací systémy (EZS);
- ČSN EN 50132 (334582, 334583) Poplachové systémy: CCTV sledovací systémy pro použití v bezpečnostních aplikacích;
- ČSN EN 50133 (334593) Poplachové systémy: Systémy kontroly vstupu pro použití v bezpečnostních aplikacích (ACS);
- ČSN EN 50134 (334594) Poplachové systémy: Systémy přivolání pomoci (SAS);
- ČSN EN 50136 (334596) Poplachové systémy: Poplachové přenosové systémy a zařízení (ATS).

EPS se zabývá ČSN EN 54 (34 2710), jejíž části jsou opět postupně zpracovávány a

vydávány z evropské normy EN 54.

Zabezpečení EZS rozdělujeme dle normy ČSN EN 50131-1 do 4 stupňů. Přičemž 1. stupeň je stupněm základním a jako nejvyšší je stupeň 4. Při zařazování chráněných objektů nám může pomoci charakteristika jednotlivých stupňů, tak jak je uvedena v samotné normě ČSN. Naším úkolem je potřeba pokusit se co nejlépe zhodnotit jednotlivé rizika a zvolit odpovídající stupeň zabezpečení. To je třeba provést nejen na základě zjištěných skutečností, ale je také třeba vzít v potaz požadavky investora.[3]

1.1.1. Stupeň 1: Nízké riziko

(rodinné domky, garáže, kiosky, byty, chaty atd.)

Předpokládá se, že narušitelé mají malou znalost EZS a že mají k dispozici omezený sortiment snadno dostupných nástrojů.

1.1.2. Stupeň 2: Nízké až střední riziko

(obchodní domy, prodejny, sklady spotřebního zboží atd.)

Předpokládá se, že narušitelé mají určité znalosti o EZS a že použijí základní sortiment nástrojů a přenosných přístrojů.

1.1.3. Stupeň 3: Střední až vysoké riziko

(banky, sklady zbraní, opiátů atd.)

Předpokládá se, že narušitelé jsou obeznámeni s EZS a mají úplný sortiment nástrojů a přenosných elektronických zařízení.

1.1.4. Stupeň 4: Vysoké riziko

(jaderné elektrárny, sklady výbušnin, velké galerie atd.)

Používá se tehdy, když zabezpečení má prioritu před všemi ostatními hledisky Předpokládá se, že narušitelé jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků v EZS.[3]

Pokud je systém EZS rozdělen do jasně definovaných subsystémů, EZS může zahrnovat komponenty různých stupňů v každém subsystému. Stupeň subsystému je určen nejnižším stupněm v něm použitého komponentu. Stupeň celého systému EZS je určen

nejnižším´stupněm jeho subsystému. Komponenty, které jsou společné pro více subsystémů, musí mít stupeň nejméně stejný jako subsystém nejvyššího stupně.

EZS musí mít stanoveno stupeň zabezpečení, který určuje následující: oprávnění, přístupové úrovně, provozování, vyhodnocení, detekce, hlášení, napájení, zabezpečení proti sabotáži, monitorování propojení, záznam události.

1.2. Volba kategorie zabezpečení objektu

Volba kategorie zabezpečení objektu se provádí několika způsoby:

- Volí si ji zákazník – převážně s ohledem na finanční možnosti a s přihlédnutím na hodnotu zabezpečovaného majetku.
- Doporučuje instalační firma – technik instalační firmy vychází z praktických zkušeností a doporučuje to nejvhodnější pro daný typ objektu a hodnotu zabezpečovaného majetku.
- Kategorie je stanovena třetí stranou – může se stát, že objekt má strategické, finanční nebo jiné využití, kde je vysoká pravděpodobnost, že by mohl být napaden. V tomto případě může být kategorie předepsána další stranou, například pojišťovnou, vnitřní směrnicí nebo normou. V takovém případě je popis a instalace upravena příslušnou normou.

1.3. Vyhledání a zhodnocení dalších známých rizik

Bezpečnostní analýza obsahuje souhrn bezpečnostních poznatků ovlivňujících podstatným způsobem střežení, hlídání objektu. Samotné umístění areálu a jeho okolí jsme již popsali výše. Areál zahradního centra Acris se nachází ve zmiňovaném průmyslovém komplexu, které má v noci sice pouze jeden vjezd s vrátnicí, ta ale v současné době nefunguje. Dalším důležitým faktorem je hodnota chráněného majetku, nebo-li možnost přímých škod, ale také pro firmy velmi důležité sekundární následky – nemožnost činnosti v případě poškození nebo odcizení výrobních prostředků.

S tím také souvisí charakter chráněného objektu a hmotných věcí v areálu umístěných. Mým úkolem nicméně nebyla úplná komplexní bezpečnostní analýza, ale jen projekt samotného technického zabezpečení areálu a hmotných statků proti případné krádeži, vloupání, napadení personálu nebo vandalismu.

Vzhledem k nabitým znalostem při studiu a také po konzultacích s pracovníky zabezpečovací firmy, se kterými jsme spolupracovali, jsme se snažili zohlednit i jiné známé rizikové faktory.

Po několika konzultacích s majiteli firmy, kdy jsme vyhodnotili všechny rizika možných škod a jejich význam pro samotný chod firmy, důkladném zmapování areálu a jednotlivých objektů, které se v něm nacházejí, jsme dospěli k žádanému kompromisu mezi kvalitou a úrovní zabezpečovací techniky a samotnými možnostmi investora. Navrhli jsme v rámci možností co nejdokonalejší zajištění areálu a zohlednili jsme i nejdůležitější zóny ochrany. Identifikovali jsme slabá místa a ta jsme se snažili zvolenými prostředky zabezpečit.

Ve volbě jednotlivých komponentů elektronického zabezpečovacího systému hrála důležitou roli také jejich cena. Snažili jsme se maximálně využít rozumného poměru mezi kvalitou, spolehlivostí, účinností a náklady zvolených komponentů.

1.4. Komplex ochrany areálu (objektu)

Komplex ochrany areálu je soubor konkrétních praktických opatření, které slouží k zajištění ochrany celého areálu. Standardně se skládá z několika níže uvedených bodů.

1.4.1. Bezpečnost osob

(klientů i vlastního personálu)

Hodnotíme rizika při násilných přepadech jako je teror, loupež a nenásilné případy jako jsou vydíraní, požár, havárie a rizika při běžné pracovní činnosti. Zde se budeme v našem případě zabývat pouze rizikem přílišné hotovosti na pokladně prodejny, případně hotovosti v kancelářích, která je umístěna v kanceláři. Tato pravděpodobnost je ale dle vyjádření majitelů firmy velmi nízká a proto jsme v tomto směru navrhli jen pro zabezpečení personálu při přímé manipulaci s penězi na pokladně a to za pomoci skrytého emergency tlačítka u prodejního pultu. Další riziko je možnost vzniku požáru v kancelářích firmy, což by mělo vážné jak primární tak sekundární následky. Samotná EPS ovšem nebyla majiteli požadována, až na naše doporučení ovšem využili alespoň detektorů kouře do prostorů kanceláře.

1.4.2. Bezpečnost majetku

(jak majetku klientů tak i vlastního při násilných případech – loupež tak i nenásilných – krádeže, podvody, požáry, havárie, běžné pracovní nebo podnikatelské činnosti)

Bezpečnost majetku je primární úkolem celé práce. Optimální zpracování problematiky technické bezpečnosti je jádrem celého projektu. Zde jsme zvažovali hodnoty jednotlivých nemovitých věcí, které se mohou v areálu nacházet (rostliny v kontejnerech, ruční a jiné nářadí v garáži, vybavení a finanční hotovost v kancelářích), možnosti vlastního zabezpečení jednotlivých věcí nacházejících se v areálu (stroje a možnosti jejich vlastního zabezpečení), zabezpečení prodeje (krádeže na prodejní ploše) a případné přímé ohrožení prodávajícího personálu při manipulaci s penězi. Dále zabezpečení v případě nepřítomnosti pracovníků tj. vloupání do objektu a následné krádeže nebo poškození zboží nebo prostředků firmy. Vyhodnocovali jsme způsoby možného neoprávněného vniknutí do areálu a s tím související možnosti škod. Na základě těchto analýz a rozborů jsme navrhli jednotlivé prvky zabezpečovacího systému a námi chráněný areál jsme i v souladu s požadavky investora zařadili do stupně 2.

1.4.3. Bezpečnost informací

Bezpečnost informací a to informací o klientech i o vlastních zaměstnancích při narušení spolehlivosti faktorů, neúmyslným působením vlastního personálu, úmyslným působením vlastního personálu a jiných osob je dalším faktorem, který bylo třeba zvážit, ale opět není součástí projektu. Informovali jsme klienta o možných rizicích v tomto směru. Společně s majiteli jsme probrali všeobecné zásady při práci s citlivými daty, vstupními kódy a dalšími informacemi ohledně zabezpečení směrem k zaměstnancům.

2. OPTIMALIZACE OSTRAHY A OCHRANY OBJEKTU

Cílem objektové ochrany je ochránit objekt, prvotně však v něm žijící nebo pracující osoby, a dále pak uložený majetek před násilnou činností, zcizením, poškozením, neoprávněnou manipulací a požárem. Rozeznáváme čtyři základní druhy ochran: klasická, technická, fyzická a režimová. EZS, CCTV i ostatní poplachové systémy patří do ochrany technické. Realizace jakékoli z těchto ochran znamená, že uživatelé musí přizpůsobit své chování určitým podmínkám, a tím jsou v určitém směru omezováni. Technická ochrana, realizována EZS, je navrhována pro zjištění narušení střeženého objektu nebo prostoru případným pachatelem (příp. skupinou pachatelů). Pachatel je však při návrhu ochrany neznámý, ale zvážení jeho možného chování je z hlediska návrhu zabezpečení zásadní. Proto je třeba znát tři základní kritéria rozhodování pachatele:

• očekávaná kořist (předpokládaná, zjištěná);

• technická náročnost provedení loupeže;

• riziko odhalení.

Z těchto kritérií lze vycházet pro sumarizaci faktoru, které mají pro pachatele přitahující nebo odpuzující účinek. V případě omezení přitahujících účinku a zajištění co největšího poctu odpuzujícího účinku klesá riziko napadení střeženého objektu. Bohužel ne u všech objektu toto lze realizovat a zajistit.

Faktory, které mají na pachatele přitahující účinek:

• husté vysoké ploty a zdi;

• optická izolace podobnými konstrukcemi v sousedství;

• vzdálenost od pohybu osob;

• otevřená a nezajištěná okna i dveře;

• znaky dlouhodobé nepřítomnosti;

• nepořádek v okolí objektu;

• nářadí na místě.

Faktory, které mají na pachatele odpuzující účinek:

• volný výhled na objekt a přilehlý pozemek;

• dobré vztahy se sousedy;

• přítomnost obyvatel;

• přítomnost psa;

• viditelně instalovaný systém EZS (sporné - dle aplikace);

• výstražné tabulky o ochraně objektu (sporné - dle aplikace).

Je nutné si uvědomit, že EZS ani ostatní poplachové systémy nezabrání pachateli v násilné činnosti. Systém EZS tedy „pouze“ detekuje a indikuje přítomnost, vstup nebo pokus o vstup pachatele do střežených objektů. Logicky tedy na tuto indikaci - poplachovou informaci, musí navazovat fyzická ochrana, ať už realizovaná náhodně (náhodní svědci), svépomocí (sám majitel) nebo smluvně – smluvně ošetřeno (PCO). Proto návrh EZS musí být přizpůsoben tomu, kam se bude přenášet poplachový signál, kdo a hlavně za jak dlouho bude schopen na tyto poplachové informace reagovat. Návrh EZS je složitým komplexem vzájemně provázaných činností. [1], [2]

2.1. Požadavky na zabezpečení

Po předcházejícím průzkumu a konzultacích s majiteli firmy nám vyšly následující požadavky na zabezpečení.

- mechanické zabezpečení areálu, kanceláří a skladu;
- signalizace narušení vnějšího pláště areálu (oplocení, plotu);
- signalizace nedovoleného pohybu osob v zabezpečeném areálu;
- signalizace vniknutí do administrativních prostor a prostor zázemí;
- signalizace napadení obsluhy u prodejního pultu v kanceláři;
- záznam obrazové informace o pohybu v zabezpečeném i otevřeném areálu;
- poplachové a případně další informace přenášet přes rádiovou síť na pult centrální ochrany, nebo volitelně přes mobilní síť, na telefony majitelů;
- umožnit vzdálený přístup k nahlédnutí pro obrazové informace snímané kamerovým systémem, pro pult centrální ochrany a pro majitele.

2.2. Obecný návrh řešení

Obě otevřené strany areálu jsou oploceny pletivem a v jeho horní části jsou pak nataženy tři ostnaté dráty. Ke vstupu do areálu slouží branka pro chodce a dále dvě velké vjezdové brány. Na základě doporučení jsme pro mechanické zabezpečení těchto vjezdových bran a vstupů do kanceláří zvolili odpovídající zámky a doporučili nainstalování ostnatých drátů nad pletivo.

Jako doplnění k těmto mechanickým zábranám na vchodových vratech a dveřích pak použít vratové magnety. Informace z těchto magnetů pak budou součástí vyhodnocování EZS. Jako hlavní ústřednu navrhujeme AMOS 1600.

K této ústředně pak dále připojíme pro perimetrickou ochranu areálu tři optické infrazávory. Jedna bude zajišťovat západní bránu od nižší budovy a další dvě budou zajišťovat do kříže proti sobě, prostor před východní bránou areálu až k okrajům budov, které tvoří další přirozenou ochranu areálu. Tyto infrazávory společně s mechanickými zábranami (oplocení, brány) a přirozenou ochranou okolních budov nám budou sloužit jako základní perimetrická ochrana areálu.

Dále otevřenou plochu prodejny zajistíme v oblastech největší kumulace zboží kombinovanými PIR –MW detektory. Pro naše účely budou dostačovat tři detektory umístěné od středu areálu a pokrývající nejexponovanější plochy areálu. Volíme tento typ detektorů s ohledem na jejich vlastnost, kdy mohou účinněji rozlišovat pohyb zvířat v objektu od pohybu člověka a tím umožňují výrazně eliminovat vznik falešných poplachů. To následně sníží také počet případných zbytečných výjezdů zásahové jednotky poskytovatele trvalé ostrahy. Jelikož budou tyto zařízení umístěny ve venkovním prostředí, musíme volit detektory s odpovídající odolností a krytím.

K zajištění proti průniku do uzavřených prostor kanceláří a skladů doplníme EZS o další čtyři detektory. V tomto případě nám již postačí levnější prostorové pasivní infračervené detektory, protože v těchto prostorech neočekáváme možnost výskytu pohybu drobných zvířat a nehrozí tak zbytečné falešné poplachy. Po jednom budou umístěny v prodejně, kanceláři, šatně a v garáži sloužící jako sklad materiálu a výrobních prostředků. To nám také umožní po napojení na ústřednu definovat jednotlivé zóny, které potřebujeme podle oprávnění jednotlivých pracovníků v těchto prostorech nastavit.

Pro přenos poplachových informací bude primárně sloužit rádiová síť v pásmu 496MHz poskytovatele trvalého střežení objektu. Připojení bude realizováno přímo

z instalované ústředny zabezpečovacího systému AMOS 1600. Součástí této ústředny je vysílač pro danou frekvenci a ústředna je také vybavena vlastní anténou. Pro případ výpadku napájení je zařízení vybaveno záložní baterií s odpovídajícím výkonem.

Jako možnou alternativu navrhujeme pro náhradní přenos poplachu záložní IP modul GPRS s vysílačem NAM 1600. Nepřímou podporou mohou být tři světla opatřená infračerveným senzorem pohybu, která budou za snížené viditelnosti a tmy přisvětlovat venkovní prostory areálu.

Případná hotovost bude umístěna v příručním trezoru s odpovídající odolností umístěném v kanceláři. Zde bude u prodejního pultu nainstalované skryté výklopné nouzové tlačítko napojené přes ústřednu na pult centrální ochrany. Jako doplnění proti požadavkům majitele doporučujeme nainstalovat do kanceláří a skladu kombinované kouřové a optické požární kouřové hlásiče, nicméně požární zabezpečení bude pravděpodobně řešit samostatný projekt. Dalším doplňkovým kanálem pro přenášení informací je také Wi-Fi připojení a to především pro přenos obrazu z dohledového kamerového systému.

Dalším, v tomto případě jen doplňkovým prvkem celého komplexu opatření, bude dohled kamerového systému na prostory areálu prodejny. Tento systém vzhledem k náchylnostem na falešné poplachy u takovéhoto charakteru prostředí a druhu zboží umísťované na prodejně bude na doporučení odborníků ze spolupracující firmy pouze doplňkový a nebude sloužit k vyhlášení poplachu. Vzhledem k ceně budou nainstalovány pouze dvě kamery s infračerveným přísvitem a vyhříváním. Kamery budou vybaveny odpovídajícím objektivem a budou zabírat areál zahradnictví z jednoho místa. Konkrétně volíme jejich umístění na konzole, na střeše kanceláře ve výšce asi pěti metrů. Předpokládáme, že z tohoto místa pokryjí svým záběrem s použitím zvolených objektivů téměř celý areál. Kamery budou v trvalém provozu a poslouží tak zároveň jako dohledový systém v době prodeje. Toho mohou využít ´pro kontrolu přes internetové rozhraní a pod příslušnými oprávněními jak majitelé firmy, tak i dispečink agentury zajišťující trvalé střežení areálu. V případě sledování informací z kamerového systému pultem centrální ochran půjde především o prověření případných příchozích poplachů z ústředny EZS před, samotným výjezdem zásahové skupiny.

Záznamy z obou kamer mohou být ve zvolené kvalitě a v různě dlouhé nastavené smyčce ukládány na odpovídající záznamové zařízení. I toto zařízení společně s kamerami je připojeno na záložní baterie a jejich narušení nebo případná ztráta video signálu bude

vyhodnocováno ústřednou EZS jako narušení zabezpečení objektu. Záznam z obou kamer bude v reálném čase přístupný přes zabezpečené připojení pomocí internetového rozhraní.

Dalším ideálním a nezbytným krokem je trvalé napojení na pult centrální ochrany. Celý zabezpečovací systém je s tímto účelem budován a samozřejmě s touto variantou počítá. Tento úkol jsme spolu s majiteli řešili za pomoci výběru vhodné bezpečnostní agentury. Vybrali pro nás zřejmě nejvýhodnější nabídku od firmy zabývající se trvalou ostrahou, která sídlí pouhé dva kilometry od zabezpečovaného areálu. To je vzhledem ke kvalitě nabízené služby a ceně poskytovaných služeb, dojezdovému času ochranné služby velmi výhodná kombinace. Krátkým dojezdovým časem zásahové skupiny poskytovatele nepřetržité ostrahy, totiž minimalizujeme možnost vzniku velmi vysokých škod v případě násilného vniknutí na plochu zahradnictví, nebo minimalizujeme riziko při napadení obsluhy.

Napojení na pult centrální ochrany se v současném průmyslu komerční bezpečnosti považuje za zcela běžné a pro prodejní a provozní areály s uloženým zbožím volně na ploše dnes už téměř jako nezbytné. A to především v případech kdy firma nemá vlastní ostrahu. V každém případě je ale nutné, dbát na pečlivý výběr agentury poskytující tyto služby. Jako vodítko nám mimo jiné posloužilo i doporučení známých a pak také doložení jejich odborné způsobilost patřičnými certifikáty a osvědčeními.

3. SHRNUTÍ TEORETICKÉ ČÁSTI

Tato diplomová práce má za úkol řešit komplexní zabezpečení prodejního areálu zahradnické firmy od mechanických zábran přes elektronickou zabezpečovací signalizaci až po kamerový systém s možností vzdáleného přístupu.

V teoretické části se zabýváme obecně podmínkami pro zabezpečování a ostrahu komerčních objektů. Seznamujeme se s normami pro zabezpečování různých druhů objektů a prostor a také jejich členěním dle norem ČSN.

Dále je uvedeno z čeho vycházíme v návrhu jednotlivých prvků a jsou popsány důvody, které nás vedly k volbě výše uvedených součástí elektronického zabezpečovacího systému. Popisuji celkový koncept, který volíme při komplexním zabezpečení areálu a uvádíme zvolené zařízení.

V praktické části budou popsány konkrétní vybrané prvky zabezpečení areálu a jejich základními vlastnosti. Následně se budeme zabývat samotnou realizací a také nastavení celého zabezpečovacího systému. Na základě provedené analýzy a konzultací, budou nainstalovány výše zvolené a popsané prvky. Instalace bude provedena ve spolupráci s certifikovanou firmou v oboru pod vedením hlavního servisního technika.

