VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

# NÁVRH A ANALÝZA SYSTÉMŮ POKROČILÉHO ZABEZPEČENÍ A STŘEŽENÍ OBJEKTŮ A PROSTOR

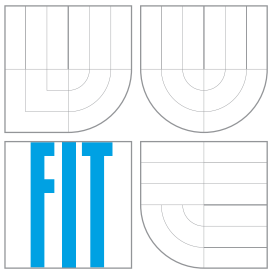
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. PETR KOMÍNEK

BRNO 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

# NÁVRH A ANALÝZA SYSTÉMŮ POKROČILÉHO ZABEZPEČENÍ A STŘEŽENÍ OBJEKTŮ A PROSTOR

DESIGN AND ANALYSIS OF SYSTEMS FOR ADVANCED GUARDING AND SECURING OBJECTS AND AREAS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. PETR KOMÍNEK
AUTHOR

VEDOUCÍ PRÁCE — Ing. JOSEF STRNADEL, Ph.D.
SUPERVISOR

BRNO 2011

*Zadání diplomové práce/10559/2010/xkomin04*

**Vysoké učení technické v Brně - Fakulta informačních technologií**

Ústav počítačových systémů Akademický rok 2010/2011

# Zadání diplomové práce

Řešitel: **Komínek Petr, Bc.**
Obor: Počítačové systémy a sítě
Téma: **Návrh a analýza systémů pokročilého zabezpečení a střežení objektů a prostor**
**Design and Analysis of Systems for Advanced Guarding and Securing Objects and Areas**
Kategorie: Vestavěné systémy

Pokyny:

1. Zdokumentujte předpisy, prostředky a postupy související s konstrukcí systémů pro zabezpečení a střežení objektů a prostor (SZSOP) obsahujících pokročilé prvky (např. docházkový podsystém, autonomní sledování pohybu, přístup přes webové rozhraní).
2. Po dohodě s vedoucím zvolte konkrétní SZSOP, na němž budete diskutovat a demonstrovat celý vývojový cyklus díla z kategorie SZSOP obsahujícího pokročilé prvky. Vytvořte detailní slovní specifikaci zvoleného SZSOP.
3. Navrhněte blokové schéma SZSOP specifikovaného v bodu 2 a zvolte prostředky k jeho realizaci. Po dohodě s vedoucím zvolte části SZOP, které budete realizovat.
4. Proveďte realizaci a demonstrujte její funkčnost v souladu se specifikací.
5. Navržené řešení analyzujte a diskutujte zejména z pohledu dostupnosti služeb, bezpečnosti, spolehlivosti a cenové náročnosti.
6. Navrhněte možné směry rozšíření Vašeho řešení.

Literatura:

- Dle pokynů vedoucího.

Při obhajobě semestrální části diplomového projektu je požadováno:

- Splnění bodů 1 až 3 zadání.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci ročníkového a semestrálního projektu (30 až 40% celkového rozsahu technické zprávy).

Student odevzdává v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Strnadel Josef, Ing., Ph.D.**, UPSY FIT VUT
Datum zadání: 20. září 2010
Datum odevzdání: 25. května 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav počítačových systémů a sítí
612 66 Brno, Božetěchova 2

L.S.

doc. Ing. Zdeněk Kotásek, CSc.
*vedoucí ústavu*

# Abstrakt

Tato diplomová práce se zabývá návrhem, realizací a analýzou systémů pro zabezpečení a střežení objektů a prostor (SZSOP) obsahujících pokročilé prvky. Součástí návrhu je elektronický zabezpečovací (EZS), přístupový (ACS), docházkový a kamerový (CCTV) systém s možností automatického sledování pohybujícího se objektu. Ovládání a monitoring jednotlivých podsystémů je možný lokálně i vzdáleně z počítače přes webové rozhraní, nebo pomocí software. Nechybí ani možnost přístupu na kamerový systém z mobilního telefonu. EZS/ACS systém umožňuje navíc ovládání a zasílání informací o jeho stavu formou SMS zpráv. Navržený systém byl kompletně realizován a jeho činnost demonstrována. Realizace je podrobně popsána, včetně ukázek konfigurace jednotlivých komponent. Na závěr je provedena bezpečnostní analýza a naznačen směr dalšího možného vývoje projektu.



# Abstract

This diploma thesis deals with design, realization and analysis of security and surveillance systems for buildings and spaces containing advanced components. One of the main design's parts is dedicated to intruder alarm system, access system, attendance and CCTV systems with the possibility of automatic motion tracking. Controlling and monitoring of particular subsystems is possible both locally and remotely from a computer via a web interface or by means of a software. The access to camera system from a mobile phone is also possible. IAS/ACS systems also enable controlling and transferring information about their state via SMS. The designed system was realized completely and its operating was demonstrated. The realization is described in detail including illustration of configuration of particular components. A security analysis and a possible future development of the project is summarized in the conclusion.



# Klíčová slova

návrh a realizace zabezpečovacího systému, analýza bezpečnosti, elektronický zabezpečovací systém, EZS, zabezpečovací ústředna, PIR detektor, GSM modul, přístupový systém, ACS, monitoring docházky, docházkový terminál čtečka karet HID Proximity, CCTV, kamera, digitální záznamové zařízení, DVR, automatické sledování pohybu, webové rozhraní, Inner Range Concept, Pinetron, Metel

# Keywords

design and realization of security systém, safety analysis, Intruder Alarm Systém, IAS, security control panel, PIR sensor, GSM module, access control systém, ACS, attendance monitoring, attendance terminal, HID card Proximity reader, CCTV, camera, digital video recorder, DVR, automatic motion tracking, web interface, Inner Range Concept, Pinetron, Metel

# Citace

Petr Komínek: Návrh a analýza systémů pokročilého
zabezpečení a střežení objektů a prostor, diplomová práce, Brno, FIT VUT v Brně, 2011

# Návrh a analýza systémů pokročilého zabezpečení a střežení objektů a prostor

## Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Josefa Strnadela, Ph.D. Další informace a odborné rady mi poskytli zaměstnanci společnosti Eurosat CS. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Petr Komínek
25. května 2011


## Poděkování

Rád bych poděkoval svému vedoucímu Ing. Josefu Strnadelovi, Ph.D. za jeho vstřícný přístup a ochotu.

# Obsah

# Kapitola 1

# Úvod

Lidé mají odjakživa potřebu chránit si svá území a majetek před různými nežádoucími vlivy. Tím se myslí nejen krádeže a vniknutí neoprávněných osob na soukromá území, ale například i požáry a jiné přírodní živly. K účelům ochrany se používají *zabezpečovací systémy*, které existují v nejrůznějších provedeních a jejich možnosti se neustále zdokonalují. Nezbytnou součástí těchto systémů jsou většinou i *osoby zajišťující fyzickou ostrahu*, mechanické zábranné systémy (ploty, zámky, závory) a *elektronické zabezpečovací systémy (EZS)*.

Tato práce se zabývá rozborem předpisů, prostředků a postupů používaných při návrhu pokročilých zabezpečovacích systémů. Následně jsou popsány všechny základní komponenty z hlediska jejich použití a principů činnosti. Za hlavní část práce lze považovat vytvoření neformální specifikace požadavků na pokročilý zabezpečovací systém, jeho následný návrh a realizaci. Takový systém obsahuje moderní bezpečnostní prvky jako jsou nejnovější zabezpečovací ústředny, barevné kamerové systémy se schopností „vidět“ i po tmě, přístupové systémy a zařízení schopná sledovat pohybující se objekty.

Konkrétní cíle, které si tato práce klade, jsou popsány v kapitole 2. Poté jsou definovány obecné požadavky na systém zabezpečení a střežení objektů a prostor (kapitola 3) následované podrobným popisem jednotlivých dílčích kroků návrhu a realizace (kapitola 4). V kapitole 5 je uveden přehled prvků (EZS, ACS, CCTV a EPS) používaných pro realizaci zabezpečovacího systému. Následuje kapitola 6 s detailní slovní specifikací vybraného SZSOP, jeho blokovým schématem a volbou prostředků pro realizaci. V kapitolách 7 a 8 je proveden návrh a popsány dílčí kroky realizace zabezpečovacího systému. Předposlední kapitola 9 se věnuje analýze navrženého řešení z hlediska bezpečnosti, spolehlivosti, dostupnosti služeb a cenové náročnosti. Dosažené výsledky jsou shrnuty a vyhodnoceny v závěrečné kapitole 10, kde je navíc naznačen směr dalšího možného vývoje projektu a jsou zde zmíněny i náměty na případná další vylepšení.