Po nainstalování provedeme spuštění systému a jeho nastavení. Pomocí imitace reálných narušení střeženého objektu se pokusíme vyhodnotit účinnost všech součástí EZS. Tyto útoky vyhodnotíme jednotlivě a navrhneme případná opatření pro zlepšení kvality ostrahy areálu.

II. PRAKTICKÁ ČÁST

4. TECHNICKÉ PROSTŘEDKY PRO OCHRANU AREÁLU

Podle výše uvedeného rozboru volíme jednotlivé technické prostředky k zajištění areálu. Začínáme od mechanických zábran přes EZS a jeho součásti, až po doplňkový CCTV systém.

4.1. Mechanické zábrany

Mechanické zábrany patří k základním prvkům ochrany majetku a osob. Jejich úkolem je třeba po určitou dobu odolávat hlavně destruktivním metodám. Samotné překonávání tohoto prvního stupně ochrany je li dostatečné, často dokáže odradit útočníka od vniknutí do areálu nebo chráněných prostor. Policejní statistiky často uvádějí, že pokud se útočníkovi nepodaří do deseti minut zdolat první zábranu, často pak od dalšího pokračování akce ustoupí. Doba nutná k překonání mechanického zábranného systému je určitým kritériem bezpečnostní třídy vybraného mechanického zábranného systému.

Do mechanických zábranných systémů patří:

- vnější oplocení objektu (ploty, zdi, vrata aj.);
- stavební prvky objektu (stěny, stropy, střechy aj.);
- otvorové výplně (dveře, okna aj.);
- úschovné objekty (trezory, bezpečnostní schránky aj.).

Bezpečnostní úroveň jednotlivých prvků je dána kvalitou výrobku (vybraný výrobek by měl mít certifikát vydaný na základě posouzení příslušné akreditované zkušebny) a kvalitou montáže (montáž by měla provádět odborně zdatná a důvěryhodná firma).

4.1.1. Brány a oplocení

Obě otevřené strany areálu jsou oploceny pletivem vyrobeného železného drátu o průměru cca. 2,5 mm a výšky zpravidla 1,5 m. Pletivo je nataženo mezi budovami a jeho upevnění je zajištěno pomocí ocelových sloupů. Je sice pachateli relativně snadno překonatelné a používá se k ochraně méně významných objektů, ale vzhledem k ceně a doplnění ochrany o EZS, bylo zvoleno jako vyhovující.

Pro zkvalitnění této mechanické zábrany bylo pletivo doplněno v jeho horní části o vrcholové zábrany, kde jsou pak nataženy tři ostnaté žiletkové dráty.

Ke vstupu do areálu slouží mohutné ocelové brány upevněné opět k zabetonovaným ocelovým sloupkům. Brány jsou vyplněny kulatinou s rozestupem patnáct centimetrů a opět jsou v horní části na nadvařených nádstavcích opatřeny třemi nataženými ostnatými žiletkovými dráty. Na branách jsou pevně navařené oka pro přichycení mohutného visacího bezpečnostního zámku.

4.1.2. Zámky a kování

4.1.2.1. Visací zámky

Ke vstupu do areálu slouží branka pro chodce a dále dvě velké vjezdové brány. Na základě doporučení jsme pro zabezpečení těchto vjezdových bran z čelní a zadní strany areálu zvolili vysoce bezpečnostní visací zámek Golem G60, masivní tělo je z kalené oceli povrchově cementované, což zabezpečuje vysokou odolnost proti hrubému násilí. Má krytý, oboustranně jištěný oblouk, jenž je chráněn proti vypáčení a přestřižení. Je dodáváno s bezpečnostní vložkou, odolnou proti odvrtání a vyháčkování. Součástí je bezpečnostní karta bránící nežádoucímu kopírování klíčů. Zámek je možné ho zapojit do systému stejného, hlavního a generálního klíče a to i ve spojení s dveřními vložkami.

Je doporučené použití s petlicí TOKOZ nebo s řetězem s průměrem oka 10 mm. Zámek je zkušebním ústavem zařazen do 3. bezpečnostní třídy podle ČSN EN 12320. Tato evropská norma stanoví požadavky a popisuje zkušební metody pro pevnost, bezpečnost, funkčnost a odolnost proti korozi visacích zámků a příslušenství visacích zámků používaných v budovách kromě kabelů a řetězů. Požadavky týkající se bezpečnosti jsou klasifikovány v šesti třídách, na základě funkčních zkoušek, které simulují útok. Tyto zámky by nám tedy měli snížit riziko neoprávněného vjezdu do areálu technikou, případně jej časově oddálit. [16]

Obr. č. 1 Visací zámek Golem G60

Zdroj: http://www.fab.cz/katalog/, [16]

4.1.2.2. Cylindrycké vložky a kování.

Malá boční branka je zabezpečena cylindrické vložkou FAB CONTROL (FAB 2224BDN)**.** Cylindrické vložky představují nejpoužívanější výrobky k uzamykání dveří, především bytů. Jsou určeny pro různé tloušťky dveří a mají charakteristický standardní profil tělesa, který koresponduje s instalačními rozměry na dveřích, v zadlabacím zámku a dveřních štítech (kování). Vyrábějí se s různým profilem klíčového otvoru, v různých délkách a v různém stupni odolnosti proti násilným i nenásilným způsobům překonávání. Bezpečnostním zámkem FAB CONTROL (FAB 2224BDN**)** je podle normy ČSN P ENV 1627 certifikován v BT 3. Splňuje požadavky NBÚ v kategorii „SS4 = 2“ dle zákona 214/2005 Sb. právní ochrana profilu klíče proti neoprávněnému kopírování. Je zde možnost sjednocení na společný uzávěr (označení SU) s ostatními výrobky řady FAB CONTROL. Délka cylindrické vložky je od 59 mm. A jeho povrchová úprava je: těleso - saténový nikl (označení N). [16]

Obr. č. 2 Cylindrická vložka FAB CONTROL (FAB 2224BDN**)**

Zdroj: http://www.fab.cz/katalog/, [16]

Vstupní dveře do kanceláře, šaten a skladu s materiálem jsou také zabezpečeny soustavou kvalitních cylindrických vložek FAB VARIANT (FAB 21320) se stupněm bezpečnosti: 4. stupeň - velmi vysoká ochrana. Podle normy ČSN P ENV 1627 je tento výrobek certifikován v BT 4, také splňuje požadavky NBÚ v kategorii „SS4 = 3“ dle zákona 412/2005 Sb. Opět má patentoprávní ochranu proti neoprávněnému kopírování klíčů. I tady je možnost sjednocení na společný uzávěr (označení SU) s ostatními výrobky řady FAB VARIANT. Vložka má 6 stavítek s bočním blokovacím systémem zajišťuje vysokou bezpečnost. Povrchová úprava: těleso - lesklý chrom. [16]

Obr. č. 3 Řada výrobků sady FAB VARIANT (FAB 21320)

Zdroj: http://www.fab.cz/katalog/, [16]

4.1.3. Bezpečnostní dveře a jejich komponenty z pohledu pojištění.

Z pohledu pojišťovny jsou pro tento druh prostoru požadovány dveře s certifikátem shody s normou ČSN P ENV 1627 s minimálně bezpečnostní třídou 3. Bezpečnostní kování, bezpečnostní uzamykací systémy a jejich komponenty by měly být také s certifikátem shody s normou ČSN P ENV 1627 s bezpečnostní třídou 3 (odpovídá modré barvě Pyramidy bezpečnosti) nebo 4 (odpovídá červené barvě Pyramidy bezpečnosti), přičemž:

- bezpečnostní zámky a bezpečnostní celoplošné závory jsou požadovány s cylindrickou bezpečnostní vložkou s překrytým profilem zabraňujícím vyhmatání a bezpečnostním kováním (štítem) zabraňujícím rozlomení vložky;
- bezpečnostní uzamykací systémy a bezpečnostní vícerozvorové zámky jsou požadovány s cylindrickou bezpečnostní vložkou s překrytým profilem zabraňujícím vyhmatání a bezpečnostním kováním (štítem) zabraňujícím rozlomení, odvrtání a vytržení vložky. Za bezpečnostní uzamykací systém lze považovat i elektromechanický zámek s odolností proti překonání na úrovni mechanického bezpečnostního uzamykacího systému;
- bezpečnostní visací zámky jsou požadovány s tvrzeným třmenem (hardened) o průměru minimálně 10 mm. Petlice i oka, jimiž prochází třmeny visacích zámků, musí mít srovnatelnou mechanickou odolnost proti vloupání jako třmeny visacích zámků, přičemž petlice i oka musí být upevněny nerozebíratelným spojem. [16]

4.1.4. Pyramida bezpečnosti

Pro snazší orientaci na trhu v této oblasti zavádí výrobci ve spolupráci s pojišťovnami takzvanou pyramidu bezpečnosti. Pyramida bezpečnosti je jednotící komunikační prvek, který usnadňuje a zpřehledňuje identifikaci výrobků s ověřenou úrovní jakosti a je zaměřen výhradně na certifikované výrobky mechanických zábranných systémů. Čtyři barevně odlišené stupně bezpečnosti reprezentují jednotlivé úrovně zabezpečení dle normy ČSN P ENV 1627. Ta definuje odolnost výrobků např. proti odvrtání, vyhmatání, vytržení, hrubému násilí, atd. Hodnocení a certifikaci výrobků zajišťuje nezávislá akreditovaná zkušební laboratoř a certifikační orgán. Zákazníkovi tak usnadňuje volbu při výběru vhodných výrobků splňujících požadovanou úroveň zabezpečení majetku. Pyramida bezpečnosti je složena ze čtyř stupňů bezpečnosti, které představují různé úrovně zabezpečení. Výrobky značky FAB jsou tak rozřazeny do čtyř skupin na základě certifikace podle normy ČSN P ENV 1627. Jednotlivé stupně bezpečnosti jsou na obalech výrobků odlišeny barvou a číslem. Okamžitě tak poznáme, jakou úroveň zabezpečení výrobek poskytuje. [16]

Barevné označení, přiřazené konkrétnímu stupni, umožní zákazníkovi optimální výběr zámku, kování, dveří i ostatních mechanických zábran. Pyramida svým tvarem i

popisem označuje, které zařízení je vhodné k základní, dostatečné, vysoké nebo velmi vysoké úrovni ochrany majetku. Tato pyramida bezpečnosti, která nabízí jednoduchou orientaci při výběru mechanických zábran, pomůže klientovi pojišťovny dosáhnout snížení škod způsobených násilným vstupem do pojištěného prostoru. Značení výrobků podle dle tohoto systému, je v souladu s požadavky na zabezpečení majetku. Stupeň pyramidy vychází z bezpečnostní třídy stanovené certifikátem. Základním předpokladem zařazení výrobku do tohoto systému je jeho přezkoušení zkušební laboratoří a u certifikačního orgánu pak následná certifikace odolnosti výrobku proti násilnému vniknutí (ČSN P ENV 1627). Současně musí výrobce prokázat, že je schopen dodávat výrobek na trh ve stálém provedení a kvalitě. Způsobilost výrobku i výrobce pro zařazení do projektu musí být osvědčena akreditovanými certifikačními orgány. [16]

Například čtvrtý stupeň - červený - představuje výrobek zajišťující nejvyšší bezpečnost. Takový kvalitní zámek je odolný proti vyhmatání, odvrtání, vytržení i hrubému násilí.

Tab. č. 1 Pyramida bezpečnosti

Pyramida bezpečnosti		
4	★★★★	**VELMI VYSOKÁ OCHRANA**
3	★★★	**VYSOKÁ OCHRANA**
2	★★	**ZVÝŠENÁ OCHRANA**
1	★	**ZÁKLADNÍ OCHRANA**

Zdroj: http://www.fab.cz/katalog/, [16]

4.2. Elektronická zabezpečovací signalizace (EZS)

Jako jádro EZS jsme zvolili ústřednu AMOS 1600. Sem připojíme také výstupy z vratových a dveřních magnetů, kterými doplníme mechanické zámky u vstupů do areálu a jednotlivých prostor. Jednotlivé prvky byly vybrány na základě našich požadavků a po konzultaci s odborníky z firmy zajišťující odbornou montáž.

4.2.1. Vratové magnety

Pro zabezpečení vrat jsme zvolili vratový magnetický kontakt BP 33 od firmy Olympo s odpovídající citlivostí pro velké vstupní brány i pro vstupní branku. Magnetický kontakt je vyroben z hliníkových odlitků a je ideálním řešením pro použití na všechny typy roletových kovových dveří např. v garážích, obchodech atd. Má velkou pracovní mezeru a vodiče jsou chráněné armovanou hadicí délky 50 cm. Část s magnetickým kontaktem se zpravidla umisťuje do středu prahu vrat a může být přišroubována nebo zapuštěna do betonového nebo jiného podkladu. Propojení magnetů s ústřednou zajišťuje koaxiální vodič. Princip magnetů spočívá v rozpojení magnetického pole zajišťující trvalý odpor ve smyčce. V případě rozpojení magnetického obvodu dojde k rozpojení a změně odporu a tím i protékajícího proudu. Tuto změnu vyhodnotí ústředna jako vniknutí.

Obr. č. 4 Magnet vratový

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

Tab. č. 2 Technické parametry vratových magnetických kontaktů BP 33 TN

Parametry vratových magnetických kontaktů BP 33 TN	
Rozsah pracovních teplot	.-25°C až + 50°C
Rozměry	150 x 40 x 28 mm
Pracovní mezera	40 mm
Délka armované hadice	50 cm

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.2.2. Optické infračervené závory

Pro zabezpečení perimetrické bezpečnosti jsme navrhli použít optické infrazávory. Systém se skládá z vysílače a přijímače. Vysílač emituje infračervené záření směrem k přijímači, který vyhodnocuje, zda na něj záření dopadá nebo ne. Při přerušení toku záření na přijímač způsobený přerušením paprsku – průchod osoby atd…) je vyvolán poplach. Infračervený paprsek je úzce směrový, což znamená, že vysílač musí mířit přímo na přijímač. V případě reflexních infrazávor je paprsek směrován sérií zrcadel.

Součástí vysílačů jsou modulátory, které modulují světelný tok, aby šířka vlastních pulzů byla úzká a amplituda malá. Podle výrobce a typu se řádově pohybuje v jednotkách, až desítkách mikrosekund, a mezera mezi jednotlivými pulzy se pohybuje v jednotkách milisekund. Toto opatření chrání infrazávory proti oklamání, například jiným infračerveným vysílačem. Pokusí-li se někdo oklamat přijímač jiným zdrojem IR záření, jehož modulace neodpovídá modulaci vlastního vysílače, reaguje vyhodnocovací zařízení vyhlášením sabotážního poplachu.

Samotné infrazávory se vyrábí v různých typech a modifikacích ať už jde o citlivost, prostředí nebo vzdálenost pro kterou jsou určeny.

4.2.2.1. OPTEX AX-130 TN- infra dvoupaprsková

Dvoupaprsková infra-bariéra pro vnitřní i venkovní prostředí je určena pro komerční aplikace i aplikace s vysokou úrovní rizik. Bariéra je schopna pracovat i při ztrátě 99 % energie paprsku. Díky tomu je funkčnost IR závor zajištěna i při hustém dešti, mlze, sněžení či v prašném prostředí.

Standardní výbavou je obvod pro adaptivní úpravu prahu detekce, kvalitní mechanické provedení, volba jednoho ze čtyř modulačních kmitočtů detekčních paprsků a paměť poplachu. Mezi vysílačem a přijímačem lze po detekčních paprscích přenést binární informaci (např. stav poplachového relé pomocného detektoru). Obvod integrovaného přenosu stavu nasměrování zpřesňuje a zrychluje proces nasměrování bariér. Čtyři volitelné modulační kmitočty paprsků umožňují umístění až 4 bariér nad sebou v jednom úseku, aniž by docházelo k jejich vzájemnému ovlivňování.

Všechny svorky jsou osazeny kvalitními přepěťovými ochranami a výstupní relé je použito v provedení se zvýšenou odolností vůči přepětí. Díky tomu je zajištěna vysoká odolnost vůči přepětí způsobované zejména bouřkovou činností až do výše přesahující 14 kV. To dále přispívá k dlouhodobě spolehlivému provozu IR závor. Obvody automatického řízení zisku (A.G.C.) nepřetržitě monitorují pomalé změny intenzity

přijímaného signálu způsobované změnami přenosových podmínek v důsledku klimatických vlivů. Citlivost vstupních obvodů přijímače je odpovídajícím způsobem upravována tak, aby následné detekční obvody pracovaly s optimální úrovní signálu.

Instalace je možná na kovový sloupek o průměru 34 - 48 mm nebo na zeď, případně do sloupů. Závory je možné doplnit o vyhřívací jednotky HU-3. Ty jsou vhodné použít při instalaci IR závor v místech, kde lze v zimním období předpokládat nepříznivé klimatické podmínky. [13]

Tab. č. 3 Technické parametry závory OPTEX AX-130 TN

Parametry závory OPTEX AX-130 TN	
Detekční princip	aktivní infračervený (přerušení 2 detekčních paprsků)
Dosah IR závory	80m interiér / 40m exteriér
Modulační kmitočty	4 kanály
Rozsah nasměrování paprsků	± 90° horizontálně, ± 5° vertikálně
Napájení	10,5 – 28,7 Vss
Odběr	41 mA vysílač, 41 mA přijímač
Krytí (podle EN 60 529)	IP 65
Poplachový výstup	NC, max. 28 V ss / 200 mA
Pracovní teplota	-35 °C až +60 °C
Relativní vlhkost	max. 95%
Doba přerušení paprsků	50/100/250/500ms (nastavitelná ve čtyř krocích)
Doba sepnutí poplachového relé	2 ± 1 s
Ochranné kontakty	NC (rozepnou při sejmutí krytu), max. 28 Vss / 200mA
Hmotnost (vysílač + přijímač)	650 g
Rozměry	65x170x70mm (v x š x h)

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

Obr. č. 5 Infrazávora OPTEX AX-130 TN

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.2.3. Kombinované perimetrické PIR-MW detektory

Jako další prvek elektronického zabezpečení bude sloužit kombinovaný PIR-MW detektor. Jak je z názvu zřejmé, detektor kombinuje metody PIR a MW, využívající aktivní mikrovlnné a pasivní infračervené detekce. V současnosti patří k nejčastěji využívaným detektorům v kategorii duálních detektorů pohybu. Využití PIR detekce umožňuje kontrolu střeženého prostoru v oblasti tepelného vyzařování, aktivní MW detektor založený na principu Dopplerova jevu zase zvyšuje citlivost na pohyb. Tyto detektory tak v sobě také sjednocují vysokou citlivost na narušitele pohybujícího se jak v radiálním tak i tangenciálním směru k ose detektoru, požadovaný dosah i odolnost před falešnými poplachy. Jednotlivé typy odlišuje frekvenční pásmo používané k mikrovlnné detekci, možnost nastavení jednotlivých subsystémů a další technické případně estetické detaily. Citlivost uváděná na PIR + MW detektorech je obecně 0,2 m/s. Jde o hodnotu vyžadovanou českou státní normou, která je plně dostačující pro potřeby technické

ochrany. Vyšší citlivost u duálních detektorů bývá proto spíše výjimkou a výrobci se často více soustředí na eliminaci vzniků falešných poplachů formou zpracování signálu. Duální detektory doplňují také nadstandardní funkce. Z řady možností například ukládání poplachových zpráv v detektoru, ochrana před vyhlášením poplachu domácími mazlíčky (tzv. PET immunity), nastavení mikrovlnného subsystému (jedná se především o jeho vypnutí v průběhu dne, kdy se v oblasti vyskytují běžně osoby) nebo nastavitelná oblast zastřežení pomocí výměnných zaostřovacích soustav.

4.2.3.1. Provedení PIR-MW detektorů

Velké množství různých provedení v případě PIR + MW detektorů poskytuje možnost velkého výběru mezi způsoby pokrytí střeženého prostoru. Kromě nejčastějšího vějířového pokrytí tak existuje i stropní varianta duálního detektoru s panoramatickým pokrytím, jehož rozsah činí 360°. Dalším typem je samozřejmě i typ se záclonovým pokrytím.

Tělo duálního detektoru je tvořeno vždy plastovým krytem, který má rozměry v řádu jednotek centimetrů. Tvarem vždy připomíná kvádr postavený na výšku a jeho zbarvení je vždy v neutrálních barvách, jejichž cílem je neupozorňovat případného narušitele. Nejčastější provedení detektoru je tedy v bílé barvě. Jeho zadní strana vždy obsahuje otvory pro uchycení a kabeláž Mezi základní části, skrývající se uvnitř, řadíme zaostřovací soustavu pro pyrosenzor, desku plošných spojů s jednotlivými součástkami a svorkovnici. Konstrukce je vždy zvolena tak, aby byl dostatečně vzdálen přijímač mikrovlnného záření od vysílače, který je tvořen sektorovou anténou. Právě konstrukce sektorové antény vyžaduje přesnost, protože její tvar určuje plochu střeženého prostoru stanovenou úhlem záběru a zároveň minimalizuje nechtěné vyzařování mimo tento tvar.

Využití kombinace mikrovlnného a pyroelektrického senzoru k jejich současnému střežení zájmového prostoru vysoce zvýšila odolnost před falešnými poplachy. Jejich vzájemná součinnost napomáhá k odstranění stavů, v kterých by samotný detektor selhával a došlo tak k vyvolání falešného poplachu. Tato koncepce využívající dvou odlišných oblastí elektromagnetického vlnění je svou konstrukcí předurčena především do náročných prostředí a zájmových prostor s vyšším rizikem falešného poplachu. Ze stejného důvodu je detektor také vhodný do prostor vyžadujících vysokou úroveň zabezpečení. Přesto, že sloučením dvou detektorů došlo k významnému úbytku falešných poplachů, detektor je stále citlivý na některé změny v jeho okolí. Mezi rizikové faktory stále zahrnujeme přímý dopad slunečního záření, vysokopříkonové tepelné zářiče nebo střežené zóny ohraničené

skleněnými plochami. Za předpokladu včasné a pravidelné údržby korekce v případě mikrovlnného senzoru a stabilního napájení je ovšem tento typ detektoru velmi kvalitním prvkem zabezpečení.

4.2.3.2. Duální detektor PIR/MW LC-103-PIMSK s antimaskingem

Detektor LC-103-PIMSK kombinuje detekční technologie PIR a MW s funkcí antimasking, která zabraňuje zneškodnění detektoru zakrytím jeho výhledu. Detektor je také odolný proti malým zvířatům do 25kg. K tomu je určena technologie Quad Linear Imaging zajišťuje přesnou analýzu rozměrů lidského těla a odlišení od pozadí a malých zvířat. Vzhledem k tomu, LC-103PIMSK je kombinovaná technika (PIR & mikrovlnná trouba), poplašný signál a aktivaci relé nastane pouze tehdy, když signály z obou čidel (PIR & MW) přijdou ve stejnou dobu. Účinný detekční rozsah, je rozsah, kde se paprsky z obou typů čidel (PIR & MW) protínají. Funkce GAIN mění nastavení pomocí potenciometru intenzitu MW signálu tak, že falešné poplachy budou redukovány.

Unikátní funkce - antimasking - zajišťuje detektoru ochranu před nežádoucím přístupem a zabraňuje jakémukoliv zastínění ze vzdálenosti 0,8 m a blíž. [12]

Závora má tyto základní vlastnosti:

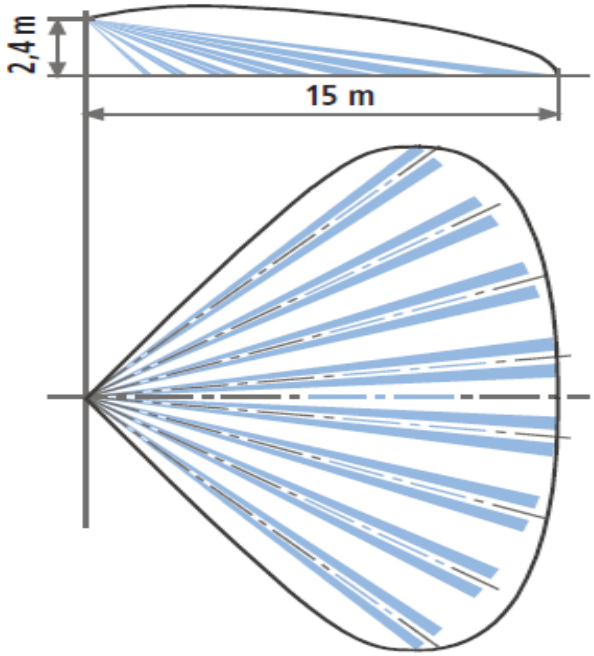
- antimasking;
- alarmový rozpínací kontakt a ochranný kontakt;
- digitální zpracování signálu;
- ignoruje pohyb zvířat do 25kg;
- technologie Quad Linear Imaging zajišťuje přesnou analýzu rozměrů lidského těla a odlišení od pozadí a malých zvířat;
- mikrovlnná detekce na principu Dopplerova efektu;
- mikrovlnný senzor se speciální anténou;
- technologie ASIC;
- bez nutnosti kalibrace podle výšky instalace;
- samostatné nastavení citlivosti PIR a MW systémů;
- snadná instalace s možností použití otočného kloubu (prodává se samostatně);

- detekční metoda: čtyřnásobný PIR senzor & MW impulsní Doppler;
- rozměry: 118x62,5x41mm;
- napájení: 8,2 - 16Vss;
- odběr v klidu/v alarmu: 18mA/25,5mA.

Obr. č. 6 PIR/MW detektor LC-103-PIMSK

Zdroj: KELCOM International, spol. s r.o., EZS 2008, [12]

Obr. č. 7 Schéma pokrytí u PIR-MW detektoru LC-103-PIMSK



Zdroj: KELCOM International, spol. s r.o., EZS 2008, [12]

4.2.4. Pasivní infračervené detektory PIR

Pro zabezpečení kanceláří nemusíme používat dražší kombinované detektory, ale postačí nám jednoduchý PIR detektor. Jde o detektory reagující na vyzařování lidského těl, modulované v přijímací části přerušováním zón, kterými v prostoru místnosti prochází.

Jejich hlavními výhodami jsou snadná montáž a seřízení, malá spotřeba elektrické energie, vysoká spolehlivost a značná odolnost proti planým poplachům. Mezi další výhody patří, že do jednoho prostoru je možné instalovat více PIR čidel, neboť nevyzařují žádnou energii. Jelikož je PIR čidlo aktivováno pouze tangenciální složkou pohybu pachatele (ve vztahu k rozložení aktivních a neaktivních zón) doporučuje se v případě nutnosti úplného vykrytí prostoru instalace více čidel k vzájemnému překrytí detekčních zón, bez nebezpečí vzájemného ovlivňování.

Nevýhodou je možnost překonatelnosti některých druhů těchto čidel a také ovlivnění jejich spolehlivost např. těmito faktory:

- faxovací přístroje: list termopapíru padající z faxu;
- světelné rušení": slunce svítící oknem dovnitř místnosti, světlomety automobilů;
- rychlé teplotní změny: podlahové topení, technická zařízení v místnosti;

- zařízení místností: pohybující se závěsy a žaluzie zahřáté slunečním zářením;
- zvířata: myši, ptáci, kočky, psi;
- proudění vzduchu: závan teplého nebo studeného vzduchu - průvan komíny ventilace topná tělesa, klimatizace.

4.2.4.1. IR120C Pasivní infračervený detektor

Všestranné použití. Diskrétní ergonomické provedení, které se hodí do každého prostředí, dobrá odolnost proti pohybu domácích zvířat a pokročilé vyhodnocování signálu – to vše činí detektor IR120C ideálním řešením pro obytné i menší komerční objekty.

Snadná a bezpečná instalace. Univerzální kryt detektoru je uzpůsoben pro přímou montáž na stěnu, pod úhlem 45° i v rozích, a to bez použití dalších montážních součástí.

Vynikající odolnost. Detektor IR120C se vyznačuje stoprocentní účinností detekce doprovázenou vysokou odolností proti vlivům okolního prostředí.

Bezpečná detekce. Optická soustava s triplexním zrcadlem, která je rozdělena do 52 zón, zaručuje vysoce spolehlivou detekci. Systém analýzy signálu využívající více kritérií inteligentně a spolehlivě rozlišuje mezi vetřelci a rušivými signály. [13]

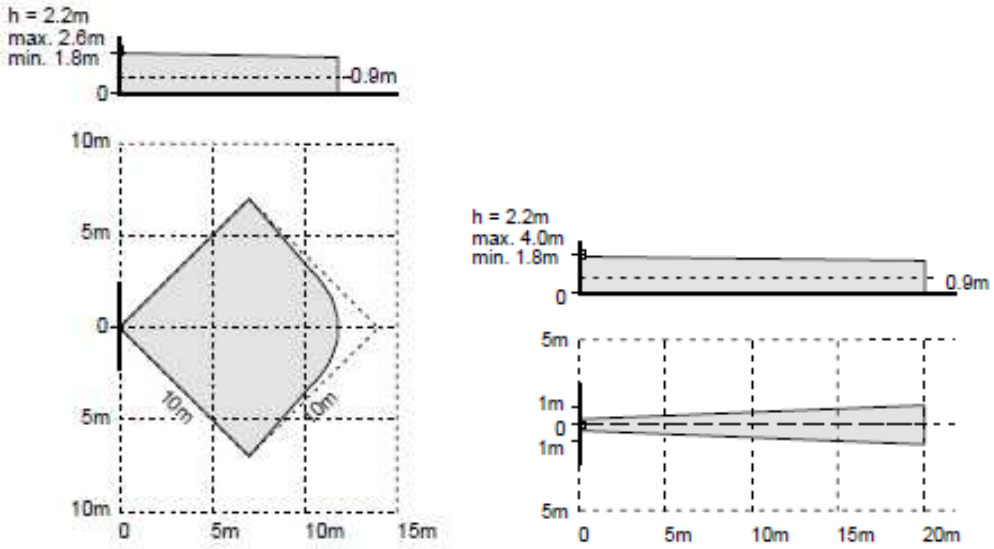
Detektor má tyto základní vlastnosti:

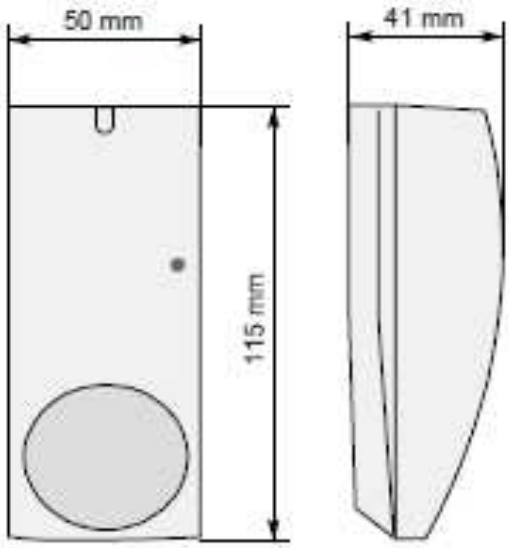
- dosah 12 m při použití zrcadla s vějířovou charakteristikou nebo 20 m při použití záclonového zrcadla;
- necitlivost na pohyb domácích zvířat do 40 kg;
- pravá teplotní kompenzace;
- digitální obvod vyhodnocování signálu AMASIC;
- účinné filtrování bílého světla prostřednictvím optické soustavy s triplexním zrcadlem;
- výběr ze čtyř nastavení citlivosti, indikace krokového testu LED;
- krytí proti vlhkosti IP41.

Obr. č. 8 Pasivní infračervený detektor IR120C

Zdroj: SIEMENS, spol. s r.o., Building Technologies 2009, [13]

Obr. č. 9 Technické parametry PIR detektoru IR 12OC





Zdroj: SIEMENS, spol. s r.o., Building Technologies 2009, [13]

4.2.5. Tísňový hlásič

Přímý prodej na pokladně a tím pádem manipulace s hotovostí představuje další riziko, které budeme řešit. Zde jsme navrhli pro ochranu obsluhy prodeje skryté nouzové tlačítko napojené přes ústřednu na pult centrální ochrany. Zde je velkou výhodou již zmiňovaná minimální vzdálenost firmy zabezpečující ostrahu objektu a její případně možná velmi rychlá reakce na vyhlášení poplachu.

Tísňové hlásiče jsou významnou součástí ochrany osob a majetku kde je včasné podání informace o vzniklé hrozbě, nebezpečí, nehodě, přepadení či jakékoliv jiné nestandardní situaci velmi důležité.

Účelem včasného podání informace je především zamezení vzniku nestandardní situace, eliminace hrozeb a rizik s nimi spojených přerušení průběhu nestandardních procesů (zejména přepadení), eliminace rozsahu následků přepadení, nehod, především ochrana života a zdraví zúčastněných osob. Ochrana zaměstnanců a veřejnosti v případě přímého ohrožení a to ohlášením do místa, odkud může být poskytnuta pomoc.

Hlášení se vyvolává manuálním aktem, případně zprostředkovaně při definovaném způsobu manipulace.

4.2.5.1. Rozdělení tísňových hlásičů

Tísňové hlásiče dělíme do dvou základních skupin.

- veřejné tísňové hlásiče;
- speciální tísňové hlásiče.

Protichůdné požadavky na tísňové hlásiče vychází z toho, že na jednu stranu mají být skryty před cizími osobami, ale přístupné k snadné aktivaci (nohou, jinou částí těla vhodnou k aktivaci v dané situaci umístěny tak, aby nebyly náhodně bezděčným pohybem aktivovány.

V našem případě volíme speciální tísňové hlásič s konstrukčním provedením dle požadavku investora v souladu s potřeby obsluhy prodejny:

- lištový určen pro sedící obsluhu, aktivuje se sešlápnutím zvednutím nártu, kolenem;
- hlásič tlačítkový (výklopný – určen k ručnímu ovládání (aktivovány osobami, jež jsou svědkem přepadení, ale nejsou přímo ohroženy).

Osobní tísňové hlásiče určeny pro odloučená pracoviště se zvýšeným rizikem nouzového stavu (benzinové pumpy, laboratoře, prodejny, pokladny aj.). V samotném systému je zajištěn přenos poplachu do centrály s využitím rádiového kanálu, nebo standardními metalickými vodiči. Tato tlačítka lze připojit také přes monitorovací středisko nebo lokálně, přes tichý alarm nebo na zvukový zvonek.

4.2.5.2. Výklopný tísňový hlásič S3040

Jako tísňový hlásič pro prodejnu jsme zvolili výklopný tísňový hlásič S3040. Spínač se umísťuje do místa, které vyhovuje koncovému uživateli podle jeho pracovních zvyklostí a je v jeho dosahu. Zároveň by uživatel při aktivaci tísňového spínače neměl budit pozornost. Typické umístění tísňového spínače S 3040 je na vnitřní straně postranic pracovního stolu nebo ze spodní strany pracovní desky stolu tak, aby nebyl spínač normálně vidět. Potom je nutno spínač umístit tak, aby LED indikace paměti aktivace nebyla zastíněna nějakou překážkou. Tísňový spínač musí být upevněn ve svislé nebo vodorovné poloze. Pro úplné vyklopení ramena spínače je nutné nechat volný prostor od montážního povrchu aspoň 8cm. My jsme pro montáž také zvolili vnitřní stranu postranic stolu v prodejně. [14]

Tab. č. 4 Technické parametry výklopného tísňového hlásiče S3040

Výklopný tísňový hlásič S3040	
Jmenovité napájení	12V ss / 6 mA
Pracovní napětí:	7 až 15 V ss max. 8 mA
Rozsah pracovních teplot	.-18 °C až 48 °C
Hmotnost	43 gramů
Rozměry	š45 x d73,7 x v19,3 mm

Zdroj: OLYMPO controls, spol. s r.o. - Security Products, [14]

Obr. č. 10 Výklopný tísňový hlásič S3040

Zdroj: OLYMPO controls, spol. s r.o. - Security Products, [14]

4.2.6. Siréna

V zásadě existují dva druhy a to zálohované a nezálohované. Nezálohované sirény se většinou instalují uvnitř objektu. Nejlepší polohou je střed budovy odkud je siréna slyšet v každé části objektu. Akustický výkon sirén se pohybuje v hodnotách nad 100 dB. S tím souvisí že, práh bolestivosti ucha je 130 dB. To je také maximální hodnota, kterou povolují hygienické normy. Díky odrazům zvuku v uzavřených místnostech je proto vnitřní siréna

tou nejúčinnější zbraní proti zlodějům. Díky pronikavému zvuku nepomáhají proti zvuku této sirény ani nejrůznější tlumítka v uších.

Zálohované sirény se instalují ven a to směrem k civilizaci. Siréna směřovaná do pole žádnou službu nevykoná. Akustický výkon těchto sirén se pohybuje okolo 128 dB. Siréna obsahuje záložní zdroj, který ji napájí v případě výpadku proudu. Takovýto typ sirény jsme zvolili pro instalaci v areálu prodejny.

4.2.6.1. Siréna PARADOX PS – 128

Siréna Paradox PS 128 je zálohová siréna řízená mikroprocesorem. Siréna je uložena v protipožárním krytu, který má vnitřní ocelovou krabici upravenou proti násilnému vniknutí a odtržení. Její součástí je vysoce efektivní reproduktor o výkonu 40W. Vlastní testování sirény je řízené vnitřním mikroprocesorem. Vydává hlasitý zvukový efekt. Další její vlastností je speciální funkce blikání pro zvýšení poplachového efektu. Automaticky provádí testování stavu baterie, žárovky a reproduktoru. Samozřejmostí je také servisní vstup a servisní funkce určené pro instalaci a vlastní užívání sirény. Obsahuje mód na úsporu energie a šetření baterie. Vstupní svorky jsou chráněny. Pro zajištění kompatibility je umožněno několik různých zapojení pro nahrazení starších typů sirén.

Tato siréna vyráběná firmou Paradox a obsahuje funkce a vylepšení, díky kterým patři mezi špičkové výrobky. První novinkou je výstup Report, který umožňuje předávat do ústředny informace o stavu baterie, reproduktoru a světla. Další inovaci je servisní vstup sirény, který přepíná sirénu do servisního módu, ve kterém lze sirénu bezpečně otevřít a jakkoliv s ní manipulovat. Mód úspory energie zabraňuje úbytku na zvukové a světelné intenzitě a prodlužuje životnost baterie. Pokud je při první montáži nízké napětí na baterii, siréna vás na to upozorni tichým dlouhým signálem a nezačne pracovat, dokud baterie nebude poskytovat požadované napětí.

Siréna ohlašuje poplach pomoci zvukové a světelné signalizace. Díky zvukové charakteristice varovného signálu je tento zvukový signál daleko silnější než u sirén s podobným výkonem, přičemž doba znění sirény je maximálně 3,5 minuty. Pravidelným monitorováním stavu baterie systém dokáže předcházet jejímu úplnému vybití. Při detekci příliš nízkého napětí baterie totiž siréna přechází do úsporného režimu. Kromě testu baterie je vyhodnocován i stav reproduktoru a světla, přičemž test baterie je prováděn v intervalech 6h nebo 24h podle nastaveni propojky (jumperu), zatímco světelný a reproduktorový test probíhá neustále. Stav výstupu Report je však aktualizován jen v okamžiku testu baterie

Tab. č. 5 Technické specifikace sirény PARADOX PS 128

Siréna PARADOX PS – 128 - technické specifikace	
Rozměry	295/200/100 mm
Váha	3,0 kg
Krytí	IP 34
Napájení	13.6 – 14.8V
Baterie	12V / 1,2 až 7.0 AH
Minimální napětí baterie	9.8V
Typ světla	12V / 18 W
Odběr při klidovém stavu	5 mA
Průměrný odběr reproduktoru	1.2 A
Maximální odběr	2.8 A
Hlasitost sirény	128 dB
Zvuková frekvence	900 – 2400 Hz
Maximální doba spuštění sirény	3.5 min
Zapínací polarita	+ / - (dá se nastavit)
Délka zapínacího pulsu	200 ms minimálně
Aktivování spínače světla	zápornou hodnotou, 200ms minimálně
Výstup zpráv	Maximálně 200 mA
Typ výstupu správ	N.O. (v klidu otevřeno)
Typ ochranného kontaktu	N.C. (v klidu zavřeno)

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.2.6.2. Zapojení sirény

Stručný přehled jednotlivých parametrů a nastavení pro připojení sirény:

- svorky +12 V a –12 V (svorky 1a 2) – Na tyto svorky se připojuje napájení +12 V (+12 V na svorku +12 V a 0 na svorku –12 V). Ztrátou tohoto napětí je siréna spouštěna;
- svorky Lamp (svorky 3 a 4) – Na tyto svorky se připojuje žárovka (12V 18W) uvnitř sirény. Řídící obvod kontroluje zablesknutím žárovky aktuální funkčnost sirény;
- svorka Start (svorka 5) – Na tuto svorku se připojuje napětí z ústředny, které také spouští sirénu (stejně jako ztráta napětí na svorkách 1a 2);

- svorka Flash (svorka 6) – Tato svorka spouští činnost žárovky v siréně (blikání) bez aktivace akustického měniče. Spuštění této funkce reaguje na záporný potenciál (zem, -12V);
- svorky Speaker (svorky 7 a 8) – Tyto svorky slouží pro připojení reproduktoru, na polaritě nezáleží;
- svorky Tamper (svorky 9 a 10) – Tyto svorky slouží pro hlídání, zda nebyl sejmut kryt sirény či zda nebyla násilně odtržena;
- svorka Service (svorka 11) – Tato svorka slouží pro instalační a servisní úkony. Je-li přiveden nulový potenciál na tento vstup, přepne se siréna do servisního módu, kdy není hlídán stav tamperu;
- svorka Report (Svorka 12) – slouží k předávání informací o stavu baterií, reproduktorů a světla, tato svorka se připojuje na patřičně naprogramovanou smyčku na ústředně. Stav tohoto výstupu není neustále měněn, ale mění se pouze při testu, tj. po určité časové periodě. Jsou-li sledované parametry v pořádku, je v okamžiku testu potenciál nulový, v opačném případě je potenciál +12 V. [11]

Obr. č. 11 Siréna PARADOX PS 128

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.3. Ústředna AMOS 1600

Ústředna je mozkem celé EZS, je to plošný spoj s mikroprocesorem, se zdrojovou částí a se vstupy pro zapojení zón s detektory. Je to také radiová ústřednu, která pro naše potřeby bude pracovat v pásmu 459 MHz a bude na této frekvenci připojena do lokální sítě firmy poskytující trvalý dohled pomocí pultu centrální ochrany (PCO) Jako záložní možnost přenosu poplachů je může posloužit připojení GSM modulu, což zařízení umožňuje.