Diplomová práce volně navazuje na moji bakalářskou práci, která se zabývala návrhem a realizací zabezpečovacího systému pro malý rodinný domek. Diplomová práce z ní nijak nečerpá a je jen jakýmsi jejím volným pokračováním. Jsou zde rozebírány zcela jiné aspekty a požadavky týkající se návrhu zabezpečovacích systémů. Dále jsou popisovány jednotlivé dílčí kroky od návrhu až po realizaci. V praktické části je proveden návrh a realizace zabezpečovacího, přístupového a docházkového systému určeného pro rozsáhlé instalace (tisíce uživatelů). Dále byl navržen a realizován kamerový systém s možností automatického sledování pohybujících se objektů pomocí otočných kamer. Jediným přímým pojítkem mezi bakalářskou a diplomovou prací je jistá společnost, která mi pro realizaci zapůjčila spoustu komponent zabezpečovacích systémů, ke kterým by se jinak prakticky nebylo možné dostat.

# Kapitola 2

# Cíle

Cílem této diplomové práce je *návrh, realizace a analýza systémů pro zabezpečení a střežení objektů a prostor* (SZSOP) obsahujících pokročilé prvky, jako je *docházkový podsystém*, *autonomní sledování pohybu* a *přístup přes webové rozhraní*. Návrh bude proveden pro dvoupodlažní budovu středně velké firmy o třiceti zaměstnancích. Součástí návrhu by měl být *elektronický zabezpečovací systém (EZS)*, *přístupový systém (ACS)*, *monitoring docházky* a *kamerový (CCTV) systém* s možností *automatického sledování pohybujícího se objektu*. Ovládání a sledování stavu jednotlivých dílčích podsystémů bude možné lokálně i vzdáleně z počítače pomocí webového rozhraní či software. Neměla by chybět ani možnost *přístupu na kamerový systém z mobilního telefonu* a zabezpečovací a přístupový systém by měl podporovat *ovládání a zasílání informací o jeho stavu formou SMS zpráv*. Navržený systém by měl být alespoň z části realizován, včetně demonstrace jeho činnosti.

Nejprve tedy budou definovány obecné požadavky na elektronický zabezpečovací systém (EZS) dle aktuálně platných českých norem (kap. 3). Následně bude popsán postup návrhu a realizace SZSOP s podrobným zaměřením se na jednotlivé dílčí kroky (kap. 4). Neměl by chybět ani přehled prvků používaných v jednotlivých podsystémech celkového zabezpečovacího systému. Budou zmíněny zejména komponenty používané pro realizaci systémů EZS, ACS, EPS a CCTV (kap. 5). Následně bude provedena „neformální“ slovní specifikace zvoleného SZSOP a uvedeno jeho blokového schéma (kap. 6).

V souladu se specifikací bude následovat návrh zabezpečovacího systému (kap. 7) a jeho realizace, včetně popisu zapojení a konfigurace jednotlivých komponent (kap. 8). Na závěr bude provedena analýza z pohledu dostupnosti služeb, bezpečnosti, spolehlivosti a cenové náročnosti (kap. 9) a naznačen směr dalšího možného vývoje projektu (kap. 10).

Posledním, tak trochu doplňkovým cílem, je natočení videoprezentací demonstrujících činnost jednotlivých realizovaných podsystémů. Výsledná videa budou dostupná na datovém médiu přiloženém k této diplomové práci.

# Kapitola 3

# Obecné požadavky na SZSOP

V této kapitole jsou definovány obecné pojmy a popsány požadavky kladené na systém pro zabezpečení a střežení objektů a prostor (SZSOP). Jsou zde rovněž zmíněny některé základní předpisy a normy týkající se návrhů a konstrukcí SZSOP. Jako zdroj velkého množství informací posloužil učební text [28].

## 3.1 Integrovaný bezpečnostní systém

Dle [28] je integrovaný bezpečnostní systém (IBS) složen z dílčích prvků, jenž by měly být spolu vzájemně propojeny. Jeho strukturu tvoří zejména:

**Mechanické zábranné systémy** – tvoří překážku při vnikání případného pachatele do chráněných prostor. Důležitý je časový interval potřebný k překonání zábran

$$\Delta t = t_2 - t_1 \qquad [s]$$

kde $t_1$ je čas začátku, $t_2$ dokončení napadání objektu.

**Signalizační zařízení a prostředky pro monitorování** – jejich úkolem je zjišťovat, zda nedošlo k narušení chráněných prostor a v takovém případě předat informace o místě a způsobu napadení do řídícího centra.

**Ostraha objektu** – má k dispozici okamžité informace o napadení objektu. Jejím úkolem je vyhodnotit vzniklý stav a vyvodit z něj takové důsledky, aby došlo k opětovnému uvedení IBS do rovnovážného stavu. Tedy do stavu před napadením.

Integrovaný bezpečnostní systém (IBS) má význam pouze za předpokladu, že jeho reakční doba plně pokryje časový interval, jenž je nutný k překonání všech překážek potenciálním pachatelem.

## 3.2 Zabezpečovací systémy

Zabezpečovací systém je soubor technických (mechanických, elektronických, atd.) a organizačních opatření, jenž mají za úkol zajistit objektu zájmu bezpečnost na požadované úrovni.

Pohlížet na něj lze ze 2 následujících hledisek:

- technické hledisko,
- operační hledisko.

### Technické hledisko

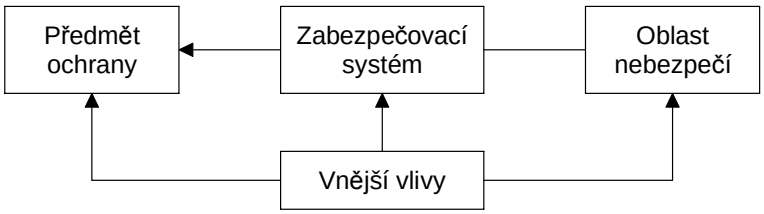
Informace o stavu chráněného objektu se získávají pomocí technických prostředků, takzvaných detektorů (někdy nazývaných čidla). Ty převádějí fyzikální jevy (různé druhy nebezpečí jako např. narušitel v objektu, stoupající hladina vody, požár, atd.) na elektrické signály, jež jsou dále zpracovávány a vyhodnocovány.

### Operační hledisko

Vyjadřuje, „co vše má zabezpečovací systém umět“. Mimo základní požadavky, jako je zamezení odcizení či poškození střežených hodnot, to mohou dále být:

- zdržení případného pachatele a tím vytvoření podmínek pro jeho dopadení,
- vliv zabezpečovacího systému na prevenci (potenciální narušitel si krádež rozmyslí, když uvidí, že je objekt zabezpečen),
- pořízení důkazních materiálů (záznam z kamerového systému, fotografie).

Celý proces poskytování ochrany je graficky znázorněn na následujícím blokovém diagramu:




Obrázek 3.1: Blokové znázornění procesu poskytování ochrany (převzato z [28])

**Předmět ochrany** – je určitá osoba či objekt, jenž má být chráněn před napadením.

**Oblast nebezpečí** – do této kategorie spadají všechna potenciální rizika, která chráněnému objektu hrozí. Patří sem např. vloupání, požáry, živelné pohromy a spousty dalších hrozeb.

**Zabezpečovací systém** – stará se o ochranu *předmětu zájmu* před *oblastí nebezpečí*. Nejčastěji je tvořen kombinací všech základních druhů ochran. Tedy klasické, technické, fyzické a režimové (více viz. kapitola 3.3).

**Vnější vlivy** – mohou nepříznivě ovlivňovat všechny předešlé kategorie. Jedná se zejména o počasí, povětrnostní podmínky, osvětlení, faunu, flóru apod.

Lze tedy říci, že co se operačního hlediska týče, má zabezpečovací systém minimálně tyto vlastnosti a přínosy:

**Preventivní vliv** – už samotná přítomnost zabezpečovacího systému působí psychologicky na případného pachatele a tím ho může odradit od zamýšleného vloupání.

**Detekce** – je zde chápána jako neustálé ověřování charakteristických rysů různých typů ohrožení (vniknutí pachatele, stoupající hladina vody, atd.) ve střeženém prostoru.

**Vyhlášení poplachu** – je signalizace pozitivní detekce (tedy např. signalizace narušení objektu). Mimo řádný poplach rozlišujeme ještě následující 2 druhy:

- *Falešný poplach* – je vyvolaný zejména chybnou funkcí zabezpečovacího systému (např. vlivem vadné součástky). Akceptovatelná hodnota je cca 1 falešný poplach na systém za 2 roky.
- *Planý poplach* – bývá nejčastěji způsoben chybou obsluhy, popřípadě různými rušivými vlivy (např. sálání tepla, pohyb závěsu vlivem průvanu, apod.).

**Reakce zabezpečovacího systému** – v případě ohrožení chráněného zájmu (objektu) může mít různé podoby. Nejčastěji se využívají poplachové sirény, volitelně pak i přenos na pult centralizované ochrany (PCO) [1] a s tím spojené výjezdy zásahových skupin.

**Spolehlivost zabezpečovacího systému** – je míra úspěšnosti při vykonávání požadované činnosti (zabezpečení/střežní) za nastolených podmínek. Zabezpečovací systémy jsou navrhovány tak, aby umožňovaly signalizovat stav, ve kterém se právě nacházejí. Tedy zejména *běžný provoz* a *porucha* (včetně upřesnění části systému které se týká).

**Efektivnost** – zabezpečovacího systému lze hodnotit s přihlédnutím k výsledkům jeho činnosti, přičemž můžeme rozlišovat následující kategorie efektivností:

- *Technická efektivnost* – platí, že současná řešení zabezpečovací techniky jsou relativně jednoduchá a spolehlivá. Tím je zaručena vysoká efektivnost při boji proti trestné činnosti.
- *Provozní efektivnost* – je vyjádřena mírou poruchovostí zabezpečovacího systému a počtem planých poplachů.

## 3.3 Základní druhy ochran

Zabezpečovací systémy bývají v praxi většinou realizovány jako kombinace *základních druhů ochran*. Přičemž musí platit, že takto navržený systém, je jako celek komplexní (obsahuje všechny potřebné druhy ochran) [13].

### Klasická ochrana

Jedná se o nejstarší, od nepaměti používaný, způsob ochrany. K tomuto účelu se používají nejrůznější mechanická zařízení, jako například ploty, zídky, mříže, okna, dveře, zámky apod. Samotné prvky klasické ochrany nejsou postačující ke komplexnímu zabezpečení. Mají pouze za úkol pozdržet případného pachatele (viz. zpožďovací faktor $\Delta t$, kapitola 3.1) a vždy je nutné je kombinovat s dalšími druhy ochran [27].

[1] PCO – Pult Centralizované Ochrany je služba poskytovaná povětšinou soukromými bezpečnostními agenturami zajišťujícími nonstop dohled nad střeženým objektem [2]. V případě narušení může být proveden zásah výjezdovou jednotkou a to mnohdy i v součinnosti s policií.

### Režimová ochrana

Je skupina organizačních opatření a postupů, jež má za cíl minimalizovat dopady trestné činnosti či vandalizmu. Prakticky se jedná o nejrůznější interní postupy a směrnice, jimiž se musí osoby pohybující se v chráněném objektu a jeho okolí řídit.

- *Opatření pro vnitřní prostory* – Pro každého uživatele objektu se jasně vymezí oblasti (místnosti, části budovy), do kterých bude mít umožněn přístup.
- *Opatření pro vnější prostory* – se týkají především vstupních/výstupních cest do/z objektu. Tedy různých bran, koryt potoků, kanalizací apod. Pro všechny tyto cesty je třeba stanovit, zda nimi má být umožněn vstup do objektu či nikoli. Neméně důležitý je i návrh a následné dodržování kontrolních opatření.

### Fyzická ochrana

Provádí ji různí hlídači, vrátní, členové výjezdové jednotky pultu centralizované ochrany apod. Na její kvalitě je do jisté míry závislá účinnost zabezpečovacího systému jako celku. Platí, že fyzická ochrana je ze všech výše zmiňovaných typů ta nejdražší, alespoň co se provozních nákladů týče. Počáteční investice nejsou sice nikterak zásadní (výzbroj, oblečení, výcvik zaměstnanců), ale dále třeba počítat s trvalými výdaji na platy zaměstnanců vykonávajících fyzickou ochranu.

### Technická ochrana

Jedná se o nejspolehlivější a pro potenciálního pachatele nejhůře překonatelný druh ochrany. Provádí rychlou detekci a o případném narušení se tak patřičná skupina lidí (zaměstnanci ostrahy, výjezdová jednotka) dozví prakticky okamžitě. Takto je možné buďto dopadnout pachatele „přímo při činu“, nebo mu alespoň zabránit v dalším protiprávním jednání.

Dlužno podotknout, že technická ochrana slouží výhradně pro doplnění klasické ochrany a ke zvyšování efektivnosti fyzické ochrany [28]. Sama o sobě (bez součinnosti s dalšími zmiňovanými typy) by příliš účinná nebyla.

## 3.4 Dělení technických ochran

Na základě platné normy [4] (ČSN EN 50131-1 ed. 2) se kategorie „technické ochrany“ dále dělí na několik podskupin učených dle následujících hledisek:

- podle prostorového zaměření,
- způsobu předávání poplachových signálů,
- kategorie rizikovosti chráněného objektu,
- stupně zabezpečení chráněného objektu.

### 3.4.1 Hledisko prostorového zaměření

Podle charakteru objektu a prostorového zaměření se technická ochrana sestavuje kombinací některých z těchto prvků (ochran):

**Plášťová ochrana** – má za úkol střežit „plášť“ objektu. Tedy převážně okna, dveře, vrata a jiná potenciální místa pro vniknutí do objektu. Používají se magnetické dveřní kontakty, detektory rozbití skla apod. (více viz. kapitola 5.1.2).

**Prostorová ochrana** – pomocí detektorů pohybu signalizuje narušení definovaných prostor střeženého objektu (viz. kapitola 5.1.3).

**Obvodová ochrana** – slouží k signalizaci narušení obvodu objektu (katastrální hranice). Ta bývá většinou vymezena plotem, zdí, nebo jinou technickou či přírodní bariérou. Patřičné detektory musí být pochopitelně v provedení pro venkovní montáž. Více o tomto pojednává kapitola 5.1.1.

**Předmětová ochrana** – slouží ke hlídání konkrétních předmětů. Nejčastěji má za úkol zabránit neoprávněné manipulaci či odcizení uměleckých děl nebo trezorů.

**Klíčová ochrana** – využívá se v místech, která jsou klíčová pro pohyb osob v objektu. Tedy nejrůznější schodiště, chodby a průchody.

**Sabotážní ochrana** – jednotlivé dílčí komponenty zabezpečovacího systému by měly být schopny samy sebe chránit před neoprávněnými zásahy a manipulací.

**Osobní ochrana** – je ochrana zdraví, či života osob před různým nebezpečím (přepadení).

**Ostatní ochrany** – jejich úkolem je včas detekovat různé události, jako je například živelná katastrofa, či začínající požár a tím pomoci k minimalizaci vzniklých škod.

V praxi je velice žádoucí kombinovat co nejvíce z výše uvedených principů ochran do jednoho funkčního celku. Tedy např. okolí pozemku hlídat venkovními detektory, vstupní dveře magnetickým kontaktem a pohyb osob v objektu pohybovými detektory.