Ústředna vyhodnocuje stav jednotlivých připojených detektorů a podle nastaveného programu nebo pokynů uživatele, nejčastěji z klávesnice, reaguje na tyto stavy. Uživatel pomocí kódu přes klávesnici ústřednu zapíná do hlídacího režimu, nebo ji naopak z hlídacího režimu vypíná. Další volbou určitých číselných a znakových posloupností se pomocí klávesnice může ústředna přepínat do programovacích režimů a režimů sloužících k nastavení celého systému. Nastavení celého sytému nebo programování ústředny lze také provádět pomocí propojení na PC. V něm se celý systém nastaví a po dosažení EZS jako funkčního programu se přehraje a celý systém otestuje. Umístění ústředny je vhodné volit s ohledem na dispozici budovy a tak, aby byla co nejlépe chráněna.

4.3.1. Popis ústředny

Jádrem celého systému bude zabezpečovací ústředna AMOS 1600. Je to elektronická zabezpečovací ústředna, kterou lze použit k elektronickému střežení objektů. Objekt, do kterého se ústředna instaluje, je možné rozdělit na zóny (chráněné oblasti, smyčky), např. podle místnosti, pater apod. Ke každé zóně může byt připojeno zařízení pro vyhodnocování signálů, tj. čidla reagující na pohyb, zvuk, kouř a ostatní zařízení pro použití v zabezpečovacích systémech. Ústředna je umístěna v kovové skříni a kromě samotného systému obsahuje i záložní napájecí zdroj - baterii, pojistky, vysilač apod. Ovládá se pomoci klávesnice nebo klíčové zóny. Pokud to vyžaduje situace, je možné ústřednu rozdělit až do osmi sekcí (podsystémů), přičemž libovolné sekci lze přidělit libovolné smyčky. Volitelné rozdělení ústředny do sekcí umožňuje selektivní přístup do jednotlivých částí zabezpečeného objektu.

4.3.1.1. Ovládání ústředny

Ústředna se ovládá pomoci klávesnice s 18-ti klávesami typ ESPRIT 616, 626, 636. Klávesnice poskytuje kompletní informaci o stavu ústředny pomocí kontrolek kláves (všechny kromě klávesy CLEAR), kontrolek READY, ARMED a bzučáku. Význam kontrolek se může měnit podle stavu, v němž se systém nachází. [15]

Klávesnice plní tyto základní funkce:

- programovaní systému;
- aktivace a deaktivace systému;
- poskytuje informace o stavu systému.

4.3.1.2. Parametry systému ústředny

Ústředna má 8 až 16 programovatelných vyvážených zón, umožňuje také možnost rozdělení zón do 8 sekcí. Ústředna má možnost výstup kódů událostí nebo paralelní výstup změny stavů. Dále má jeden výkonový výstup pro sirénu 12 V DC. Umožňuje připojení až čtyř klávesnic. Je kódovatelná šestnácti čtyřmístnými nebo šestimístnými přístupovými kódy a dvěma master kódy. Umožňuje maximálně osm vstupů pro aktivaci ústředny pomocí klíče. Lze také použít aktivace na dálku po telefonní lince pomocí programu AMOS 1600 Manager. Ústředna umožňuje pro připojení využít rozhraní RS 232 a také obsahuje telefonní komunikátor. Součástí ústředny je vysilač v pásmu 299 – 314 MHz nebo 339 - 345 MHz o řízeném výkonu do 1W pro radiové sítě NAM SYSTEM 2000 a Radom Security vysílač 450 MHz o řízeném výkonu do 1W (200 mW) pro radiové sítě GLOBAL a GLOBAL 2. [11]

4.3.1.3. Konfigurace zón

- 8 vyvážených vstupů pro připojení čidel;
- 8 napěťových vstupů oddělených pomoci optočlenů;
- možnost konfigurace vyvážených vstupů jako jednoduché nebo dvojitě vyvážené zóny;
- možnost nastaveni 8 vstupů pro aktivaci ústředny pomoci klíče;
- možnost zapnuti kontroly zkratu nebo rozpojení zóny;
- volba polarity napěťového vstupu.

4.3.1.4. Napájení

Ústředna může být napájena stejnosměrným napětím 13 V nebo střídavým napětím 16 Vef z doporučeného typu transformátoru. Na desce ústředny je pak stabilizovaný zdroj 12V pro napájení klávesnice, čidel a sirény. Zálohování je řešeno baterii 12 V / 6.5 Ah.

Ústředna má vlastní ochranu proti statické elektřině a poskytuje tedy ochranu proti napětím indukovaným statickou elektřinou. Zapojovací svorky jsou chráněny proti vysokonapěťovým špičkám.

4.3.1.5. Paměť EEPROM

Konfigurace ústředny a základní informace o stavu je uchována v paměti EEPROM. Obsah paměti zůstane vzhledem k vlastnostem paměti uchován i v případě odpojeni síťového napájení a baterie.

V paměti EEPROM jsou uloženy tyto informace:

- konfigurace ústředny;
- stav ústředny;
- paměť poplachů;
- paměť událostí.

Paměť poplachů a paměť událostí má kapacitu 256 položek, které obsahuji kód událostí (zavřeni, otevřeni, poplach, porucha atd.) a čas výskytu této události. Paměť poplachů obsahuje 16 poplachů se záznamem o času výskytu poplachu.

- **Paměť poplachů** - Záznamy o poplaších zón, vyvolaných v období od poslední aktivace, se ukládají do paměti poplachů. Přítomnost dat v paměti poplachů je indikována kontrolkou [MEM]. Paměť poplachů je umístěna v paměti EEPROM, z čehož vyplývá, že uložené údaje zůstanou uchovány i po vypnutí napájení. V paměti je uvedeno číslo zóny, která způsobila poplach a čas výskytu poplachu v hodinách a minutách. Kapacita paměti poplachů je 16 údajů. K vymazání údajů z paměti a zhasnutí kontrolky [MEM] dochází automaticky při aktivaci systému. Zruší se pouze ty údaje, které odpovídají aktivovaným zónám. Funkce [ENTER] umožňuje tyto poplachy zobrazit.
- **Paměť událostí** - Paměť událostí je umístěna v paměti EEPROM a má kapacitu 256 položek. Ukládají se do ní všechny záznamy o změně stavu systému a zprávy přijaté po telefonní lince nebo sériové lince z externí

ústředny. Kromě poplachů se do ní ukládají kódy poruch, záznamy o vstupu a opuštění objektu, stavu tísně, vypnuti poplachů atd. Zápis se provádí cyklicky. V případě naplněni paměti se začnou přepisovat nejstarší položky. Údaje v paměti události jsou přístupné po telefonní lince (downloading), po sériové lince prostřednictvím speciálního softwaru pro PC, ale zároveň mohou být ve zjednodušené formě zobrazeny pomoci kontrolek klávesnice. [11]

4.3.1.6. Komunikace ústředny

Ústředna pro komunikaci s okolními zařízeními umí využít několika různých způsobů spojení. Tyto typu spojení jsou určeny k rozličným účelům a to například k oboustranné komunikaci s jednotlivými prvky zabezpečovacího systému, dále připojení sloužící pro servis ústředny a systému a v neposlední řadě také připojení pro komunikaci s externími zařízeními což je v našem případě pult centrální ochrany.

- **Příjem zpráv z externích zařízení EZS** - Ústředna je schopna přijímat zprávy z externích ústředen, a to po telefonní nebo sériové lince, a následně odvysílat vysilačem. Funkce ústředny zůstává přitom zachována.
- **Komunikace po sériové lince** - Sériová linka RS 232 umožňuje připojení počítače. Pomocí počítače lze načíst z ústředny důležitá data a provést její konfiguraci. Software pro obsluhu sériové linky TSM – Amos Manager není ve standardní sestavě ústředny. Je poskytován zdarma na vyžádaní při koupi ústředny, nebo jej lze stáhnout z internetových stránek výrobce.
- **Vysilač** - Ústředna se dodává buď s vysilačem v kmitočtovém pásmu 299 – 345 MHz nebo v kmitočtovém pásmu 420 - 470 MHz. Pro vysilače v nižším pásmu je výkon nastavitelný ve třech stupních 0.1, 0.5 a 1 W, pro vysilače ve vyšším pásmu ve čtyřech stupních 0.1, 0.25, 0.5 a 1 W. Lze rovně ž objednat variantu ústředny bez vysilače pro jiný druh připojení přenosů poplachu.
- **Komunikátor** - Komunikátor umožňuje vysílat kódy událostí ústředny po telefonní lince v běžně používaných formátech. Umožňuje příjem zpráv z externích ústředen a jejich odvysílaní vysilačem. Komunikátor je schopen zpracovat jak formáty s paritou tak bez parity, a to 4 + 2, 4 + 3, 3 + 2 a také formát Ademco Contact ID. [11]

4.3.1.7. Poruchy a funkce pro omezení poplachů

Ústředna má několik velmi zajímavých a užitečných funkcí. Pro samotný provoz jsou velmi důležité systémy schopné sledovat vlastní provozní stavy ústředny a jejich operativní a správné vyhodnocování. To následně umožňuje předcházet falešným poplachům vzniklým z důvodu těchto poruchových stavů.

Sledovaní poruch

Ústředna nepřetržitě sleduje mnoho základních poruchových stavů. Pokud se některý objeví, rozsvítí se kontrolka TRBL. Kontrolka TRBL zůstane svítit, dokud není příčina poruchy odstraněna Číslo, které svítí k němu definovaná porucha, její možná příčina a případný způsob odstranění:

Mezi tyto sledované poruchové stavy patří:

- slabá nebo odpojena baterie;
- porucha síťového napájení;
- porucha pojistek;
- porucha telefonní linky;
- porucha tamperu;
- změna systémového času;
- neúspěšné telefonní spojeni.

Informace o poruchách je dostupná z klávesnice stisknutím [ENTER][2] nebo [TRBL]. Kontrolky kláves informuji o druhu poruchy. Seznam poruch indikovaných klávesnicí ukazuje tab. 1. Stisknutím klávesy [ENTER] v módu zobrazeni poruch zobrazí kontrolky kláves poslední poruchu. Paměť poruch je vhodná jako diagnosticky nastroj při instalaci a opravách ústředny. [11]

Tab. č. 6 Tabulka poruch ústředny AMOS 1600

Svítí číslo	Porucha	Možná příčina	Způsob odstranění
1.	Vybitá baterie	Pokles napětí baterie pod 10.2V	Zajistěte provedení výměny baterie
2.	Porucha síťového napájení	Přerušení dodávky sítě 220V	Zajistěte přítomnost sítě 220V v objektu
3.	Přerušené pojistky	Pojistka Po2 nebo Po3 je přerušena	Zajistěte výměnu pojistek
4.	Odpojená telefonní linka	Na telefonní lince není napětí	Zkontrolujte funkčnost telefonní přípojky
5.	Porucha tamperu	Otevřené víko ústředny	Uzavřete víko krabice ústředny
6.	Ztráta času v systémových hodinách	Objeví se jen po resetu	Nastavte systémové hodiny
7.	Neúspěšný pokus o komunikaci	6 neúspěšných pokusů volání na PCO	Kontaktovat servisní firmu

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

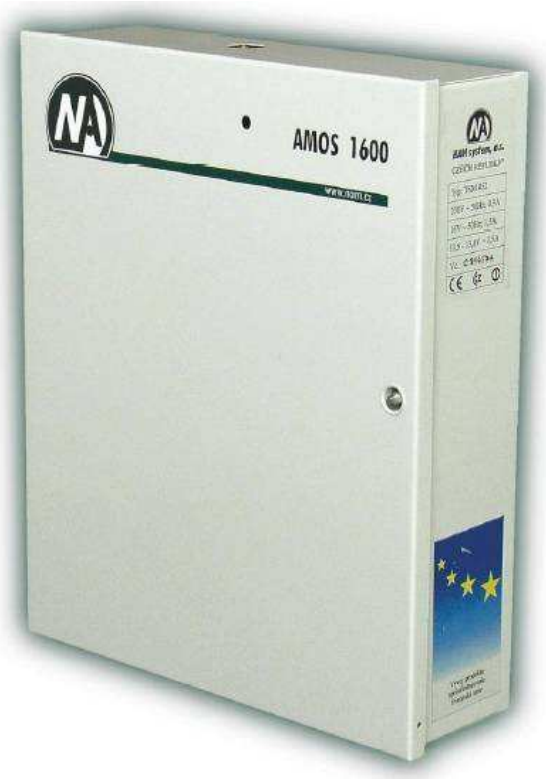
Volitelné funkce pro omezení planých poplachů

- hlasitá signalizace doby pro odchod;
- hlasitá signalizace nesprávného zapnuti;
- softwarový filtr pro eliminaci naindukovaných rušivých pulsů do kabeláže čidel.

4.3.1.8. Další funkce ústředny

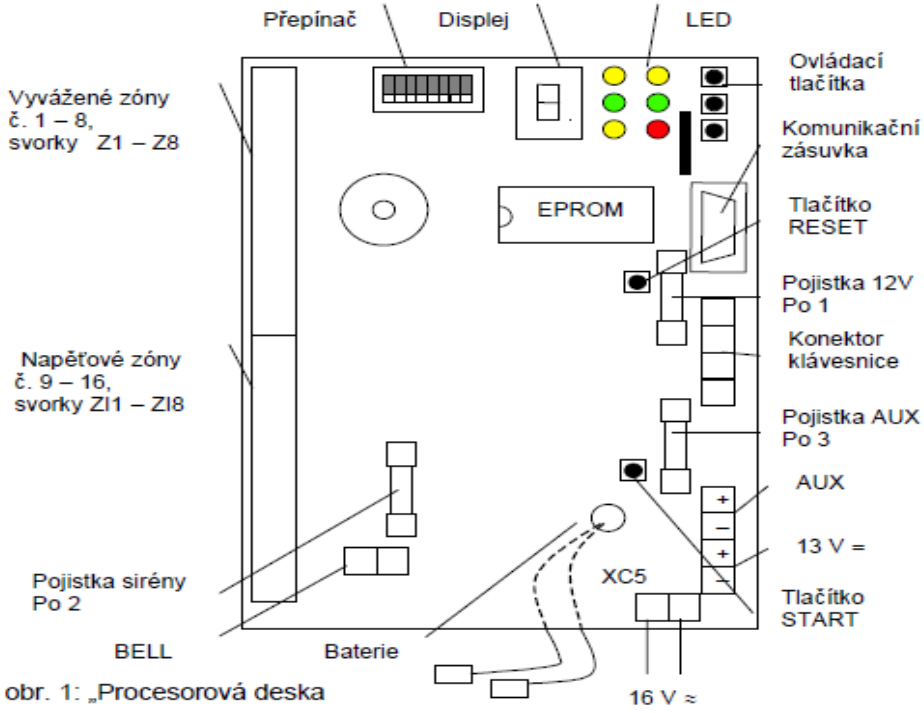
Ústředna má možnost downloadingu (tj. načteni hodnot z ústředny na dálku/ programování na dálku) po sériové lince nebo po telefonní lince. A také odpojování zón z klávesnice.

Obr. č. 12 Ústředna AMOS 1600



Zdroj: EUROSAT s.r.o., Duben 2009, [11]

Obr. č. 13 Procesorová deska ústředny AMOS 1600



Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.4. Klávesnice

Klávesnice je základní vstupní a výstupní zařízení sloužící k ovládání EZS. Na základě požadavku zákazníka a také vzhledem ke komfortnímu ovládání EZS budou nainstalovány dvě klávesnice. Poslouží to k efektivnímu využití zabezpečovacího systému vzhledem k rozlehlosti areálu. Při vstupu z obou stran budou pro oprávněné pracovníky k dispozici jak na východní tak i na západní straně areálu. Je to důležité i pro včasné zadání kódu při nastavené časové toleranci po vstupu a otevření objektu.

Klávesnice obecně se rozdělují do dvou základních skupin. Jde o klávesnice LCD a klávesnice LED.

4.4.1. Klávesnice LCD

Informace sloužící k obsluze systému jsou zobrazovány na LCD display. U tohoto systému lze listovat v historii ústředny a zjišťovat, co se v systému dělo v určitý čas. Většina LCD klávesnic již komunikuje s obsluhou s českým popisem. Klávesnice LCD je připojena do ústředny pomocí sběrnice. Sběrnici lze zapojit do tvaru hvězdy nebo do tvaru stromu. Sběrnice digi-bus je 4 žilová komunikační sběrnice umožňující obousměrnou komunikaci mezi ústřednou a klávesnicí. Klávesnice grafika umožňuje jednoduché a přehledné ovládání systému. Na velkoplošném LCD displeji je možné pomocí ikon ovládat a programovat celý systém. Grafiku lze uživatelsky přizpůsobit pomocí programů. Pomocí programu lze navíc vytvářet půdorys místností i s umístěním čidel. Tato funkce, kdy klávesnice graficky zobrazuje objekt i s narušenými zónami, umožňuje maximální přehled o narušených zónách přímo na LCD. Půdorys s čidly si může jednoduše vytvořit a nahrát do klávesnice přímo konečný uživatel pomocí programu. [4]

4.4.2. Klávesnice LED

Informace sloužící k obsluze systému jsou zobrazovány pomocí LED diod. Tento systém je méně přehledný a pro obyčejného uživatele náročnější na ovládání ale také výrazně levnější. Komunikace mezi klávesnicí a obsluhou probíhá zobrazováním informací na LED diodách pomocí tří stavů, dioda svítí, dioda nesvítí, dioda bliká.

4.4.2.1. Klávesnice ESPRIT 636

Pro náš systém a ústřednu jsou primárně k ovládání určeny klávesnice ESPRIT řady 636. Jedná se klávesnice LED, kdy pro komunikaci slouží klávesnice s osmnácti klávesami.

Klávesnice Esprit obsahuje 12 zónových kláves, osm funkčních kláves a akustický piezoměnič. Okamžitě prostřednictvím těchto prvků upozorňuje na poplach v systému a jiné funkční stavy zařízení. Pohybové detektory, požární hlásiče, čidla destrukce skla, stejně jako vibrační snímače a magnetické kontakty budou sledovány procesorovým mozkem a celkový stav systému je možné sledovat na přehledné klávesnici. Vše, co je potřeba vědět o bezpečnostním systému, je jednoznačně a jednoduše zobrazováno na klávesnici Popis klávesnice uvedený níže je dokonalým popisem funkčních prvků klávesnice. Zónové klávesy zobrazují stavy v jednotlivých zónách. Jestliže příslušná klávesa nesvítí, stav odpovídající zóny je "klid", pokud svítí trvale, zóna je narušená (pohyb v prostoru, nezavřené okno, dveře). Pokud klávesa bliká, odpovídající zóna jeví známky sabotáže (porušení tamperu, zkrat vedení). Pokud je naprogramováno, zprávy o sabotáži se přenáší na monitorovací stanici (pult centrální ochrany PCO). Kdykoliv je stisknuta klávesa, bzučák klávesnice krátce pípne (0.5 sec tónem), čímž potvrzuje akceptování stisku.