### 3.4.2 Způsoby předávání poplachových signálů

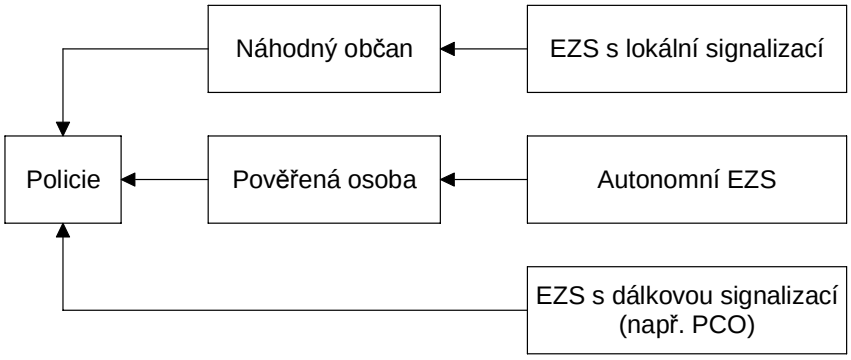
Na základě toho, jakým způsobem *elektronické zabezpečovací systémy* (EZS) předávají informaci o nastalém poplachu, je lze rozdělit na tři následující kategorie:

**EZS s lokální signalizací** – Při narušení střeženého objektu je poplach indikován akustickou, nebo optickou signalizací (případně oběma způsoby současně) přímo v místě instalace EZS. Tím je splněna jak *informační funkce* zabezpečovacího systému, tak *preventivní*. *Informační funkcí* je myšleno, že okolí objektu (např. sousedé) má přehled o skutečnosti, že došlo k narušení a může zareagovat (např. zavolat policii). Běžné sirény totiž produkují pronikavý zvuk o intenzitě okolo 110 dB, což je poměrně velký a ze spánku spolehlivě budící hluk. *Preventivní funkce lokální signalizace* potom spočívá v psychologickém vlivu na pachatele, který většinou z místa činu uteče, aniž by stihl napáchat mnoho škod. V praxi je mnohdy informace o poplachu dále šířena například majiteli objektu, kdy ho zabezpečovací systém upozorní pomocí telefonního komunikátoru či GSM brány. *Lokální poplachová signalizace* se používá při ochraně bytů, chat a menších objektů. Základním předpokladem pro adekvátní reakci okolí na ni je dobře fungující zabezpečovací systém s minimální mírou falešných poplachů.

**EZS s autonomní signalizací** – jsou prakticky totožné se systémy s lokální signalizací. Jediný rozdíl je v tom, že výstup poplachové signalizace je zde navíc napojen na ostrahu, která je neustále přítomna v hlídaném objektu (hlídač, bezpečnostní agentura).

**EZS s dálkovou signalizací** – mají poplachový výstup napojen na smluvního partnera (např. pult centralizované ochrany), jenž zajišťuje stálou službu. V případě narušení objektu se postará o provedení zásahu a zařídí všechny potřebné náležitosti vedoucí k opětovnému zajištění objektu.

Rozdíly mezi výše zmiňovanými způsoby předávání poplachové informace jsou graficky znázorněny na následujícím blokovém diagramu. Důležité je povšimnout si, že v případě *EZS s lokální signalizací* závisí předání informace o poplachu na *náhodném občanovi*, u *autonomních EZS* na *pověřené osobě* a u *EZS s dálkovou signalizací* je to řešeno přímo na úrovni samotného systému.




Obrázek 3.2: Možné způsoby předávání poplachového signálu (převzato z [28])

### 3.4.3 Kategorie rizikovosti chráněného objektu

Pro každý objekt je třeba individuálně posoudit možná bezpečnostní rizika a podle toho pak volit vhodný typ EZS. Zastaralá a již neplatná norma [1] (ČSN 33 4590) dělila ústředny EZS podle míry rizika do čtyř kategorií:

**Kategorie 4 - nízká rizika** – byty, vilky, malé provozovny, obchůdky, garáže, objekty s nízkým objemem chráněných hodnot.

**Kategorie 3 - průměrná rizika** – obchody, sklady, provozovny, obchodní domy.

**Kategorie 2 - vysoká rizika** – peněžní ústavy, velká klenotnictví, prodejny zbraní, galerie, výroba a skladování opiátů, apod.

**Kategorie 1 - nejvyšší rizika** – vybrané státní instituce, centrální úložny, atomové elektrárny, státní pokladny, velkosklady výbušnin.

V současné době se požadovaná úroveň ochrany dle normy [4] (ČSN EN 50131-1 ed. 2) určuje na základě požadavků pojišťoven, případně policie. Posuzování a kategorizaci dílčích komponent systému EZS (ústředna, detektory) provádí nezávislá akreditovaná zkušebna. U nás jsou to např. Národní bezpečnostní úřad (NBÚ), TestAlarm Praha a Ministerstvo obrany. Ti také vydají příslušná osvědčení a certifikáty. Platí, že všechny prvky systému EZS musí být zařazeny do minimálně stejné bezpečnostní kategorie, jakou má mít systém jako celek. Při montáži je třeba dodržet podmínky, pro něž byly komponenty certifikovány.

### 3.4.4 Stupeň zabezpečení chráněného objektu

Již zmiňovaná stará norma ČSN 33 4590 stanovovala *stupeň zabezpečení* na základě druhu objektu a dle výše uchovávaných hodnot a pravděpodobnosti napadení. V aktuálně platné české verzi evropské normy ČSN EN 50131-1 ed. 2 je *stupeň zabezpečení* určen na základě rizika odvozeného od typu objektu, obsaženého majetku a znalostí a technického vybavení potenciálních narušitelů [4].

Stupeň zabezpečení musí být stanoven pro každý navrhovaný elektronický zabezpečovací systém (EZS). Přičemž stupeň 1 odpovídá základnímu zabezpečení, stupeň 4 potom nejvyššímu možnému. Většina objektů spadá do stupně zabezpečení 1 – 2. Stupeň 3 se používá pro objekty typu klenotnictví, banky a budovy obsahující tajné materiály. Nejvyšší stupeň 4 zahrnuje vyjímečné objekty jako např. jaderné reaktory a muniční sklady. Přesná kritéria pro určování stupně zabezpečení chráněných objektů shrnuje následující tabulka.

| **Stupeň zabezpečení** | **Míra rizika** | **Typ narušitele, potřebné znalosti a vybavení** |
|---|---|---|
| 1 | Nízké | Předpokládá se, že narušitelé mají malou znalost EZS a že mají k dispozici omezený sortiment snadno dostupných nástrojů. |
| 2 | Nízké až střední | Předpokládá se, že narušitelé mají určité znalosti o EZS a že použijí základní sortiment nástrojů a přenosných přístrojů (např. multimetr). |
| 3 | Střední až vysoké | Předpokládá se, že narušitelé jsou obeznámeni s EZS a mají úplný sortiment nástrojů a přenosných elektronických zařízení. |
| 4 | Vysoké riziko | 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.<br>Pokud je 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 EZS je určen nejnižším stupněm jeho subsystému. Komponenty, které jsou společné pro více subsystémů musí mít stupeň nejméně stejný jako subsystém nejvyššího stupně. |

Tabulka 3.1: Stupně zabezpečení dle platné normy [4] (ČSN EN 50131-1 ed. 2)

## 3.5 Elektronický zabezpečovací systém (EZS)

*Elektronický zabezpečovací systém (EZS)*, respektive přesněji dle nové normy ČSN EN 50131-1 ed. 2 již *poplachový zabezpečovací systém (PZS)* je skupina elektronických komponent, jež jsou jako celek schopné akusticky a/nebo opticky signalizovat narušení střeženého objektu. Za narušitele je považována každá osoba, která do objektu vstupuje neoprávněně.

Nejčastěji je EZS složen z níže uvedených základních prvků, z nichž každý plní přesně specifikované funkce:

**Detektory (čidla)** – reagují na fyzikální změny bezprostředně související s narušením objektu (otevření dveří, rozbití okna, pohyb pachatele) a převádí je na elektrické signály. Detektorům se věnuje kapitola 5.1.

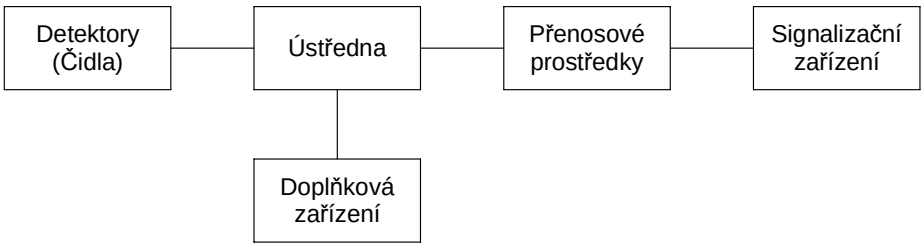
**Ústředna** – tvoří „mozek“ celého zabezpečovacího systému. Neustále přijímá informace z detektorů a ty dále vyhodnocuje. V případě narušení objektu zajistí příslušnou reakci systému (akustická signalizace sirénou, přenos na PCO). Podrobně o ústřednách EZS pojednává kapitola 5.1.5.

**Přenosové prostředky** – umožňují přenos informací z ústředny do místa, kde probíhá signalizace. Tedy nejčastěji do poplachové sirény či na PCO.

**Signalizační zařízení** – při vyhlášení poplachu tuto informaci převede na akustický a často zároveň i optický (blikání majáčku zpravidla oranžové barvy) signál.

**Doplňková zařízení** – slouží pro ovládání zabezpečovacího systému nebo k jeho rozšíření o nejrůznější funkce. Patří sem např. ovládací klávesnice či GSM brány zajišťující komunikaci s PCO, nebo s majitelem objektu přes mobilní síť.

Způsob propojení jednotlivých dílčích prvků tvořících elektronický zabezpečovací systém (EZS) je patrný z následujícího obrázku.




Obrázek 3.3: Blokové schéma elektronického zabezpečovacího systému (převzato z [28])

## 3.6 Přehled platných norem pro poplachové systémy

Parametry a podmínky montáže zabezpečovacích zařízení jsou jasně definovány a normalizovány evropskými normalizačními organizacemi. Konkrétně organizací *CEN – European Committee for Standardization (Evropský výbor pro normalizaci)* a *CENELEC – European Committee for Electrotechnical Standardization (Evropský výbor pro elektrotechnickou normalizaci)*. České verze (doslovný překlad) těchto evropských norem mají status českých technických norem a zahrnují především následující problematiku [4]:

- požadavky na funkčnost jednotlivých komponent poplachových systémů,
- požadavky na odolnost jednotlivých komponent proti povětrnostním vlivům,
- metody testování miry splnění všech požadavků,
- zásady montáže a používání poplachových systémů,
- návody a doporučení ohledně správné činnosti poplachových systémů.

České normy zabývající se poplachovými systémy jsou členěny následovně [12]:

**ČSN EN 50130-x** – tato skupina norem definuje všeobecné požadavky na poplachové systémy. Jsou to např. metody zkoušek vlivu prostředí, elektromagnetická kompatibilita, požadavky na odolnost komponent požárních systémů, zabezpečovacích systémů a systémů přivolání pomoci.

**ČSN EN 50131-x** – Poplachové zabezpečovací a tísňové systémy (PZTS), dříve nazývané elektronické zabezpečovací systémy (EZS, popř. Intruder Alarm System (IAS).

- ČSN EN 50131-1 ed.2 – Systémové požadavky,
- ČSN EN 50131-2 – Detektory,
- ČSN EN 50131-3 – Ústředny,
- ČSN EN 50131-4 – Výstražná zařízení,
- ČSN EN 50131-5-3 – Požadavky na zařízení využívající bezdrátové propojení,
- ČSN EN 50131-6 – Napájecí zdroje,
- ČSN EN 50131-7 – Pokyny pro aplikace,
- ČSN EN 50131-8 – Zamlžovací bezpečnostní zařízení/systémy.

**ČSN EN 50132-x** – systémy uzavřených televizních okruhů (CCTV – Closed Circuit Television). Tedy lokální kamerové systémy včetně záznamových zařízení. Patří sem například:

- ČSN EN 50132-1 – Systémové požadavky,
- ČSN EN 50132-2-1 – Černobílé kamery,
- ČSN EN 50132-4-1 – Černobílé monitory,
- ČSN EN 50132-5 – Přenos videosignálu,
- ČSN EN 50132-7 – Pokyny pro aplikaci.

**ČSN EN 50133-x** – systémy kontroly a řízení vstupu (ACS – Access Control System). Kontrola a evidence vstupu a docházky, zamezení přístupu neoprávněným osobám.

**ČSN EN 50134-x** – systémy přivolání pomoci (SAS – Social Alarm Systems). Poskytují prostředky k přivolání pomoci ohroženým osobám.

**ČSN EN 50135-x** – systémy tísňové (HUAS – Hold-Up Alarm Systems). Obsluha může kdykoli vyvolat poplach, (např. v případě přepadení).

**ČSN EN 50136-x** – přenosová zařízení (ATS – Alarm Transmission Systems). Zajišťují přenos poplachových stavů do monitorovacího centra (např. na PCO).

**ČSN EN 50137-x** – systémy kombinované nebo integrované (IAS). Poplachové systémy, jež jsou kombinací několika předchozích jednoúčelových systémů.

**ČSN EN 54-x** – elektrická požární signalizace (EPS – Electronic Fire System). Slouží ke včasnému rozeznání příznaků začínajícího požáru, k signalizaci tohoto stavu s k aktivaci požárně-bezpečnostních zařízení (např. odemčení nouzových východů).

# Kapitola 4

# Postup návrhu SZSOP

Účelem projektování zabezpečovacích systémů je návrh komplexního systému zajišťujícího ochranu daného objektu před různými negativními vlivy. Těmi se myslí zejména vniknutí neoprávněné osoby, krádeže, vandalství, ale i požár či povodeň.

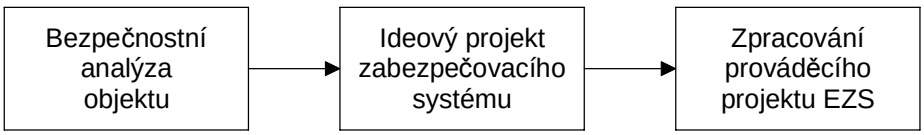
Tato kapitola si klade za cíl popsat kritéria a možná úskalí návrhů takových systémů. Stejně jako v jiných oborech i zde platí, že čím kvalitněji se provede samotný návrh, tím méně komplikací lze očekávat při následné realizaci. Mnohé informace zde obsažené jsou čerpány z učebního textu [28] a diplomové práce [17].

## 4.1 Subjekty podílející se na projektování SZSOP

Nejprve je třeba si ujasnit role jednotlivých subjektů figurujících v procesu návrhu a projektování.

**Zadavatel** – stanovuje požadavky na projektovaný zabezpečovací systém. Účastní se počátečních fází realizace a i později po dobu užívání systému zprostředkovává řešiteli zpětnou vazbu.

**Řešitel** – navrhuje a projektuje zabezpečovací systém a zodpovídá za dodržení zadavatelem určených podmínek a příslušných norem. Po celou dobu návrhu spolupracuje se zadavatelem a do projektu pak přidává případné změny. Před samotným návrhem musí projektant určit vhodnou koncepci systému, a to na základě typu chráněného objektu, hodnoty majetku a míry rizika vniknutí pachatele. Celý postup při návrhu je graficky znázorněn na obrázku 4.1.