Po zadání celého příkazu na klávesnici je toto provázeno rovněž akustickým signálem. V zásadě se jedná o dva různé zvuky:

- Potvrzovací tón - Je-li příkaz úspěšně zadán (např. zapnuto/vypnuto), piezoměnič produkuje sérii krátkých pípnutí - přerušovaný tón.
- Konec/odmítnutí - Pokud příkaz není zadán správně nebo se systém vrací do předchozího stavu, piezoměnič generuje dlouhý nepřerušovaný tón.

Na základě našich požadavků naprogramujeme tzv. dělený systém. Každou zónu přiřadíme do části A nebo části B, případně do obou. Rovněž uživatelské kódy budou nastaveny tak, aby zapínaly/vypínaly jen jednotlivé části nebo obě zároveň. Klávesnice pak zobrazuje stav obou částí. Pokud je systém rozdělen a je-li zapnuta jen část A, pak klávesa 11/STAY bliká; pokud je zapnuta jen část B, pak bliká klávesa 12/AWAY. Pokud je zapnut celý systém, blikají obě klávesnice současně.

Nastavíme, zda systém bude akceptovat čtyř nebo šestimístné kódy a zároveň definujeme přístupová práva jednotlivým kódům. Každý přístupový kód je tvořen čtyřmi nebo šesti číslicemi.

Tab. č. 7 Tabulka volby přístupových kódů

Každý uživatelský kód je identifikován dvěma číslicemi - číslem kódu:			
přístupový kód	číslo kódu	přístupový kód	číslo kódu
master 00	00	uživatelský kód 3	03
uživatelský kód 1	01	uživatelský kód 4	04
uživatelský kód 2	02	atd. až uživatelský kód 48	

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

Nadstandardní a účelná může být z hlediska obsluhy volba zadání kódu pod nátlakem. Jestliže máte od instalační firmy povolen 48 kód jako Duress, je po jeho natipování na klávesnici odeslána zpráva na policii nebo pult centrální o tísni. Kód normálně ovládá ústřednu dle svých práv, ale vždy po jeho zadání je odeslána tato zpráva. Funkci lze povolit pouze pro kód číslo 48. [9]

Všechny klávesnicové povely se uskutečňují po sobě jdoucími stisknutími jednotlivých kláves. Výjimkou je stisknuti kombinace dvou kláves najednou, čímž se aktivuji funkce Požár [F], Nemocnice [A] a Tíseň [P]. Aktivaci tří klávesových panik poplachů je provedena následující kombinací kláves s přiřazením jednotlivých poplachů PANIK 1 [1] + [3] PANIK 2 [4] + [6] PANIK 3 [7] + [9].

Jak jsme již uváděli výše, klávesnice poskytuje kompletní informaci o stavu ústředny pomocí kontrolek kláves (všechny kromě klávesy CLEAR), kontrolek READY, ARMED a bzučáku. Význam kontrolek se může měnit podle stavu, v němž se systém nachází. Klávesnice se standardně nachází ve výchozím stavu. Pokud nebude po dobu dvou minut stisknuta žádná klávesa, klávesnice se vždy vrátí do výchozího stavu. Význam kláves a kontrolek ve výchozím stavu je znázorněn na obr. 1. Kontrolka ARMED sviti, když je alespoň jedna zobrazovaná sekce aktivovaná, kontrolka READY svítí, když jsou všechny neaktivované zobrazované sekce připraveny k aktivaci.

Bezpoplachový vstup do chráněného prostoru lze uskutečnit prostřednictvím vstupní / výstupní trasy. Po narušení prvního senzoru na této trase klávesnice akusticky upozorní na nutnost vypnout systém. V době, než uplyne čas vstupního zpoždění, je třeba zadat přístupový kód. Pokud jsme zadali kód špatně, zmáčkneme klávesu [CLEAR] a kód

zadáme znovu. Po korektním zadání kódu zhasne červená dioda ARMED, bzučák klávesnice vydá potvrzovací tón a utichne. [9]

Obr. č. 14 Klávesnice Esprit 636

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

Tab. č. 8 Popis klávesnice Esprit 636

Tlačítko	Popis klávesnice
√	Zelený svit indikuje klid v systému. Blikání upozorňuje na čas zpoždění pro odchod.
	Červený svit indikuje zapnutí systému do ostrahy. Blikání signalizuje poplach
1-6	Stiskem a 3 sec. podržením - povolujeme / zakazujeme chime u zón 1 – 6
8	Stiskem a 3 sec. podržením - povolujeme / zakazujeme chime u klávesových zón.
9	Stiskem a 3 sec. podržením - povolujeme / zakazujeme umlčení akustické signalizace klávesnice.
10	Pokud je povoleno instalační firmou lze 3 sec. stiskem řádně zapnout systém do ostrahy.
11	Při zapnutém systému signalizuje blikáním zapnutí STAY nebo podsystému A
12	Při zapnutém systému signalizuje blikáním zapnutí AWAY nebo podsystému B
2ND	Pokud jsou narušeny zóny s vyšším číslem než 12 je tento stav indikován svitem klávesy 2nd. Stiskem této klávesy dojde k přepnutí ze zobrazování zón 1 – 12 na zobrazování 13 – 24.
TRBL	Svitem je indikována přítomnost poruchy. Stiskem zobrazíte, o kterou poruchu se jedná.
MEM	Svitem se indikuje uložení zón, které během posledního zapnutí vyvolaly poplach.
BYP	Slouží pro vyřazení zón z ostrahy – uvedeno v manuálu.
CLEAR	Ruší omyly, vrací klávesnici do původního stavu, maže paměť.
ENTER	Potvrzuje příkazy zadávané z klávesnice, ukládá do paměti zadaná data

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.4.2.2. Zobrazení poruch

Ústředna neustále kontroluje svůj stav a je schopna rozlišit 10 poruchových stavů a ty zobrazit na klávesnici. O 8 poruchových stavech může zaslat zprávu na PCO, je-li naprogramováno. Jestliže systém vyhodnotí poruchový stav, rozsvítí se klávesa [TRBL] a pokud je povoleno, ozve se bzučák klávesnice. Zmáčknutím klávesy [TRBL] se klávesnice přepne do režimu zobrazování poruch. Svit kláves indikuje přítomnost příslušné poruchy. Zmáčknutím libovolného tlačítka (kromě [2ND]) se klávesnice přepne do normálního režimu zobrazování zón. V režimu zobrazování poruch se při stisku [CLEAR] mažou poruchy, které jsou již odstraněny, ale jsou uloženy v paměti. [11]

Tab. č. 9 Zobrazení poruch na klávesnici a jejich význam

Zobrazení poruch		
Klávesa [1]	Porucha baterie / baterie nepřipojena	Baterie není připojena nebo má tak nízkou kapacitu, že nevyhověla testu baterie. Baterii je potřeba vyměnit.
Klávesa [2]	Selhání napájení	Není připojeno napájení AC, a/nebo baterie není dobíjena, a/nebo baterie je přebíjena. Pro přenos zprávy na PCO může být programováno zpoždění. Jestliže je během doby zpoždění napájení obnoveno, je přenos anulován. Při této poruše klávesa [TRBL] rychle bliká.
Klávesa [4]	Nezapojena siréna	Není připojena siréna na výstup BELL.
Klávesa [5]	Přetížení výstupu sirény	Pokud mikroprocesor vyhodnotí proudové přetížení výstupu BELL, automaticky odpojí tento výstup. Odpojení je signalizováno svitem klávesy [5]. Po odeznění přetížení se výstup automaticky obnoví.
Klávesa [6]	Přetížení výstupu AUX	Při proudovém odběru z AUX větším jak 1A, (748ES 3A) mikroprocesor automaticky odpojí tento výstup. Při odeznění přetížení se výstup automaticky obnoví.
Klávesa [7]	Porucha komunikace s PCO	Pokud se komunikátor nemůže spojit s monitorovací stanicí, je to indikováno svitem klávesy [7]. Zpráva o tomto je uložena do paměti událostí.
Klávesa [8]	Porucha časové kontinuity	Po totálním výpadku napájení (AC i baterie) se musí do ústředny zadat čas následující procedurou. [ENTER] + kód - instalační / master / uživ.1 + [MEM] + dvě číslice pro hodiny (00-23) + dvě číslice pro minuty (00-59) + [ENTER]. Ústředna má reálný čas a porucha 8 zmizí.
Klávesa [9]	Porucha tamperu nebo vedení	Je narušeno vedení k čidlům nebo tamper čidel (čidlo je otevřené).
Klávesa [10]	Monitorování telefonní linky	Je odpojena telefonní linka.
Klávesa [11]	Porucha požární zóny	Jestliže systém vyhodnotí poruchu požární zóny, rozsvítí se klávesa [11].

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.4.3. Přístupové kódy

Většina funkcí, které poskytuje ústředna AMOS 1600, se provádí zadáním příslušného kódu. Ústředna umožňuje zadat až 18 různých přístupových kódů. Přístupové kódy jsou čtyřmístné nebo šestimístné dekadické číslo, sloužící k aktivaci a deaktivaci systému. Přístupovému kódu lze přiřadit sekce, které lze tímto kódem ovládat. Podle nastaveni systému, lze tyto sekce nastavovat buď jednotlivě, anebo lze změnit stav všech sekcí najednou. Změnu stavu jednotlivých sekcí se provádí pomocí menu (svíticích kláves), které se objeví po zadání přístupového kódu. Kódy se používají rovněž pro vstup do instalačního režimu a pro zadávání uživatelských funkcí. Délku použitých kódů může měnit pouze technik při programování. Pro standardní využiti se používají čtyřmístné kódy. Šestimístné kódy, u příkladů jsou uvedeny v závorce, zajišťuji větší bezpečnost systému. Přednastavené instalační a master kódy jsou uvedeny v systémovém manuálu. [11]

4.4.4. Master kód

Tento speciální kód slouží jak k aktivaci a deaktivaci ústředny, tak i k umlčení sirény po poplachu, programování dalších 16 přístupových kódů a k volání dalších uživatelských funkcí. Prvotní nastavení ústředny zakazuje uživateli master kód změnit. Ústředna může byt naprogramovaná instalačním technikem tak, aby si uživatel mohl master kód změnit. Ústředna má k dispozici také druhy master kód, který plní stejnou funkci a lze jej využit v případě, kdy jsou určení dva správci systému. Master kódy poskytují přístup do všech sekcí systému. [11]

4.5. Kamerový systém

Doplňkovou službou k zabezpečení celého areálu je kamerový systém. Vzhledem k ceně a i k doporučení od odborníků jsme nepoužili tento systém k přímému vyvolání poplachů – snadná náchylnost na falešné poplachy. Bude sloužit především jako doplněk a podpora zabezpečovacího systému. Zde pak půjde o trvalý záznam v časově uzavřené a nastavené smyčce a samozřejmě vzdálený přístup jak pro kontrolu majitelům firmy tak pro dálkové ověření případných poplachů pro pult centrální ochrany vyvolaných jinými součástmi zabezpečovacího systému.

Pro tyto funkce jsme zvolili kamery s infrapřísvitem KPC s objektivy 3,6mm a 8mm , zařízením SDVR 4300 pro záznam s diskovým polem o kapacitě 250GB. Na toto

zařízení můžeme zaznamenat v odpovídajícím rozlišení zhruba jeden měsíc trvalého záznamu. Přístroj má dálkový přístup přes LAN a umožní výše zmíněný vzdálený přístup. Dále je možné uvažovat o externím infrapřísvitu, otázkou je samozřejmě cena.

Vzhledem k tomu že se jedná o veřejně přístupný prostor prodejny je třeba dle platné legislativy zažádat o povolení na Úřadu před zpracováváním osobních údajů.

Ten určí v jakém rozsahu a za jakých podmínek a kde je možné záznam pořizovat.

4.5.1. Kamery a jejich vlastnosti

Kamera pracuje podobně jako lidské oko. Snímá odražené světlo, pocházející z přirozených (Slunce, měsíc, hvězdy), či umělých (žárovky, zářivky, výbojky) zdrojů. Pomocí soustavy čoček jej směřuje na světlo citlivý prvek (CCD, CMOS) a pomocí vnitřních obvodů jej dále zpracuje.

4.5.1.1. Optická soustava kamery

Soustava čoček v kameře pracuje obdobně jako lidské oko. Má za úkol nasměrovat odražené paprsky, od snímané scény, světla na světlo citlivý prvek (CCD, CMOS). Obecně se dá říci, že čím je průměr objektivu větší, tím je také vyšší množství světla dopadajícího na senzor a díky tomu dosahujeme kvalitnějšího obrazu. S rozměry objektivů roste také jejich cena, proto používáme přiměřeně velké objektivy a spíše se snažíme dosáhnout dobrých světelných podmínek. Vždy je nutné volit vhodný objektiv na základě požadavků zadavatele.

Rozlišujeme 4 stupně rozpoznání objektu a za předpokladu použití CCTV systému se 400 řádky dělíme následovně:

- identifikace = rozpoznání detailů obličeje. Alespoň 120 % výšky obrazovky;
- rekognoskace = rozpoznání obrysů objektu. Minimálně 50 % výšky obrazovky;
- detekce = zjištění přítomnosti objektu. 10 % výšky obrazovky;
- monitorování skupin osob. 5 % výšky obrazovky.

Při výběru objektivu by se mělo brát v úvahu:

- zorné pole objektivu;
- úroveň osvětlení snímacího prvku závisí na clonovém čísle objektivu a jeho propustnosti, která je ovlivněna konstrukcí objektivu.

Rozeznáváme tyto typy objektivů:

- s pevnou ohniskovou vzdáleností.(FFL);
- s proměnou ohniskovou vzdáleností;
- ZOOM objektivy (poměry až 1-50);
- panoramatické objektivy 360°;
- skryté objektivy (Jehlové objektivy - Pinhole Lens);
- speciální objektivy.

4.5.1.2. Uspořádání kamery

Optická soustava přenáší světlo na senzor. Zde je scéna snímána bod po bodu a řádek po řádku. A optický signál je převeden na elektrický. Frekvence snímání se liší od 25 cyklů za sekundu 25Hz až po 4,2 milionů cyklu za sekundu u kamer s vyšším rozlišením. Elektrický signál z kamery je časově proměnná funkce. Další elektronické obvody v kameře produkují tzv. synchronizační pulzy, díky nim je následně možné obraz zrekonstruovat na monitoru u analogových systémů. Signál je poté poslán k zobrazení, či dalšímu zpracování drátově či bezdrátově. Téměř všechny kamery používají snímače CCD a CMOS. V podmínkách s nedostatečným osvětlením se užívají citlivější ICCD snímače. V poslední době se nasazují do kamer digitální signálové procesory (DSP). Ty zajišťují celou řadu funkcí např. Elektronické ovládání uzávěrky, clony, zoom, synchronizaci a časování, ovládají skenování a zajišťují kompresy obrazu atd.

4.5.1.3. Digitální kamery obsahuje následující části

- **Optiku** (Lens) Směřuje paprsky světla na snímač.
- **Snímač** (sensor) CCD, CMOS světlo citlivý prvek převádí optický signál na elektrický.
- **Video processor** (DSP) zajišťuje celou řadu funkcí např. Elektronické ovládání uzávěrky, clony, zoom, synchronizaci a časování, ovládají skenování, ovládání pohybů a zoom kamery PAN/TIL, kompresy obrazu, ovládání alarmových vstupů a výstupů atd.
- **Ovládání snímání řádků a sloupců** (Column / row pixel scanning)
- **Synchronizace a časování** (Timing and synchronizing) možnost synchronizace z vnějšího zdroje synchronizačních pulsů.

- **Komprese videosignálu** (Video signal compression) Obvod zajišťující kompresy snímků. To je možno řešit i přímo v DSP, ale je to náročná operace na výkon.
- **Komunikační porty** (Ethernet, Wireless port).

S příchodem digitálních kamer a možnosti zpracovávat obraz na PC a digitálních zobrazovacích zařízeních (LCD, plazma) se změnil přístup ke snímání obrazu. Po sejmutí obrazové informace, maticí světlo citlivých prvků na snímači CCD či CMOS, již není potřeba převádět signál podle některé z televizních norem (PAL, SECAM, NTSC) na 625 respektive 525 viditelných řádků a frekvenci 50/60Hz. Ale obraz jako takový je rozdělen na malé body (pixel) nesoucí informaci o intenzitě a barvě. A po vzoru informačních technologií může nabývat obraz řadu rozlišení a poměru stran. Výhodou digitálních kamer je možnost volby rozlišení a rychlosti snímání.

Dalším krokem ve vývoji kamer byla implementace komunikačního rozhraní typu ethernet do kamery. Díky tomu může kamera posílat záběry na libovolné místo na planetě (kde je internet). Přístup ke kameře je chráněn heslem, jen vybrané osoby mohou dané záběry vidět. Díky tomu, že propojení kamery po internetu je obousměrná komunikace, je možné tímto způsobem kameru ovládat (PTZ), nebo využít programovatelné výstupy na kameře a ovládat tak libovolné zařízení.

4.5.1.4. Snímání obrazu

Klíčovou součástí kamery je snímací element – optický senzor, který přímo ovlivňuje kvalitu obrazu Senzor, který může mít různou strukturu, rozlišení, citlivost a výrobní technologii. Každý obraz, v televizní obrazovce, monitoru, či projektoru je složen z různého počtu miniaturních bodů tzv. pixel. Jejich zdrojem jsou právě snímací prvky CCD a CMOS. Principielně je u obou technologií potřeba přeměnit světlo, v podobě dopadajících fotonů na snímač, následně převést na elektrický signál, který je dále upravován obvody v kameře jev, při kterém se při dopadu fotonu na polovodič uvolní pár elektron – díra se nazývá fotoefekt. Elektrony jsou vyráženy do vyšších vrstev a stávají se vodiči proudu. Fotoefektu se také využívá při výrobě solární energie, U CCD a CMOS tohoto jevu využívají fotodiody a tranzistory.

U senzorů je důležitá jeho citlivost, ta se zvyšuje spolu s plochou dopadajícího světla a efektivitou fotoelektrické přeměny. Ta je závislá na tvaru krystalu a na vlnové délce dopadajícího světla. Obecně platí, že čím je plocha elementu větší, tím se zvyšuje i

citlivost senzoru a pro dosažení kvalitního obrazu pak postačuje menší osvětlení. Jednotlivé obrazové elementy mohou být realizovány za pomocí fotodiody nebo fototranzistoru. Nižší citlivost fotodiody se kompenzuje pomocí miniaturních čoček nad elementem.

4.5.1.5. Rozlišení v televizních normách

V souvislosti s omezením normy počtu řádků a poměru stran dosáhneme maximální rozlišení, po digitalizaci obrazu pro standarty PAL 704×576 pixel a pro NTSC 704×480 pixel. To odpovídá 0.4 megapixel

V zabezpečovací technice se používají rozlišení odvozené z těchto norem. S příchodem digitálních kamer se omezení standardy stávají bezpředmětná a začínají se používat rozlišení běžná v informačních technologiích. Jsou to hodnoty odvozené z VGA (Video Graphics Array), vyvinuté pro PC. Jeho hodnota je 640x480. Další změnou přicházející s užitím digitálních kamer je poměr stran. Můžeme volit 4:3,16:9 atd.

Z hlediska množství detailů ve snímané scéně je vyšší rozlišení vhodnější. Dnes není problém dosáhnout u kamery rozlišení 4168x4168, čímž se dostáváme na 16megapixelů. Množství detailů ve scéně bude nesrovnatelné. V průmyslu komerční bezpečnosti, se využívá kamer s vysokým rozlišením ke sledování davů a identifikace pachatele ze záběru pořízeného kamerou s vyšším rozlišením je mnohem snadnější, také algoritmy analýzy videa aplikované na vyšší rozlišení dosahují přesnějších výsledků.

4.5.2. Kamera KPC-N680WPH

Je to barevná kamera s vysokým rozlišením a nočním viděním. Kamera je vybavena digitálním zpracováním signálu a přídavnou funkci WDR (Wide Dynamic Range) a ovládání pomocí OSD menu.

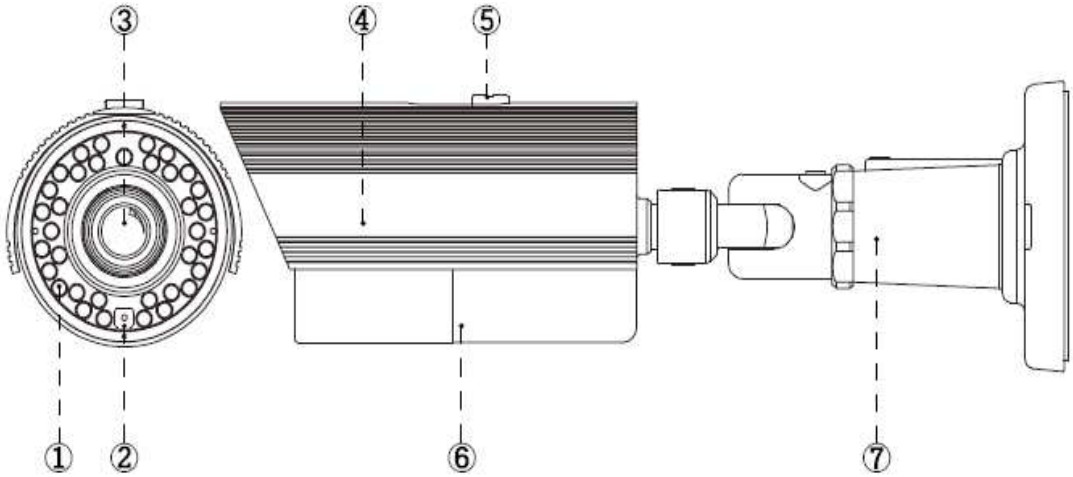
Barevná bezpečnostní CCD kamera je vybavena IR reflektorem. Je zejména vhodná pro sledování vjezdů, zahrad, garážových stání, okolí rodinných domků a prakticky všech venkovních i vnitřních prostorů. Díky aluminiovému obalu je dokonale odolná vůči povětrnostním vlivům, prachu a dalším nečistotám. Vestavěná špičkové IR technologie podává realistický obraz i v noci. Instalovaný 8.0 mm objektiv, který má zorný úhel 40° je schopen sledovat vzdálenější předměty a prostranství v jednom záběru.[11]

4.5.2.1. Technické parametry kamery:

- formát signálu: PAL/NTSC;
- čip: SONY 1/3“ SUPER HAD CCD s dvojitou hustotou vertikálního prokládaní;
- systém snímání: 2 : 1 prokládaně;
- horizontální rozlišení: 550 TV řádků (BAREVNĚ);
- digitální pomalá elektronická závěrka: PAL: 1/50 - 1/100,000 – Auto;
- S/N poměr: Více jak 48dB (AGC vypnuto);
- citlivost: 0.001 Lux (IR LED aktivní) při zapnuté funkci DSS - digital slow shutter - digitální pomalá elektronická závěrka;
- gamma korekce: $\gamma = 0.45$;
- synchronizace: vnitřní;
- video výstup: kompositní 1 [Vp-p] 75Ω nesymetrický;
- napájení / odběr: DC 12V (±10%) / max. 630mA, volitelně verze s napájením AC 24V;
- pracovní teplota: -10˚ C ~ + 50˚ C;
- skladovací teplota: - 20˚ C ~ + 60˚ C;
- přípustná vlhkost: 10% ~ 80%;
- 8 privátních zón;
- detekce pohybu;
- IR LED: 35 kusů IR LED automaticky spínané soumrakovým spínačem, dosvit až 40 metrů;
- délka IR vln: 850nm;
- úhel IR LED: ±15 stupňů;
- funkce DWS - protekce reflexů IR LED;
- kabel skryty v držáku;
- aplikace: venkovní prostředí / vodotěsná – krytí IP 67;
- rozměry: 75mm(Ř) x 120mm (s clonou proti slunci).

Obr. č. 15 Kamera KPC-N680WPH

Obr. č. 16 Popis kamery KPC-N680WPH



Popis k obrázku:

1. Deska IR přísvitu, IR LED - 35ks, 850nm
2. Optický snímač
3. Objektiv
4. Sluneční clona
5. Šroub k upevnění sluneční clony
6. Kryt kamery - přední a zadní díl
7. Držák

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

4.5.2.2. Další funkce kamery

Funkce WDR úroveň dynamického rozsahu - (Wide Dynamic Range) umožňuje přesně zobrazit detaily v obraze, i když jsou části obrazu příliš jasné, zatímco ostatní části obrazu jsou tmavé. WDR je vhodné zapnout, například pokud je ve snímané scéně více prosvětlených oken, je snímána vstupní hala a podobně.

Obr. č. 17 Ukázka funkce WDR

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

Sekundární video konektor umožňuje propojení se servisním monitorem pro snazší nastavení a servis kamery na místě instalace.

DC řízení clony, funkce AGC - automatické řízení zesílení, AWB -auto vyvážení bílé.[11]

Funkce IR přísvitu je zapnuto při osvětleni 1 Lux a vypnuto při osvětleni 3 Lux. Pro nejlepší podání obrazu kamera přepíná barevné režimy automaticky v závislosti na osvětlení. Barevný režim je zapnuty přes den, černobílý režim je zapnuty v noci.

Všechny funkce kamery se ovládají prostřednictvím OSD menu.

DSS - digitální pomalá elektronická závěrka – (Digital Slow Shutter) - Digitální pomalou závěrku je vhodné použít v případě velmi nízkého osvětlení snímané scény. Zpomalením rychlosti závěrky se zvýší kvalita obrazu, na CCD čip bude dopadat více světla.[11]

4.6. Záznamové zařízení

Pro záznam pořízeného signálu nám bude sloužit záznamové zařízení. Rozeznáváme v zásadě dva základní druhy pořizování záznamu. A to pomocí analogových nebo digitálních zařízení.

4.6.1. Analogová záznamová zařízení

Analogová zařízení využívají videorekordéry. Dříve se používaly téměř výhradně a občas se s nimi setkáváme i dnes.

- Videorekordér (VRC – Video Cassette Recorder) Jde o analogové záznamové zařízení, které slouží k záznamu a reprodukci videosignálu a zvuku. Jako záznamová média se využívají videokazety typu VHS (Video Home System) a S – VHS. [9]
- Pomaloběžné videorekordéry (Time Lapse) Jde o videorekordéry, které umožňují nastavení různých rychlostí záznamu. Na videokazetu typu E180 je možné nahrát až 960 hodin záznamu. [15]

4.6.2. Digitální záznamová zařízení

V současnosti se jednoznačně prosazují k záznamu obrazu z bezpečnostních kamer především digitální zařízení. A to jak vzhledem k jejich obrovské kapacitě a možnému potenciálu tak i k další snadnější práci s uloženými daty.

Rozlišujeme dva základní typy digitálních záznamových zařízení:

- DVR se záznamem na magnetickou pásku - Analogový signál se nejdříve digitalizuje A/D převodníkem a na magnetickou pásku se zaznamenává datový tok komprimovaný kodekem.
- DVR se záznamem na pevný disk - Záznam může probíhat na jeden nebo více pevných disků. [15]

4.6.3. Záznamové zařízení NADATEL SDVR-4000

Pro naši instalaci jsme vybrali záznamové zařízení Nadatel SDVR-4000. Je to triplexní čtyřkanálový digitální videorekordér (DVR) s kompresí MPEG-2 a zálohováním přes rozhraní USB, LAN a na CD.

Mezi jeho vlastnosti patří:

- real-time zobrazení i záznam všech čtyř kanálů;
- triplexní provedení (současné přehrávání, záznam a komunikace po LAN - monitorování i přenos veškerých dat);
- mód MUX - Možnost libovolného nastavení záznamové rychlosti pro každý kanál;
- vysoce kvalitní živý i zaznamenaný obraz v rozlišení 720x576;
- kvalita snímků je podpořena moderní kompresní metodou MPEG-2;
- možnosti rozhraní LAN: Vzdálené vyhledávání a přehrávání, monitorování aktuální scény, změna nastavení, ovládání PTZ kamer a nahrávání (upgrade) nového prostředí;

- připojení rozhraní LAN klasickým způsobem s pevnou IP, přes DHCP server, nebo přímo na ADSL modem;
- až čtyřkanálový záznam audiosignálu;
- různé možnosti spuštění záznamu: Pomocí detektoru pohybu, externího vstupu, tlačítkem na panelu, nebo pomocí časového plánu;
- vyhledávání záznamu dle data, času a kanálu v přehledném grafickém menu
- uživatelsky přívětivé grafické menu;
- snadné nastavení komplikovaného týdenního časového plánu;
- ikony poskytující různé informace o systému přímo v živém obraze;
- pokrokový detektor pohybu umožňující nastavení až čtyř samostatných oblastí pro každý kanál zvlášť;
- dva USB porty (v1.1) umožňující export uložených snímků (ne videa) a nahrávání (upgrade) nového prostředí pomocí USB disku;
- zachytávání snímků a možnost prohlížení jako JPEG souborů přímo v DVR, nebo v PC;
- možnost ovládání PTZ kamer;
- snadné ovládání pomocí hlavního panelu, nebo pomocí IR DO;
- rozlišení uživatele na základě vloženého hesla;
- detekce ztráty videosignálu.

V tomto zařízení máme skrytý potenciál, který bychom mohli následně využít při případném potřebě zvýšení kvality zabezpečení. Do DVR lze nainstalovat maximálně dva HDD, popř. jeden HDD a jednu mechaniku na vypalování CD. Nastavení se provádí zkratovací propojkou na pinech, umístěných zezadu mezi datovým (40-pin) konektorem a konektorem pro napájení.

DVR lze pomocí rozhraní LAN zapojit do klasické počítačové sítě, nebo do sítě ADSL. Možnosti připojení jsou celkem dvě a to buď přes klientský software, nebo pomocí webového rozhraní (pouze IE).

Možnosti softwaru:

- monitorování LIVE režimu;
- vyhledávání a přehrávání záznamů uložených v DVR;
- rozšířené zálohování - Ukládání dat do PC během monitorování LIVE režimu, nebo přehrávání a přímé kopírování zachycených snímků;
- plné nastavení systému;

- ovládání kamer;
- podpora dynamické IP adresy;

V nastavení DVR je nutné v menu SÍŤ povolit KLIENTSKÝ PŘÍSTUP, nastavit ČÍSLO PORTU pro komunikaci a zvolit typ sítě (LAN, ADSL) v níž je DVR používáno. Pokud je zvolen typ LAN, je dále možné nastavit použití DHCP serveru v dané síti, který pak automaticky přiděluje DVR IP adresu. Pokud se v síti žádný DHCP server nenachází, nebo jej nechcete z nějakého důvodu používat, bude nutné všechny parametry sítě (IP ADRESA, GATEWAY, MASKA PODSÍTĚ) nastavit ručně. Při použití sítě typu ADSL je nutné zadání přihlašovacího jména (ADSL ID) a hesla. Pokud je použita síť typu ADSL, nebo je používán DHCP server, je dobré mít v menu INFO povolen parametr POŠLI MAIL s nastavenou emailovou adresou a IP adresou SMTP serveru. Při jakékoli změně IP adresy DVR, toto odešle na zadanou emailovou adresu hlášení o této změně, z důvodu připojení. [11]

Obr. č. 18 Záznamové zařízení NADATEL SDVR-4000

Zdroj: EUROSAT s.r.o., Duben 2009, [11]

5. NAPOJENÍ NA PCO

Jak jsme již zmínili ve vlastnostech ústředny AMOS 1600 je možnost přímého napojení přes rádiovou frekvenci do sítě poskytovatele trvalého dohledu na pult centrální ochrany PCO.

V našem regionu působí několik organizací zajišťujících tuto službu. Po zhodnocení nabídek a také ostatních parametrů poskytované služby dohledu PCO jsme vybrali firmu Systém plus. Tato firma provozuje vlastní pult centrální ochrany s vlastním výjezdem a s garancí dojezdu. Na PCO je možno se připojit pomocí jejich vlastní rádiové sítě ve frekvenčním pásmu 459 MHz NAM Global. Záložní možnost je napojení telefonem a nebo přes GSM/GPRS síť.

Námi zvolená firma SYSTEM plus Zlín, s.r.o. je dodavatelem zabezpečovací techniky s dlouholetou tradicí a zkušenostmi v tomto oboru. Filozofií firmy je, jak sami deklarují, budování vzájemné prospěšnosti a důvěry. To je v této oblasti průmyslu komerční bezpečnosti velmi důležité.

V technické oblasti je politika firmy zaměřená na nejnovější poznatky v oborech zabezpečení a zvyšování kvality nabízených služeb. V obchodní oblasti se orientuje na pochopení současných a budoucích potřeb zákazníků, plnění jejich požadavků a snažíme se vyhovět a překonat jejich očekávání.

Firma zahájila svou činnost v roce 1990, přičemž od počátku její existence je kladen důraz na maximální profesionalitu, spolehlivost a kvalitu provedených prací a instalované techniky v zabezpečeném objektu. Samozřejmostí je, že veškeré informace a poznatky, které jsou firmě poskytnuty o majiteli, výši chráněných hodnot, či bezpečnostních opatřeních považují pracovníci firmy za přísně důvěrné.

Společnost SYSTEM plus Zlín, s.r.o. se zabývá:

- Provozem Pultu Centrální Ochrany s vlastním výjezdem a s garancí dojezdu. Na PCO je možno se připojit pomocí vlastní rádiové sítě NAM Global, telefonem, GSM/GPRS sítí.
- Provozem Pultu Požární ochrany s výjezdem Hasičského Záchranného Sboru.
- Projekcí, montáží, revizemi, servisem elektronických zabezpečovacích signalizací, elektronických požárních signalizací, kamerových, kontroly přístupu a docházky, kontroly obchůzek strážných.

- Servisem a připojováním elektrické zabezpečovací signalizace (EZS) na Městskou policii Otrokovice, TOMA Otrokovice
- Připojování požární signalizace (EPS) na PCO Hasičského záchranného sboru Zlínského kraje.

Od listopadu 2004 pracuje firma dle standardu systému jakosti ISO 9001. Volba této společnosti byla provedena nejen z hlediska pohledu nákladů na tuto službu, ale také především vzhledem k pověsti profesionality, které se firma těší v našem regionu a v neposlední řadě také vzhledem k parametrům, které jejich služba nabízí. Obrovskou výhodou je dojezdová vzdálenost zásahové jednotky a tedy i minimalizace času od vzniku a přenesení poplachu na PCO k dojezdu zásahové jednotky do chráněného areálu.

Firma nám také po dohodě bude provádět odborný dohled a na veškeré montáže systému a následně i revizi certifikovanou osobou. S výhledem do budoucna kdy lze také využít jejich služby připojování požární signalizace (EPS) na PCO Hasičského záchranného sboru Zlínského kraje nebo k rozšíření samotného systému o systém kontroly přístupu a docházky nebo využití jejich činnosti v oblasti střežení a sledování mobilních objektů.

Obr. č. 19 Mapa dojezdové trasy zásahového vozidla

Body: A – Systém plus s.r.o, B – Acris s.r.o - vzdálenost 950m

Zdroj: Google maps.cz, [17]

6. PRAKTICKÁ REALIZACE EZS

Po provedeném detailním rozboru dispozice areálu, zjištění předpokládaného počtu zón je nutno definovat počty podsystémů, určení počtu uživatelů, zjištění požadavků na automatizaci v objektu a výběru jednotlivých prvků použitých v EZS bylo potřeba tento systém instalovat.

6.1. Orientační nákres rozmístění zařízení

Pro snadnou orientaci poslouží pracovní nákres s rozmístěním jednotlivých prvků zařízení spolu s popisem potřebné kabeláže a propojení do daných míst. Samozřejmostí je pak dodržení doporučených instalačních výšek a umístění pro jednotlivé prvky zabezpečovacího systému.

6.2. Instalace kabeláže

Pro zabezpečovací systémy se využívají víceţilové vodiče, buď lankové, nebo s pevným jádrem. Který typ je vhodnější nelze jednoznačně říci. U lankových vodičů dochází s jejich stárnutím k povolování šroubovaných spojů a u kabelů s pevným jádrem dochází k oxidaci mědi a tím ke ztrátě kontaktu.

Pro datové přenosy se využívají kabely s průřezem vodiče 0,22 mm a pro napájení s průřezem 0,5 mm. Typy kabelů pak bývají označovány 2x0,22 mm + 2x0,5 mm. To znamená, že vodič obsahuje 4 žíly, dvě o menším a dvě o větším průřezu.

Správné provedení kabeláže je pro chod systému nezbytností. Mnohé firmy šetří již zde a tím pak trpí kompaktnost celého systému. Je proto dobré uvést několik zásad, které by měly být dodrženy:

- rozvod je tažen ve větvích, na které jsou připojovány detektory. Každý detektor potřebuje minimálně 2 žíly pro napájení a dvě žíly pro přenos svého stavu.
- každá větev by měla být ukončena tak, aby v posledním detektoru byla rezerva dvou žil
- nikdy by nemělo být připojeno na dvě žíly více detektorů. V konečné ceně na kalkulaci to nebude mít velký vliv
- kabeláž je dobré provést do ochranných trubek (husí krk)

Po výběru míst pro osazení detektorů, rozvržení plánovaných tras a umístění ústředny započala realizace. Bylo provedeno měření a prověření podle realizačního projektu, kudy vedou stávající elektrická vedení a především ověření viditelnosti u optických závor. Byly připraveny chráničky pro přenosové kabely a připraveny průchody do místnosti s ústřednou. Jednotlivé průchody, místa osazení detektoru, případně vyvedení rezervních kabelů pro rozšíření systému byly propojeny.

K instalaci byly vybrány dva typy kabelů. Pro venkovní rozvody kabel CEKFLE 5x4x0,5 a pro vnitřní rozvody kabel CYKFY 3x2x0,5. Jednotlivé zkratky kabelů definují jejich vlastnosti. Kabel CEKFLE je odolnější a proto je určený pro venkovní prostředí, ale je dražší. Kabel CYKFY je levnější a je určen pro vnitřní instalace. Každý kabel byl po naměření na koncích popsán a označen pro snazší identifikaci při zapojení. Kabely byly přivedeny do všech míst, kde budou nainstalovány jednotlivé prvky zabezpečovacího systému.

6.3. Osazení základen pro elektronické prvky

Po nainstalování kabelového vedení, byla započata montáž spodních částí detektorů a prvků EZS. Každý prvek, který měl být připevněn na stěnu nebo do vybraných míst, byl rozebrán a část, která měla být osazena na stěnu, byla připravena k montáži. Pokud neobsahovala montážní otvory, byly tyto otvory vyvrtány, nejčastěji u detektorů. Po přiložení na stěnu bylo zaznačeno místo pro vyvrtání děr a osazení hmoždinek. Spodní díly prvků byly připevněny a do nich protaženy kabely a přichystány ke kontrole, která prověřila, že kabely nejsou porušeny a signál se po kabeláži šíří. Nad klávesnice umístěné ve venkovním prostředí byly umístěny ochranné plechy zabraňující přímému dopadu srážek na tyto prvky. Kabeláž byla proměřena a označena pro zapojení. Drobné uvolnění kabeláže bylo opraveno.

6.4. Zapojení elektronických prvků

Po proměření následovala montáž elektroniky a osazení modulů na plastové distanční sloupky v boxu ústředny. Následovalo zapojení kabeláže do svorkovnic detektorů, ústředny a klávesnic. Rezervní vodiče byly označeny a svázány tak, aby nepřekážely a nezasahovaly do instalovaných modulů.

6.5. Zprovoznění systému

Po zapojení elektroniky bylo provedeno proměření větví napájecího napětí, následovalo proměření uzemnění a uzemnění kovových krytů elektroniky, které mělo odhalit, zda není v zapojení chyba. Byla provedena vizuální kontrola všech prvků a vizuálně prověřeno zapojení. Po této kontrole bylo zapojeno napájení všech prvků systému a systém byl zprovozněn. Provedla se inicializace jednotlivých prvků, připojených na sběrnici BUS. Po inicializaci následovalo propojení PC a EZS a nahrání firmware do software. Software vytvořil architekturu namontovaného systému, a jednotlivým prvkům, zónám a zařízením byly přiděleny požadované informace a hodnoty sloužící k ovládání celého zařízení. Pak se doladily drobné nedostatky a odzkoušela se funkčnost systému.