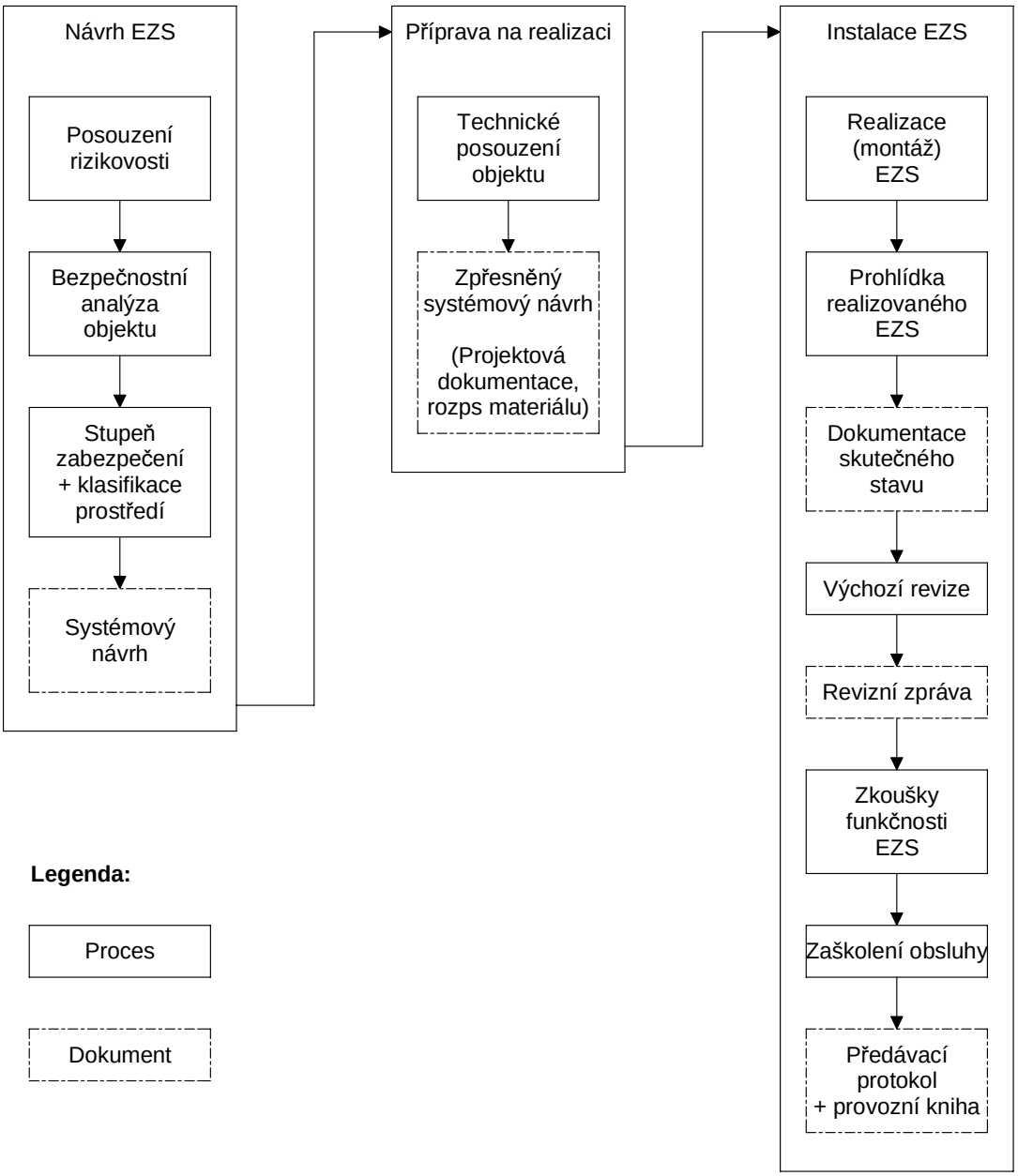



Obrázek 4.1: Postup při návrhu zabezpečovacího systému (převzato z [28])

**Provozovatel** – nese hlavní zodpovědnost za provoz a pravidelnou údržbu (odstranění pavučin z detektorů, kontrola stavu akumulátoru, atd.) realizovaného zabezpečovacího systému. Četnost a rozsah činnosti je smluvně dohodnutá s uživatelem. U menších objektů je často provozovatelem systému samotný uživatel.

## 4.2 Návrh SZSOP

Proces návrhu a realizace elektronického zabezpečovacího systému je ovlivněn mnoha faktory, z nichž nejvýznamnější jsou požadavky zadavatele a plánovaná cena. Sled kroků vedoucích od návrhu k funkčnímu zabezpečovacímu systému je znázorněn na obrázku 4.2.




Obrázek 4.2: Celkový proces návrhu a realizace SZSOP (převzato z [17])

Na počátku samotného návrhu se provádí posouzení rizikovosti objektu (zařazení do příslušné kategorie) a určení požadovaného stupně zabezpečení. Tato problematika byla již popsána v kapitolách 3.4.3 a 3.4.4. Následuje vysvětlení dalších dílčích kroků z procesu návrhu a realizace zabezpečovacího systému.

### 4.2.1 Bezpečnostní analýza objektu

Bezpečnostní analýza objektu slouží jako jeden z hlavních podkladů pro vypracování projektu zabezpečovacího systému. Určuje, co se bude chránit (předmět zájmu), jakým způsobem a pomocí jakých prostředků.

Vzhledem k tomu, že zabezpečovací systémy jsou sestaveny z prvků klasické, technické, režimové a fyzické ochrany (viz kapitola 3.3), bývají součástí bezpečnostní analýzy i jiné speciální studie. Jsou to například analýzy ekonomické, protipožární, ochrany utajovaných skutečností, ochrany osobních údajů a jiné.

Z hlediska elektronických zabezpečovacích systémů (EZS) jsou důležité zejména tyto položky [28]:

- popis chráněného objektu a prověření lokality,
- režimová studie objektu,
- přizpůsobení projektu EZS režimu ostrahy objektu,
- seznam a popis možných nebezpečí,
- analýza potenciálních způsobů napadení objektu.

#### Popis chráněného objektu a prověření lokality

O zabezpečovaném objektu je velice důležité získat co nejvíce informací. Důležité je zaměřit se na zhodnocení stavu klasické ochrany, srovnání stavební dokumentace s realitou a popis charakteru objektu a jeho okolí. Zajímavé je rovněž nahlédnout do statistiky vloupání či krádeží v daném regionu a v případě, že v daném objektu již došlo ke vloupání, se zaměřit i na způsob, jakým bylo provedeno.

Následně se stanoví potřebný stupeň zabezpečení (viz kapitola 3.4.4). Posuzuje se zejména konstrukce pláště budovy (zdi, zídky) a jeho otevíratelných částí (dveře, okna), poloha objektu (městská zástavba, samota u lesa) a počet a typ lidí (uklízečka, technik), jenž mají do objektu přístup. Velice vhodné je prozkoumat i vnitřní a vnější vlivy, které by mohly negativně působit na komponenty navrhovaného EZS. Vnitřními se myslí elektromagnetická rušení, přítomnost domácích zvířat, nebo průvanu. Vnějšími potom mohou být různá vysokofrekvenční rušení (dráty vysokého napětí) nebo vibrace (těžké stroje).

#### Režimová studie objektu

Pohyb osob v objektu se řídí jeho režimem. Je velký rozdíl mezi rodinným domkem s pěti stálými uživateli, kteří jsou přes den mimo objekt a tovární halou se třísměnným provozem. Platí tedy, že režim ovládání EZS se nutně musí přizpůsobit režimu objektu. Rozlišujeme [13]:

**Režim vyzývaný** – EZS je zapnut pověřenou osobou (pracovník ostrahy) na základě požadavku odcházejícího zaměstnance. Takže například pracovník skladu při svém odchodu pověřené osobě sdělí tuto skutečnost a ta poté zajistí zapnutí příslušné smyčky EZS. Zodpovědnost za správný provoz EZS má v tomto případě pracovník ostrahy.

**Režim časový** – k zapnutí či vypnutí příslušné smyčky EZS dojde na ústředně v předem stanovený čas. Tedy například 30 minut po skončení pracovní doby dojde k automatickému zastřežení a 30 minut před jejím začátkem k odstřežení. Tento způsob lze použít jen u objektů, kde je pracovní doba zaměstnanců stálá. Nevýhodou je, že případný přesčas se musí hlásit předem a pověřená osoba musí poté zajistit příslušný zásah do systému. Přístup mimo pracovní dobu a bez vědomí pověřené osoby (vrátného) není v takovém případě možný vůbec.

**Režim vázaný nebo odvozený** – zapínání a vypínání EZS je prováděno při odevzdání klíčů či načtení osobní karty čtečkou. Vhodné je například svazky klíčů označit stejným číslem, jako je číslo příslušné smyčky. Výhodou tohoto řešení je jednoznačnost v zodpovědnosti. Pokud zaměstnanec odevzdal klíče a systém přesto nebyl zapnut, padá veškerá vina na strážného, protože danou smyčku nezapnul.

**Režim autonomní** – jednotlivé smyčky EZS jsou zapínány samostatně dle potřeby přímo samotnými uživateli. Výhodou je, že není třeba dalšího zaměstnance jako v předchozích případech. Nevýhodou pak potenciální prostor pro lajdáctví uživatelů (zaměstnanci jsou líní na noc zapínat EZS aby ho nemuseli ráno zase vypínat).

**Režim úklidu v objektu** – je důležitý režim, při němž je v objektu přítomen úklidový personál. V tuto chvíli je hodně smyček EZS vypnutých a objekt je tak poměrně zranitelný. Z toho důvodu je vhodné úklid pokud možno provádět v pracovní době, případně zajistit přítomnost ostrahy.

### Přizpůsobení projektu EZS režimu ostrahy objektu

Role fyzické ochrany a elektronického zabezpečovacího systému je třeba jasně vymezit. Buďto musí být EZS navrhnut tak, aby byl v souladu s režimem objektu, případně je třeba režim objektu přizpůsobit nárokům zabezpečovacího zařízení.

V některých objektech má ostraha za úkol vykonávat tzv. obchůzkovou strážní službu. To znamená, že musí v přesně definovaných časových intervalech obejít určená místa objektu a svoji přítomnost potvrdit například zadáním kódu. I takovým požadavkům by měl být EZS v případě potřeby přizpůsoben.