6.6. Připojení ústředny do rádiové sítě a k PCO

Po zprovoznění systému bylo potřeba doladit a ověřit spojení na pult centrální ochrany. Poskytovatel má licenci a provozuje svoji vlastní rádiovou síť na frekvenci 495 MHz. Pomocí této sítě bude tedy primárně připojena ústředna na pult centrální obsluhy a trvalým dohledem a připravenou výjezdovou jednotkou. Na ústředně byla nastavena požadovaná frekvence a na pultu centrální ochrany poskytovatele bezpečnostních služeb bylo ověřeno připojení ústředny do sítě. Následně byla změřena síla signálu a byly provedeny první zkušební datové přenosy. Po ověření komunikace byla ústředna pně funkční.

Další praktické ověření přenosů poplachových signálů bude provedeno při samotném testování pomocí praktických zkoušek napadení areálu.

6.7. Připojení na Internet

Jako sekundární napojení části systému, především pro vzdálený přístup do kamerového systému, můžeme využít připojení na internet. Investor sice nemá pevnou telefonní linku, ale využívá připojení na internet pomocí lokálního poskytovatele WIFI. Tímto poskytovatelem je firma IT-Help.cz, která poskytuje Wi-Fi připojení na frekvenci 5GHz s níže uvedenými parametry.

K příjmu tohoto signálu je na střeše kancelářské budovy umístěna panelová anténa s odpovídajícími parametry.

Obr. č. 20 Panelová anténa pro připojení do WiFi sítě na výložníku

Zdroj: vlastní zpracování

6.7.1. Parametry připojení:

- Rychlost připojení 4Mbps/2Mbps, sdílení 1:1
- Připojení k internetu bez časového omezení, neomezený objem přenesených dat
- Poštovní schránka 250 MB, WebHosting 300 MB
- 3 GB bezpečného prostoru pro zálohy
- Pevná IP adresa
- Hot line 24h x 7dní v týdnu, On-line statistiky přes webové rozhraní

Toto připojení je již několik měsíců využíváno a vzhledem k tomu, že do dnešního dne na něm nebyla zaznamenána žádná porucha, jeví se jako vcelku spolehlivé.

7. MĚŘENÍ A TESTOVÁNÍ SYSTÉMU

Po instalaci následovalo samozřejmě měření a testování samotné instalace a systému. V první řadě jsme pomocí nastavení úhlů a clonek nastavovali dosah venkovních PIR-MW čidel. Nastavení jednotlivých zón jsme ověřili vyvoláním poplachu – pochůzkovým testem na okrajích zón. Následně také vnitřní čidla v kanceláři a garáži. Při vyvolání poplachu byla také ověřena funkčnost venkovní sirény jak zvukový signál tak i optický.

Dalším testem bylo prověření funkčnosti systému při výpadku napájení distribuční sítě. Byly ověřeny vlastnosti akumulátorů kapacitním testem.

Po té bylo ověřeno spojení ústředny na pult centrální ochrany včetně umělého vyvolání poplachů jednotlivých komponentů. Provedli jsme otestování jednotlivých smyček systému EZS a ověřili jsme komentáře k jednotlivým smyčkám přicházející na pult centrální ochrany.

Samozřejmostí byla také konečná revize nainstalovaného zařízení. Při revizi nebyly zjištěny žádné závady a bylo konstatováno, že instalované zařízení je v pořádku a schopné bezpečného provozu.

Vzhledem k ceně bohužel nebyl prozatím nainstalován kamerový systém. Ovšem po jeho instalaci provedeme následující sled kroků. Na monitoru prověříme on-line sledování prostoru přes umístěné kamery. Zaostříme obraz a ověříme rozsah a kvalitu záznamu. Po telefonické domluvě následně ověříme také přenos signálu na dispečink firmy zajišťující ostrahu a také jejich přístup na základě nastaveného přiděleného oprávnění. Ve večerních hodinách pak otestujeme také funkci infrapřísvitu u kamer a opět ověříme přenášený obraz i záznam. Nakonec budou opět ověřeny všechny funkce dálkového přístupu do kamerového systému jak z pozice majitelů firmy, tak z obsluhy pultu centrální ochrany napojeného na systém.

7.1. Prověření pomocí narušení systému a jeho vyhodnocení

Po dohodě s firmou zajišťující ostrahu přes pult centrální ochrany jsme provedli několik způsobů imitace možného skutečného narušení a vniknutí do zastřeženého areálu. Provedli jsme několik typů napadení obsluhy a areálu.

7.1.1. Napadení obsluhy

Pokusili jsme se imitovat napadení obsluhy násilným pachatelem. Ověření časového zásahu jednotky na pokyn PCO jsme v tomto případě neprováděli. Zaměřili jsme se pouze na přenos do ústředny EZS a ověření odchozího alarmu na pult centrální ochrany. Sledovali jsme především možnost obsluhy co nejnenápadněji využít tísňového tlačítka umístěného pod obslužným pultem vedle pokladny.

7.1.2. Vniknutí do areálu přes sousedící objekty

Při této formě narušení jsme využili pro nás známého zřejmě jednoho z nejslabších míst systému a to zastřežení proti vniknutí přes střechy sousedících budov. Jelikož jsme o této slabině věděli, pokoušeli jsme se také nastínit škodu, která by za určitý čas mohla vzniknout vzhledem k tomu, než dojde k odhalení napadení systému a následnému dojezdu zásahové skupiny. Samozřejmě jsme se také teoreticky zabývali případným zajištěním důkazů proti možným pachatelům, což by byl v našem případě videozáznam ze zatím nenainstalovaného kamerového systému.

7.1.3. Násilné vniknutí do areálu přes hlavní vstupní brány

V tomto případě jsme imitovali vniknutí do areálu za účelem co maximální finanční škody, v podobě odcizení co největšího množství skladovaného materiálu nebo techniky za předpokladu, že útočník má představu o způsobu zabezpečení a je patřičně vybaven, přičemž se pokouší obelstít zabezpečovaný systém. Pro tento případ jsme si dohodli na centrále dohledu PCO zkušební výjezd zásahové skupiny poskytovatele trvalé ostrahy. Předpokládali jsme znalost o instalovaném systému, takže jsme do objektu pronikali přes plot s tím, že jsme se pokusili vyhnout optickým závorám. Nicméně ani při tomto typu útoku se nám nepodařilo obelstít PIR-MW detektor s antimaskingem a také proniknutí do prostor kanceláře by znamenalo okamžité odhalení.

7.1.4. Útok vandalů, případně konkurence

Poslední imitace útoku měla nastínit možnost vniknutí a poškození majetku vandaly případně konkurence za účelem vytvoření co největší škody nebo znemožnění tvorby a plnění dohodnutých činností poškozením nebo zničením výrobních a pracovních prostředků nebo skladovaného zboží a materiálu. Tady jsme brali v úvahu násilné vniknutí bez ohledu na instalované bezpečnostní zařízení nebo případné vhození zápalné láhve do areálu.

8. VYHODNOCENÍ JEDNOTLIVÝCH ÚTOKŮ

Po jednotlivých útocích samozřejmě následuje rozbor účinnosti jednotlivých prvků a opatření proti těmto narušení.

8.1. Případ napadení obsluhy

Impuls z tlačítka i odchozí alarm proběhl okamžitě a tím byla funkčnost nouzového tlačítka úspěšně ověřena. Při napadení obsluhy bylo zjištěno, že ideální pro vyhlášení poplachu by zřejmě byla i poplachová lišta, ale i skryté tlačítko se jeví jako dostačující a obsluha neměla problém toto tlačítko bezpečně a především nenápadně zmáčknout. Zde sehrálo roli těsné umístění tlačítka vedle pokladny.

8.2. Vniknutí přes střechu a způsobené škody

Tím že pachatel vnikl přes střechu a seskočil do nezastřežené zóny nedošlo samozřejmě k okamžitému vyhlášení poplachu na PCO. Ovšem v případě, kdyby se pokusil páchat jakoukoliv škodu, už by dříve či později byl nucen vniknout do střežené zóny a zároveň by tím i vyvolal poplach. Dojde k tedy k opoždění informace o narušení, ale vzhledem k možným škodám, které může spáchat v nestřeženém prostoru a vzhledem k namáhavému a často velmi obtížné manipulaci s jakýmkoliv odcizeným předmětem přes okolní střechy, jeví se nám toto zpoždění jako nevýznamné a riziko vysokých škod jako minimální.

Zároveň s vniknutím do areálu by se také dostával do záběru plánovaného kamerového systému a jeho činnost by tak byla zaznamenána případné trestní stíhání.

Jako problém se v tomto případě tedy jeví pouze proniknutí do nezastřežených oblastí v prostoru, který je jinak pokrytý detektory.

8.3. Násilné vniknutí za účelem odvozu zboží a materiálu

Varianta tohoto útoku by mohla být pro areál reálnou velkou hrozbou, pouze v případě že by selhal dálkový přenos na pult centrální ochrany. Pachatel musí překonat nejen mechanické zábrany, ale musel by také obelstít několik dalších zabezpečovacích prvků. V případě, že by tyto prvky ignoroval, měl by pouze asi tři minuty do příjezdu zásahového vozidla s hlídkou. Za tuto dobu nemůže reálně naložit a odvézt takové množství materiálu, aby vznikla majitelům výrazná škoda. Z hlediska tohoto typu útoku bez obelstění elektronických prvků se jeví areál jako velmi dobře zabezpečený.

Závažnějším typem vloupání za účelem zcizení majetku by byl případný útok pachatele obeznámeného poplachovými systémy. Zde by šlo pravděpodobně o útok takzvaně na objednávku. V tomto případě, by ale i tak musel pachatel vyřadit několik bezpečnostních prvků elektronického zabezpečovacího systému. V prvé řadě by musel obejít magnetické kontakty brány a to nejspíše tím, že by se pokusil proniknout do areálu přes pletivo. Tady by bylo třeba přemostit nebo jinak přejít přes kabeláž k infrazávorám, které částečně také slouží jako perimetrická zábrana. Následovalo by obelstění infrazávor a to jedině jejich kvalifikovaným vyřazením – což se nezdá jako příliš pravděpodobné ani zrovna jednoduché. Nebo jejich překonání pomocí připravené konstrukce. To už by možná připadalo v úvahu.

V další chvíli by se mohl pokusit zakrýt objektiv kamery, v případě že by byly nainstalovány a pak by se mohl pustit do odcizení majetku nacházejícím se v prostorech nezabezpečených PIR-MW čidly. Vyřazení těchto vysoce kvalitních čidel s antimaskingem se nám už ale z hlediska běžného pachatele a jeho možného zisku nejeví jako vůbec pravděpodobné. Zde již předpokládáme, že by došlo k odhalení pachatele. Průnik do kanceláří nebo garáže se skladem nářadí s obelstěním systému je dle nás také velmi komplikovaný a tedy i nepravděpodobný.

Jako slabé místo se nám tedy jeví zabezpečení perimetru pomocí mechanických zábran v tomto případě pletiva. Tady je určitě prostor ke zlepšování systému.

8.4. Škody následkem útoku vandalů nebo konkurence

Jako nejnebezpečnější a možná pravděpodobný útok se nám jeví kombinace útoku s prostředím obeznámeného pachatele, za účelem znemožněné provozu firmy a vytvoření co největší škody firmě.

Zde může jít jak o konkurenci, tak také o případně nespokojeného propuštěného zaměstnance nebo zákazníka. Zde je riziko škody opravdu vysoké. Pachatel jednak může být obecně obeznámen se systémem zabezpečení areálu, anebo ho naopak vůbec nemusí zajímat a zaútočí přes mechanické zábrany (plot) vhozením například zápalné láhve do areálu.

V tomto případě je nutné dbát především na vnitřní bezpečnostní předpisy firmy. A to jak ve sdělování přístupových kódů zaměstnancům tak také uvážené rozdělení

pravomocí k jednotlivým zónám. Jako samozřejmost by pak měla být okamžitá změna nebo zrušení přístupových kódů v případě odchodu zaměstnance.

Útok tohoto typu bude velmi těžké absolutně eliminovat a jako možné řešení by se mohlo jevit zvýšení mechanických zábran – plotu. Pro následnou eliminaci škod pak by také bylo vhodné rozšíření o elektronický protipožární systém. Jednak by to mohlo zlepšit případný zásah proti požáru způsobeným vandaly, ale také proti případnému požáru způsobenému například závadou na instalaci nebo odstavených pracovních mechanismech. Zároveň bychom tím mohli částečně eliminovat škody vzniklé případnými požáry.

9. KOMPLEXNÍ HODNOCENÍ SYSTÉMU A NÁVRHY OPATŘENÍ

Při jednotlivých typech napadení jsme zjistili možné slabiny systému. Jako kvalitní se nám jevila volba všech zámků a bezpečnostních vložek ve dveřích ve vyšším stupni zabezpečení a také systém univerzálního klíče byl pro investora dle jeho ohlasu komfortní.

V celku očekávanou slabinou bylo mechanické zabezpečení areálu oplocením. Tady by pomohla pouze otřesová čidla nebo změna oplocení na pevný železný plot s betonovým základem. Další slabinou je možnost průniku do areálu přes sousedící střechu. O tomto hendikepu víme již od začátku, nicméně řešení tohoto problému je možné jen uvnitř našeho areálu.

V případě napadení obsluhy je tísňové tlačítko dostatečné a spuštění sirény je výrazným výstražným efektem. Obsluha pokladny neměla problém toto tlačítko bezpečně skrytě aktivovat. Zvažujeme pouze to, zda by nebyla vhodnější forma tichého poplachu, aby nedošlo k případnému zkratovému jednání možného pachatele.

Jako nedostatečné je dle našeho názoru zabezpečení proti požáru a vzhledem k tomu že i na tuto eventualitu je zvolená ústředna připravena doplnili jsme dodatečně požární čidla alespoň do prodejny a kanceláří zahradnictví.

Pokud jde o zvolenou bezpečnostní agenturu funkce přenosu poplachů, byla několikrát ověřena a byla naprosto bezproblémová. Také dojezd zásahové jednotky poskytovatele ostrahy byla ve vynikajícím čase.

Plánovaný kamerový systém bude určitě dalším výborným pomocníkem, očekáváme jen horší rozlišení v případě tmy a pohybu na okraji dosahu záběru kamery. Přenosová rychlost pro vzdálený přístup přes internet bude určitě vzhledem k parametrům připojení dostačující a předpokládaná kvalita pořizovaného záznamu vzhledem k vlastnostem navrhovaných kamer bude jistě ve velmi dobré kvalitě.

9.1. Zabezpečovací prvky a jejich případné rozšíření

Po předchozích vyhodnoceních jsme investorovi navrhli následující rozšíření. Jedná se o několik bezpečnostních prvků, které by výrazně zvýšili kvalitu ostrahy objektu.

9.1.1. Oplocení

Pokud jde o slabý článek perimetrické ochrany objektu kterým je oplocení, tak zde jsme již při prvních návrzích chtěli využít otřesových čidel nainstalovaných na pletivo. Tyto otřesové čidla umožňují zachycení jakéhokoliv narušení plotu a je také velmi obtížné je obelstít. Bohužel vzhledem k ceně takovéhoto systému jsme museli od instalace upustit. Nicméně v případě že by to finanční situace majitelům zahradnické firmy dovolila, je náš systém pro toto rozšíření připraven a můžeme ho zahrnout do celkového konceptu EZS. Navrhovali bychom systém KeyGUARD který je prioritně určený pro střežení obvodového oplocení a venkovních prostor. Princip činnosti plotového detekčního systému je založen na vyhodnocení mechanických ruchů pomocí senzorického kabelu.

Systém vyvolá poplach, pokud se narušitel pokusí:

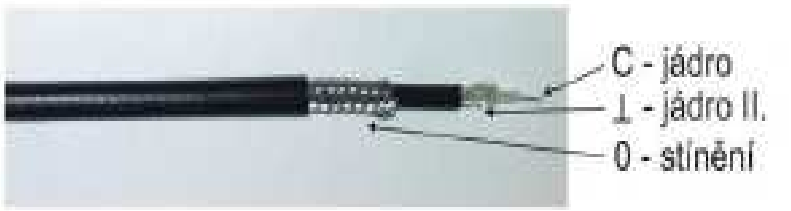
- přelézt přes plot
- prostříhat pletivo
- nadzvednout pletivo nebo konstrukci plotu
- vstoupit do střeženého prostoru

Mezi další základní vlastnosti patří:

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

Opět je to především otázka financí, v jakém časovém horizontu a v jaké výši budou k dispozici pro rozšíření EZS.

Obr. č. 21 Senzorický kabel



Zdroj: EUROSAT s.r.o., Duben 2009, [11]

9.1.2. Detektory

Detektory jako takové se velmi osvědčili. Především pak kombinované PIR-MW detektory které umí rozeznat zvíře od člověka. V tomto změnu bychom asi změny nedělali, maximálně bychom mohli doplnit k úplnému pokrytí areálu dvě čidla, což by ale také vyžadovalo doplnění kabelových rozvodů. Došlo by tím k hustějšímu pokrytí areálu a omezili bychom tím nezabezpečené místa.

Dalším doplněním, které určitě doporučujeme provést je instalace alespoň tří protipožárních čidel. Dvě by byly umístěny v kanceláři a šatně a jedno pak ve skladu nářadí. Při relativně malé investici rozšíříme systém EZS o elektronický protipožární systém EPS a výrazně tím můžeme zvýšit zabezpečení proti tomuto riziku. Ústředna je připravena na zapojení těchto detektorů a obousměrnou komunikaci s nimi.

Zvolili bychom kombinovaný detektor opticko-kouřový a teplotní FDR-36-SHR Opticko-kouřový a teplotní požární detektor je určen jako doplňková signalizace k systémům EZS. Detektory odpovídají normě EN54 a je možné je použít dle vyhlášky o Požární ochraně objektů. Podmínkou je jednoznačné dohledání poplachu na detektoru. Jeden detektor jedna smyčka ústředny.

Detektor pracuje na kombinovaném principu vyhodnocování vniknutí kouře do vyhodnocovací komůrky a překročení mezní teploty 57ºC. Na přítomnost kouře nebo zvýšené teploty reaguje detektor svitem LED diody a překlopením relé. Detekce kouře probíhá v optické měřící komoře a teplota je sledována termistorem. Optická detekce kouře je založena na principu vniknutí kouře do vyhodnocovací komůrky, která je prosvětlovaná IR diodou a tento svit je zpětně vyhodnocován. Vlivem kouře se změní odrazové parametry v komůrce a detektor vyhodnotí poplach

Aktivace poplachu proběhne při vniknutí kouře do detektoru nebo vyšší teplotě než 57ºC. K vyvolání poplachového stavu stačí detekce na jednom ze dvou senzorů.

Obr. č. 22 Opticko-kouřový a teplotní detektor FDR-36-SHR

Zdroj: OLYMPO controls, spol. s r.o. - Security Products, [14]

9.2. Kamerový systém

Plánované rozšíření EZS o kamerový systém bude zcela jistě výhodné. Díky této instalaci budeme mít nejen kvalitní dohledový systém jak pro majitele, tak i také pro pult centrální ochrany. V dohledovém kamerovém systému totiž máme další skrytou rezervu. Bylo by možné využít pomocí přiloženého softwaru na základě schopností kamer také střežit snímaný prostor. Jak už jsme ale uváděli dříve, ze zkušeností zabezpečovacích firem je tento způsob zabezpečení náchylný na falešné poplachy. Spíše by bylo praktické využít schopnosti tohoto zařízení vyvolat poplach v případě výskytu otevřeného ohně. Tím bychom rozšířili oblast zabezpečení chráněného areálu i proti tomuto druhu rizika.

9.3. Další možnosti v oblasti zabezpečení

Jako další možnost rozšíření EZS je také instalace přístupového systému. Tento systém by firma mohla využít pro evidenci a vyhodnocení docházky, přípravu podkladů pro mzdy, sledování přítomnosti na pracovišti a pohybu zaměstnance v průběhu pracovní doby. Systém by prováděl načítání dat do systému přes evidenční terminály pomocí identifikačních médií zaměstnanců. Zároveň bychom mohli tento systém využít jako přístupový systém k odkódování příslušných zón podle přístupových práv zaměstnance. ACS systémy umožňují i spolupráci s GPS systémy sledování vozidel.

Výstupy a data z tohoto sledování by mohly sloužit pro automatické vytváření záznamů o služebních cestách. Služba sledování vozidel pomocí GPS systému by umožňovala jak střežit a sledovat vozidla a navigovat a kontrolovat řidiče tak také chránit životy, zdraví a majetek a samozřejmě podpořit nízkonákladový management firmy.

I tato varianta rozšíření by mohla připadat v úvahu, v případě nárůstů činnosti a zvyšování počtu zaměstnanců společnosti a obzvláště v případě nárůstu finančních příjmů společnosti.