### Seznam a popis možných nebezpečí

Při projektování zabezpečovacího systému musí být jasně definováno, před jakými zdroji nebezpečí je třeba předmět ochrany (objekt) chránit.

Existují dva typy nebezpečí, vnější a vnitřní. Vnějším se myslí například vniknutí pachatele do objektu. Vnitřním pak rozkrádání majetku, vynášení utajovaných skutečností, sabotáž, či nedbalostní jednání (zavinění požáru).

### Analýza potenciálních způsobů napadení objektu

Seznam možných nebezpečí slouží jako podklad pro analýzu předpokládaných způsobů napadení objektu. Účelem této analýzy je nalezení všech potenciálně zranitelných míst.

Z hlediska vnějšího nebezpečí to mohou být například málo odolné dveře, nízko umístěná okna, nebo snadno přístupné větrací šachty. Z pohledu vnitřních nebezpečí pak špatně zabezpečený sklad nebo místnost s tajnými materiály.

### 4.2.2 Klasifikace prostředí

Při výběru komponent zabezpečovacího systému je nutno brát ohled na prostředí, ve kterém budou použity. Třídu prostředí pro jednotlivé součásti EZS stanoví výrobce. Platí, že zařízení vyšší třídy může být použito v aplikaci nižší třídy. Naopak to z pochopitelných důvodů není přípustné.

| Třída | Název prostředí | Popis prostředí, příklady | Rozsah teplot |
|---|---|---|---|
| I. | Vnitřní | Vytápěná obytná nebo obchodní místa. | + 5 °C až +40 °C |
| II. | Vnitřní všeobecné | Přerušovaně vytápěná nebo nevytápěná místa. | −10 °C až +40 °C |
| III. | Venkovní chráněné | Prostředí vně budov, kde komponenty nejsou trvale vystaveny vlivům počasí (přístřešky). | −25 °C až +50 °C |
| IV. | Venkovní všeobecné | Prostředí vně budov, kde komponenty jsou trvale vystaveny vlivům počasí. | −25 °C až +60 °C |

Tabulka 4.1: Klasifikace prostředí dle normy [4] (ČSN EN 50131-1 ed. 2)

### 4.2.3 Systémový návrh

Proces návrhu zabezpečovacího systému je završen vytvořením dokumentu zvaného *systémový návrh*, který dále slouží jako podklad pro následnou realizaci. Zadavateli je předložena prvotní nabídka a získává tak alespoň rámcovou představu o celkové ceně systému.

Při přípravě a následné realizaci instalace mnohdy dochází ke zpřesňování jednotlivých bodů systémového návrhu. Ten by měl obsahovat alespoň následující položky [17]:

- identifikační údaje o zadavateli,
- údaje o objektu pro nějž je návrh EZS vytvářen,
- požadovaný stupeň zabezpečení,
- určení třídy okolního prostředí,
- seznam a přibližná cena použitého materiálu (odhad),
- legislativa (prvky EZS musí splňovat požadavky národní legislativy),
- typ a umístění poplachových signalizačních zařízení (sirény),
- údaje o nastavení parametrů ústředny,
- informace o certifikaci jednotlivých komponent EZS,
- plánovaná odezva na vyhlášení poplachu (kdo a za jakou dobu může zasáhnout),
- interval servisních prací a revizí,
- kontaktní údaje na servisní firmu.

## 4.3 Fáze přípravy na realizaci EZS

Příprava na realizaci zabezpečovacího systému vychází hlavně ze systémového návrhu, který je nadále zpřesňován a rozšiřován až do podoby umožňující provedení instalace. Jednoznačně se určí konkrétní typ ústředny a ostatních komponent systému. Následně se provede upřesnění finanční analýzy.

### 4.3.1 Technické posouzení objektu

Na základě technického posouzení objektu se zvolí vhodné komponenty zabezpečovacího systému a určí přesné podmínky jejich montáže (poloha, způsob propojení, apod.).

**Ústředna** – by měla být situována uvnitř střežených prostor tak, aby nebyla veřejně přístupná. V praxi se navíc umisťuje do plechového boxu, který obsahuje mechanický kontakt pro hlídání otevření víka. Tento kontakt se napojí na jeden ze vstupů ústředny a slouží jako tzv. *24 hodinová zóna*. Při otevření boxu s ústřednou neoprávněnou osobou (nezadání hesla na klávesnici) dojde k okamžitému vyhlášení poplachu.

**Klávesnice** – slouží pro uživatelské ovládání zabezpečovacího systému. Vzhledem k požadované funkci EZS, tedy zapnutí při odchodu z objektu a vypnutí při příchodu, se umísťuje do vnitřních prostor, co nejblíže vstupním dveřím (předsíň, chodba).

**Napájecí zdroj** – zabezpečovací zařízení stupně ochrany 1 a 2 je možno napájet pohyblivým přívodem ze zásuvky rozvodné sítě. Zařízení se stupněm ochrany 3 a 4 musí být napájeno ze samostatného nn (nízké napětí – 50 - 1000 V) rozvaděče. Napájecí zdroj musí být dimenzován tak, aby vydržel s rezervou dodávat potřebný proud při běžném i poplachovém stavu.

**Dimenzování vedení** – při návrhu je nutné uvažovat úbytek napájecího napětí na vedení vlivem jeho délky. Většina komponent EZS dokáže pracovat při napětí v rozsahu 10 - 15 V. Pro výpočet úbytků existuje řada metod, ale v praxi postačí odhad na základě tabulky s předpočítanými hodnotami pro nejčastěji používané průřezy vodičů. Hodnoty jsou vypočítány pro délku páru vodičů. Dle tabulky 4.2 bude tedy na prvku EZS s proudovým odběrem 100 mA napojeném na 12 V napájecí zdroj párem vodičů o průřezu 0,22 mm$^2$ a vzdáleném od něj 100 m napětí 10 V (úbytek na vedení je 2 V).

| | **Vodič o průřezu 0,22 mm$^2$ (úbytek napětí [V])** | | | | | **Vodič o průřezu 0,5 mm$^2$ (úbytek napětí [V])** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **10 m** | **20 m** | **50 m** | **100 m** | **300 m** | **10 m** | **20 m** | **50 m** | **100 m** | **300 m** |
| **5 mA** | 0,01 | 0,02 | 0,05 | 0,1 | 0,3 | 0 | 0 | 0,02 | 0,04 | 0,12 |
| **10 mA** | 0,02 | 0,04 | 0,1 | 0,2 | 0,6 | 0 | 0,01 | 0,04 | 0,08 | 0,24 |
| **20 mA** | 0,04 | 0,08 | 0,2 | 0,4 | 1,2 | 0,01 | 0,03 | 0,08 | 0,16 | 0,48 |
| **50 mA** | 0,1 | 0,2 | 0,5 | 1 | 3 | 0,04 | 0,08 | 0,2 | 0,4 | 1,2 |
| **100 mA** | 0,2 | 0,4 | 1 | 2 | × | 0,08 | 0,16 | 0,4 | 0,8 | 2,4 |
| **200 mA** | 0,4 | 0,8 | 2 | 4 | × | 0,16 | 0,32 | 0,8 | 1,6 | 4,8 |
| **300 mA** | 0,6 | 1,2 | 3 | × | × | 0,24 | 0,48 | 1,2 | 2,4 | × |
| **400 mA** | 0,8 | 1,6 | 4 | × | × | 0,32 | 0,64 | 1,6 | 3,2 | × |
| **500 mA** | 1 | 2 | × | × | × | 0,4 | 0,8 | 2 | 4 | × |

Tabulka 4.2: Hodnoty úbytků napětí na vedení při různé proudové zátěži (převzato z [35])

**Volba trasy vedení** – je důležitá a často bagatelizovaná činnost. Trasu je vhodné navrhnout tak, aby nedocházelo k souběhům se silovým vedením, či jinými datovými kabely a zabránilo se tak nežádoucím induktivním vazbám.

| **Rušivý faktor** | **Analogové propojení** | **Datové propojení** | **Bezdrátové propojení** |
|---|---|---|---|
| Elektromagnetické rušení (výbojky, souběhy kabelů, motory řízené vysokofrekvenčními měniči) | ✓ | × | ✓ |
| Vysokofrekvenční rušení, případně velké kovové předměty (stěny, přepážky) | ✓ | ✓ | × |

Tabulka 4.3: Způsoby propojení ústředny s detektory v zarušeném prostředí (převzato z [17])