Obr. č. 23 Schéma principu docházkového systému

Zdroj: SIEMENS, spol. s r.o, Building Technologies 2009, [13]

ZÁVĚR

Tato práce mi poskytla zcela nový komplexní pohled na oblast elektronické zabezpečovací signalizace v průmyslu komerční bezpečnosti. Umožnila mi praktické ověření znalostí nabitých při studiu v oboru bezpečnostních technologií a zároveň také přímou konfrontaci praktických zkušeností zprostředkovaných spolupracujícími techniky bezpečnostní firmy.

V této práci shrnuji jednotlivé kroky od samotného návrhu řešení se zhodnocením potřeb daného zákazníka až po konečnou realizaci projektu. Snažil jsem se nastínit, co nás vedlo k výběru daných komponentů v patřičném rozsahu a kvalitě. Podrobněji pak popisuji jednotlivé prvky zabezpečovacího systému, principy jejich činnosti a také funkce, kterými disponují v souvislosti s jejich využitím pro začlenění do celkového konceptu ostrahy areálu zahradního centra.

Dále popisuji samotnou instalaci zařízení, některé zásadní postupy a materiály použité pro zkompletování celého systému EZS.

Nadstandardní je pak fyzické testování za pomoci námi definovanými typy útoků na zabezpečený areál a následné vyhodnocení těchto testů.

V závěru pak navrhuji možná opatření pro zlepšení kvality ostrahy, nebo případné rozšíření EZS o další funkce jako je EPS nebo systém ACS a tím tak zvýšit efektivitu a účinnost celého systému.

Skvělé bylo na celém projektu to, že šlo o reálný projekt s hmatatelným výsledkem.

Přinesl mi nejen další zkušenosti s návrhem EZS ale také mnoho dalších praktických zkušeností s problematikou komplexního zabezpečení a ostrahy objektů v průmyslu komerční bezpečnosti.

SUMMARY

The work gave me a whole new perspective on the complex area of electronic security alarm systems in the commercial security industry. It allowed me practical knowledge verification charged with study of the security technologies, while also a direct confrontation with practical experience of the security companies and its staff.

In the work I summarize the different steps of the actual design solutions to the appreciation of the customer needs to the final project accomplishment. I try to outline component selection of required types and quality. I also describe in detail view designed elements, its functions and whether it is suitable for integration into the overall design of garden centre security system.

I also describe installation of own device, some basic procedures and materials used to complete the ESS system.

Another part was the extra physical testing to help us define security attacks, its types and the subsequent evaluation of those tests.

In conclusion I suggest possible measures to improve the quality of security and possible expansion of additional functions such as FAS and ACS systems and thereby improvement of the effectiveness and function of the whole system.
I found great that it was a real project with a tangible results.

The project got me not only more experience with the real designed ESS but also many other practical knowledge about problems of safety installations and building security in the commercial security industry.

SEZNAM POUŽITÝCH ZDROJŮ

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

[2] KŘEČEK, Stanislav. Příručka zabezpečovací techniky, Praha, Cricetus, 4.vydání 2002. 350 s. ISBN 80-902938-2-4

[3] UHLÁŘ, Jan. Technická ochrana objektů II. díl - Elektrické zabezpečovací systémy. Praha: PA ČR, 2001. 208 s. ISBN 80-7251-076-2.

[4] ČERNÝ, Josef, IVANKA, Ján. Systemizace bezpečnostního průmyslu. 1. vyd. Zlín: UTB, 2006. 135 s. ISBN 80-7318-402-8

[5] ČANDÍK, Marek. Objektová bezpečnost II. 1. vyd. Zlín: Univerzita Tomáše Bati, 2004. 100 s. ISBN 80-7318-217-3

[6] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. 1. vyd. Zlín: Univerzita Tomáše Bati, 2003. 64 s. ISBN 80-7318-119-3.

[7] VLČEK, Jiří. Bezpečnost elektrických zařízení: příručka pro konstruktéry.1. vyd. Praha: BEN - technická literatura, 2007. 109 s. ISBN 978-80-7300-222-0

[8] HORST, J.: Informační a telekomunikační technika. Praha, BEN, 2004, 231 s. Terminologický slovník. ISBN 80-7300-127-6

[9] ZÁHLAVA, V., VOBECKÝ, T.: Elektronika - Součástky a obvody, principy a příklady. Praha, Grada, 2006, 220s. ISBN 80-247-1241-5

[10] BASTIAN, P.: Praktická elektrotechnika. Europa – Sobotáles, Brno, 2004, 295 s. ISBN 80-86706-07-9

[11] Interní elektronický zdroj firmy, EUROSAT s.r.o, EZS Duben 2009

[12] Interní elektronický zdroj firmy, KELCOM International, spol. s r.o, EZS 2008

[13] Interní elektronický zdroj firmy, SIEMENS, spol. s r.o, Building Technologies 2009

[14] Interní elektronický zdroj firmy, OLYMPO controls, spol. s r.o. - Security Products

[15] LOVEČEK, Tomáš, NAGY, Peter. Kamerové bezpečnostné systémy. Žilina: EDIS, 2008. 283 s. ISBN 978-80-8070-893-1. (9)

[16] ASSA ABLOY Rychnov, s.r.o Strojnická 633, 516 01 Rychnov nad Kněžnou, FAB c.z. [online]. 2005 [cit. 2010-05-24]. Dostupný z WWW: <http://www.fab.cz/stranky/pyramida-bezpecnosti>.

[17] Google maps.cz. [online].; Dostupný z WWW: <http://maps.google.cz/>.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH ZKRATEK

ACS – Přístupový kontrolní systém – Acces Control Systém

ADSL - Asymetrická digitální účastnická linka - Asymetric Digital Subscriber Line

ATZ - Zapojení 2 nezávislých zón pomocí jedné smyčky - Advanced Technology Zoning

CCD - Zařízení s vázanými náboji - Charge-Coupled Device

CCTV - Uzavřený přenos televizního signálu - Closed circuit TV

CMOS - Doplňující se kov-oxid-polovodič technologie - Complementary Metal – Oxide – Semiconductor

ČSN EN - Česká technická norma přejímající evropskou normu

DCCH - Podpůrný řídící kanál - Dedicated Control Channel

DSP - Digitální signální procesor - Digital Signal Processing

DSS - Digitální pomalá elektronická závěrka - Digital Slow Shutter

DVR – Digitální videorekordér - Digital Video Recording

EEPROM - Elektricky vymazatelná PROM paměť - Electrically Erasable PROM

EZS - Elektronické zabezpečovací systémy – Electronic Security System

EPS - Elektronické požární signalizace – Fire Alarm System

FUP - Sledování vytěžování internetu - Fair User Policy

GPS - Globální triangulační systém - Global Position Systém

GPRS - Obecná paketová rádiová služba - General Packet Radio Service

GSM - Globální systém pro mobilní komunikaci - Global System for Mobile communications

IP protokol – Protokol internetu - Internet Protocol

MW detektor – Mikrovlnný detektor- Micro Wave Detector

LAN - Lokální síť (počítačová) Local Area Network

LCD - Displej z tekutých krystalů - Liquid Crystal Display

LED - Světlo emitující dioda - Light Emitting Diode

NBÚ - Národní Bezpečnostní Úřad

PCO - Pult centrální ochrany

PIR detektor - Pasivní infračervený detektor - Passive Infrared Detector

PKB – Průmysl komerční bezpečnosti

VGA - Grafické videopole - Video Graphics Array

VHS - Systém domácího videa - Video Home Systém

VRC – Videorekordér - Video Cassette Recorder

WiFi – Lokální bezdrátové sítě - Wireless LAN

SEZNAM PŘÍLOH

PŘÍLOHA P I: FOTODOKUMENTACE

PI. 1 Východní vstup do areálu

PI. 2 Kanceláře firmy a výložník pro umístění kamer

PI. 3 Umístění infrazávory u východní vstupu do areálu

PI. 4 Umístění infrazávory u boční branky

PI. 5 Infrazávora a její upevnění východní strana

PI. 5 Západní vstup do areálu a umístění infrazávory

PI. 6 Západní vstup do areálu a umístění protější infrazávory

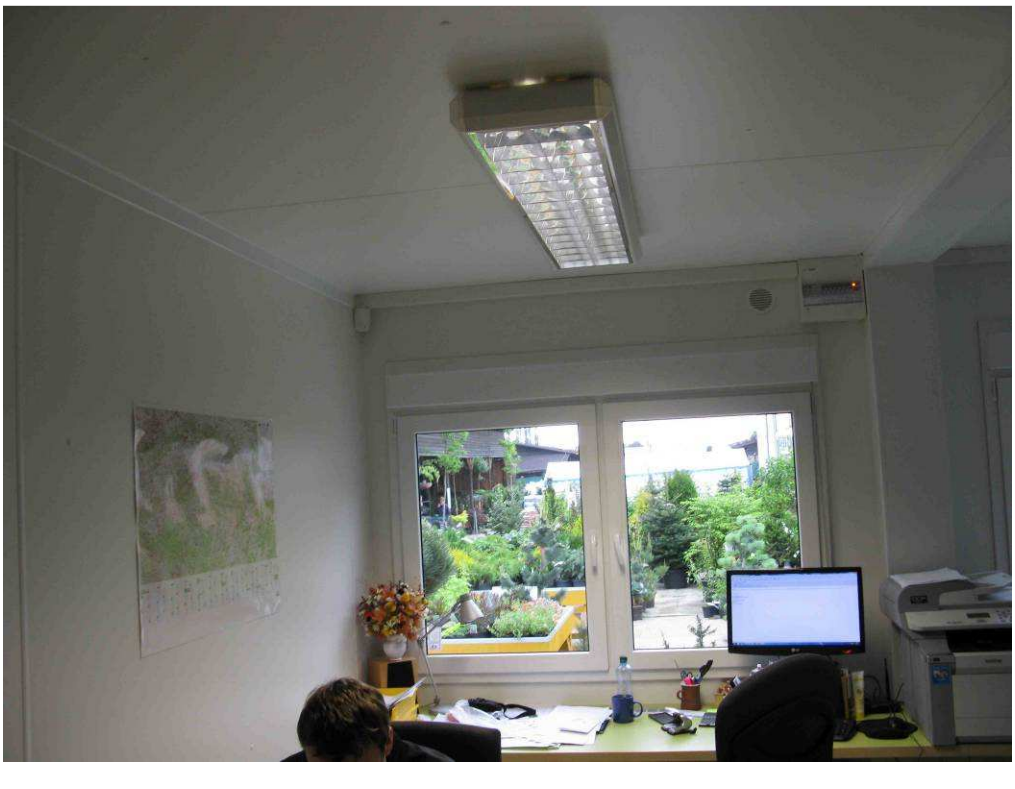
PI. 6 Západní vstup do areálu a detail infrazávory

PI. 7 Ústředna nainstalovaná v kancelářích firmy

PI. 8 Nainstalovaná klávesnice v ochranném krytu na východní straně

PI. 9 Siréna

PI. 10 PIR detektory v kancelářích firmy



PI. 11 Detail PIR detektoru v kancelářích firmy

PI. 12 Prodejní pult s tísňovým tlačítkem

PŘÍLOHA PII: VZOROVÁ SMLOUVA O NAPOJENÍ NA PCO

Smlouva o dílo č. 0000

o připojení elektrické zabezpečovací signalizace na pult centrální ochrany a monitorování objektu

---

Zhotovitel:	**System plus Zlín, s.r.o.**
sídlo firmy:	Kelníky xx, 763 07 Velký Ořechov
provozovna:	Pod xxxxxx 4260, 760 01 Zlín
zastoupený:	Zdeňkem xxxxxxxxx – jednatelem
IČO:	xxxxxxxxx
DIČ:	xxxxxxxxx
společnost je zapsaná u:	KOS v Brně, oddíl C, vložka xxxx

Objednatel:	……
sídlo firmy:	……
zastoupený:	……
IČO:	……
DIČ:	……
společnost je zapsaná u:	……
e-mail pro fakturaci:	……

Pro objekt:

název objektu:	……
adresa objektu:	……
tel. spojení do objektu:	……
e-mail:	……

Dodavatel EZS /tel. kontakt	System plus Zlín, s.r.o. / xxx xxx xxx
Servis a pravidelné revize zajištěné dodavatelem EZS:	ano ~~ne~~

---

1. Předmět smlouvy:

1.1 Předmětem této smlouvy je závazek zhotovitele poskytovat ochranu objektu objednatele napojením elektrické zabezpečovací signalizace (dále jen EZS) na pult centralizované ochrany (dále jen PCO) zhotovitele.

1.2 Zhotovitel poskytuje ochranu objektu objednatele na základě poplachového signálu z EZS objednatele přeneseného do systému PCO zhotovitele:

a) Okamžitým výjezdem zásahové jednotky do objektu objednatele s cílem odvrátit nebezpečí a zabránit škodám, a to v nejkratším čase od obdržení poplachového signálu, pokud nenastanou nepředvídatelné okolnosti.

b) Kontrolou objektu a provedením nezbytných opatření k zajištění bezpečnosti objektu při jeho narušení, zejména vnějším střežením objektu do příjezdu policejních orgánů a obnovení činnosti EZS, pokud objednatel nevydá jiný pokyn.

c) Okamžitým oznámením zjištěného stavu příslušným orgánům, jestliže nelze vlastním přičiněním nebo úsilím zabránit škodě, nebo je podezření, že narušením objektu byl spáchán trestný čin nebo přestupek.

d) Vyrozuměním objednatele nebo jím pověřené osoby.

1.3 Předmětem této smlouvy není, a za neplnění této smlouvy se nepovažuje, jestliže pracovníci zásahové jednotky přes vynaložené úsilí nedopadnou narušitele objektu.

2. Další ujednání:

Objednatel splní následující podmínky pro připojení na PCO:

2.1 Objekt bude vybaven zařízením EZS s ústřednou schopnou komunikace:

a) pomocí metalické telefonní linky nebo

b) pomocí dodaného zařízení zhotovitele (vysílač NAM, komunikátor GPRS-SMS, ethernet komunikátor)

2.2 EZS bude v objektu objednatele instalována oprávněnou fyzickou či právnickou osobou. Systém EZS musí splňovat ČSN 33 4590, resp. ČSN EN 50 131 a komponenty EZS budou mít platný atest pro minimálně stupeň zabezpečení 2 - nízké až střední riziko dle ČSN EN 50131-1.

2.3 Obsluha EZS v objektu bude prováděna osobami, které byly prokazatelně seznámeny s činností a obsluhou.

2.4 Objekt bude (dle charakteru) vybaven potřebnými mechanickými zábranami proti vloupání.

2.5 Objednatel bude neprodleně informovat o nových skutečnostech, které mají vliv pro připojení na PCO, zavazuje se aktualizovat kontaktní osoby pro vyrozumění v případě narušení objektu.

2.6 Objednavatel tímto prohlašuje, že je oprávněn nakládat se střeženým předmětem ostrahy (objektem) z titulu vlastnictví či nájemní smlouvy, a že tento předmět ostrahy je samostatně pojištěn smlouvou proti škodám na majetku v souvislosti s krádeží vloupáním.

3. Cena a platební podmínky

3.1 Cena:

Za připojení na PCO:	-----,- Kč + DPH
Za technické zabezpečení přenosu:	-----,- Kč + DPH / měsíc
Za použití tísňového tlačítka (napadení osob)	-----,- Kč + DPH / měsíc
Za pravidelné zasílání výpisu historie EZS e-mailem	-----,- Kč + DPH
Za střežení objektu dle bodu 4.8. a nad rámec uvedený v bodě 4.3 této sml.	-----,- Kč + DPH / 1hod.

3.2 Paušální čili opakované platby za technické zabezpečení přenosu budou prováděny na základě vystavené faktury se splatností 10 dní na účet banky HVB ve Zlíně, č.ú. XXXXXXX/XX00, variabilní symbol je číslo faktury. Faktury budou vystavovány čtvrtletně dopředu tj. za I. čtvrtletí 1. 1., za II. čtvrtletí 1. 4., III. čtvrtletí 1. 7., IV. čtvrtletí 1. 10. Tento den bude považován za datum uskutečnění zdanitelného plnění. Vystavení faktury bude provedeno během prvních 15 dní příslušného měsíce, který připadá jako první měsíc čtvrtletí.

3.3 Cena je uvedena bez DPH, daň bude vypočtena při fakturaci dle zákona o DPH. Objednatel se zavazuje uhradit cenu za provedené služby do 10 kalendářních dnů ode dne doručení faktury.

4. Zhotovitel se zavazuje:

4.1 Zajistit bezprostředně po přijetí poplachového signálu fyzické prověření příčin vyslání signálu a zabránění vzniku následných majetkových a jiných škod. Zásah bude proveden profesionálními pracovníky s cílem co nejrychlejšího dosažení objektu objednatele tak, aby bylo v co největší míře zabráněno vzniku následných majetkových a jiných škod.

4.2 Na místě zásahu jsou pracovníci zhotovitele povinni se přesvědčit o příčině signálu. V případě skutečného napadení postupovat neprodleně tak, aby bylo zabráněno vzniku následných majetkových a jiných škod, uvědomit Policii ČR nebo městskou policii a zástupce objednatele, popř. zajistit pachatele, který škodu způsobil. Při těchto činnostech se řídí pracovníci obecně závaznými předpisy, především pak ustanovením §13 a §14 tr.zákona, aj. zákonných ustanovení, dotýkajících se ochrany majetku a zdraví osob.

4.3 Pokud nebude nutný okamžitý zásah, zhotovitel se zavazuje, že bude vstup a zásahy do vnitřních prostor objektu objednatele provádět pouze v přítomnosti osob, jež jsou uvedeny jako oprávnění zástupci objednatele (kontaktní osoby). Pokud se do 30 min odpovědná osoba nedostaví, povinnost ve smyslu tohoto bodu pomíjí.

4.4 Poskytovat odbornou pomoc a informace ke zvýšení účinnosti ochrany objektů.

4.5 K přísné mlčenlivosti o všech skutečnostech, se kterými se seznámí v souvislosti s plněním ustanovení této smlouvy i po skončení smluvního vztahu.

4.6 Spolupracovat při připojení na PCO a testování spolehlivosti EZS prováděném instalační firmou.

4.7 V případě vzniku škody zaviněné zhotovitelem, bude tato řešena v návaznosti na jeho pojistnou smlouvu a odpovědnosti za způsobené škody.

4.8 V případě potřeby zajistit fyzické střežení objektu, pokud by to situace vyžadovala.

5. Společná ujednání:

5.1 V případě, že nebude provedena platba za plnění dle předmětu této smlouvy ve stanoveném termínu a dohodnuté výši, má zhotovitel právo objednatele z PCO bez prodlení odpojit. O odpojení bude zhotovitel objednatele informovat.

5.2 Zhotovitel není odpovědný za neplnění činností obsažené v bodě 1. Předmět smlouvy v případě, kdy objednatel nemá poskytnuty funkční služby: přenos tel. linkou, přenosy GPRS -SMS, přenos internetem.

5.3 Smlouva se uzavírá na dobu neurčitou. Každá ze smluvních stran ji může vypovědět bez uvedení důvodů doporučeným dopisem s tříměsíční výpovědní lhůtou. Výpovědní lhůta začíná běžet od prvního dne měsíce následujícího po doručení výpovědi. Doplňky nebo změny této smlouvy je třeba společně projednat a realizovat písemnou formou jako doplněk smlouvy.

5.4 Obě smluvní strany souhlasí s tím, že mohou být druhou stranou prezentovány ve firemní dokumentaci, kde budou uvedeny jen všeobecné informace a vzájemně se tímto obě smluvní strany nebudou poškozovat.

5.5 Smlouva je vyhotovena ve dvou výtiscích uložených u objednatele 1ks a u zhotovitele 1ks.

5.6 Smlouva nabývá platnosti dnem podpisu oprávněných zástupců obou smluvních stran.

5.7 Při přerušení telefonní linky, zrušení služby GPRS-SMS u mobilního operátora, zrušení služby u provozovatele internetu, nedobití kreditu SIM karty nelze zařízení EZS považovat za funkční a monitorovat na PCO.

5.8 Výše úhrady za nedůvodný opakovaný výjezd se stanovuje na **xxx,- Kč + DPH** (při nedbalém zabezpečení objektu, včasným neodvoláním poplachu nebo nedůvodného vyslání signálu z tlačítka „Tíseň“).

Ve Zlíně dne ……..

……

……

zhotovitel objednatel

PŘÍLOHA PIII: VÝKRESOVÁ DOKUMENTACE - PŮDORYS