**Zálohovací akumulátor** – slouží pro napájení systému při výpadku primárního zdroje napájení. Minimální doby zálohování pro jednotlivé stupně zabezpečení jsou[1]:

| | **Stupeň 1** | **Stupeň 2** | **Stupeň 3** | **Stupeň 4** |
|---|---|---|---|---|
| **Pohotovostní doba (napájení z aku.)** | 12 hod | 12 hod | 60 hod | 60 hod |
| **Max. doba dobíjení na 80 % kapacity** | 72 hod | 72 hod | 24 hod | 24 hod |

Tabulka 4.4: Doby zálohování a nabíjení pro jednotlivé stupně zabezpečení (převzato z [14])

**Detektory** – je nutné volit takového provedení, aby na ně co nejméně působily případné rušivé vlivy. Těmi se myslí zejména domácí zvířata, elektromagnetické rušení, výtahy (vibrace), nebo vzduchotechnika a zdroje tepla (např. sálání způsobí pohyb záclon a tak může docházet k planým poplachům). Užitečnou pomůckou při výběru vhodného typu detektoru do určitým způsobem zarušeného prostředí je následující tabulka:

| **Rušivý faktor** | **Infrapasivní detektor (PIR)** | **Mikrovlnný detektor (MW)** | **Ultrazvukový detektor** | **Duální detektor (PIR+MW)** |
|---|---|---|---|---|
| Plastová vodovodní potrubí | ✓ | × | ✓ | ✓ |
| Klimatizace a ventilace | × | ✓ | × | ✓ |
| Zářivková osvětlení | ✓ | × | ✓ | ✓ |
| Halogenová světla | × | ✓ | ✓ | ✓ |

Tabulka 4.5: Výběr vhodného detektoru do zarušeného prostředí (převzato z [17])

**Signalizační zařízení** – (siréna) slouží k akustické a/nebo optické signalizaci narušení objektu. Většinou se v používají oba typy, tedy venkovní i vnitřní. Umísťují na hůře dostupná místa, čímž se minimalizuje možnost jejich poškození pachatelem. Venkovní siréna by měla být zálohovaná, tzn. mít svůj vlastní sekundární napájecí zdroj (baterii) pro případ výpadku napájení, či sabotáže.

[1] U EZS stupně zabezpečení 3 a 4 napojených na PCO mohou být doby zálohování a nabíjení poloviční oproti dobám uvedeným v tabulce 4.4.

**Uvedení do stavu střežení či klidu** – by mělo být na klávesnici indikováno akustickou a/nebo optickou signalizací. Je-li při zapínání EZS detekován některým z čidel pohyb, nebo je například rozpojený magnetický kontakt plášťové ochrany (otevřené dveře), nemělo by být možné systém zastřežit.

### 4.3.2 Zpřesněný systémový návrh

Dokument, zvaný *zpřesněný systémový návrh*, vzniká během fáze *přípravy na realizaci EZS* postupným rozšiřováním a zpřesňováním původního *systémového návrhu*. Volba vhodných komponent zabezpečovacího systému je provedena v rámci prohlídky a *technického posouzení objektu* (viz kapitola 4.3.1). Určí se plánované cesty vedení kabelů a zakreslí se do projektové dokumentace. Ta je potom spolu se zpřesněným systémovým návrhem a seznamem materiálu souhrnně nazývána jako *prováděcí dokumentace* (někdy též projektová dokumentace pro provedení stavby) a slouží jako hlavní podklad pro realizaci.

## 4.4 Instalace SZSOP

Instalace EZS je završením celého procesu budování zabezpečovacího systému. Výsledkem je správně nakonfigurovaný a plně funkční systém, který je připravený pro předání uživateli (zadavateli). Následuje popis jednotlivých dílčích kroků instalace:

**Realizace (montáž) EZS** – začíná převzetím objektu (pracoviště) od zadavatele a je zakončena existencí funkčního zabezpečovacího systému určeného ke kontrole a provedení výchozí revize (viz dále). Montáž je prováděna na základě projektové dokumentace, přičemž je kladen důraz na dodržování všech podmínek uvedených v kapitole *technické posouzení objektu* (4.3.1). Měli by s nimi být seznámeni všichni, jenž se na montáži nějakým způsobem podílejí. Projektová dokumentace totiž neobsahuje a ani nemůže obsahovat popis všech detailů instalace. Velká pozornost by měla být rovněž věnována podmínkám instalace kabelových rozvodů. Tím se myslí zejména dodržování barev vodičů (červená odpovídá „+“ pólu napájecího zdroje, černá případně modrá pak „−“), způsob napojování kabelů [2] a co nejmenší podíl souběhů se silovým vedením. Kabely by měly být vedeny v elektroinstalačních trubkách pod omítkou nebo na povrchu, popřípadě v instalačních lištách [17].

**Prohlídka EZS a dokumentace skutečného stavu** – provádí se na realizovaném systému odpojeném od napájení. Účelem je zjištění skutečného stavu a zanesení odchylek od původního projektu do projektové dokumentace. Zkoumá se zejména správnost umístění jednotlivých prvků dle požadavků či norem, mechanické a estetické provedení kabeláže a způsob zapojení smyček a jejich shoda s projektovou dokumentací.

**Výchozí revize** – na každém realizovaném zabezpečovacím systému musí být před jeho uvedením do provozu a předáním zadavateli vykonána revize. Tu může provádět pouze osoba s platným osvědčením dle § 9 vyhl.č.50/1978 Sb. Zabezpečovací systém musí být revidován v pravidelných časových intervalech (dohodne si zadavatel s realizační firmou, běžně 1 - 3 roky) po celou dobu jeho životnosti. První revize nově zřízeného EZS se nazývá *výchozí revize*. Ke každé vykonané revizi musí být vytvořen dokument zvaný *revizní zpráva*.

[2] U EZS lze kabely spojovat jen v montážních krabičkách které jsou osazeny sabotážním kontaktem, zvaným též „tamper“. Spojení lze realizovat jen pomocí svorkovnice, případně spájením.

**Zkoušky funkčnosti EZS** – mají za úkol prověřit správnou funkci realizovaného zabezpečovacího systému. Kontroluje se zejména správné nastavení a funkčnost všech detektorů a výstražných zařízení (sirény), dimenzace napájecích zdrojů a výdrž akumulátorů. Důležitý je rovněž celkový test systému včetně přenosu poplachové informace na PCO, disponuje-li EZS touto funkcí.

**Zaškolení obsluhy** – se provádí před nebo při předávání systému zadavateli k užívání. Všem zúčastněným je demonstrován způsob zastřežení a odstřežení systému a je jim vysvětleno, jakým způsobem mají reagovat v případě vyhlášení poplachového stavu. Vybraným uživatelům jsou navíc přidělena vyšší práva a stanou se tak lokálními správci. Mohou ostatním přidělovat a měnit uživatelská oprávnění, hesla, případně nastavovat datum a čas systému.

**Provozní kniha a předávací protokol** – jsou dokumenty, které obdrží zadavatel při přebírání zabezpečovacího systému. Provozní kniha slouží k vedení záznamů o nejrůznějších událostech v průběhu užívání EZS. Evidují se především změny systému a provádění revizí či funkčních testů. Předávací protokol pak obsahuje všechny další nezbytné informace, a to zejména [17]:

- jméno přebírající osoby,
- předmět díla (objekt),
- místo umístění díla (adresa objektu),
- rozsah díla (seznam použitých komponent),
- datum,
- výsledky funkčních testů,
- jména osob zaškolených v ovládání EZS,
- záruku na dílo,
- údaje o firmě zajišťující servis (záruční i pozáruční),
- případné dodatky.

## 4.5 Význam schematických značek při budování EZS

Ke správnému průběhu celého procesu návrhu a realizace zabezpečovacího systém přispívá použití normalizovaných schematických značek EZS. Díky tomu je zajištěna jednoznačnost a správná interpretace projektové dokumentace, kterou v praxi většinou někdo jiný vyprojektuje (projektant) a někdo jiný podle ní následně realizuje zabezpečovací systém (montážní firma).

Schematické značky byly definovány v normě ČSN EN 50131-1/Z1 - Národní příloha, vydané v roce 2000. Aktuální platná norma ČSN EN 50131-1 ed. 2 z roku 2007 jejich platnost zachovává.

# Kapitola 5

# Prostředky používané pro realizaci SZSOP

Moderní systém pro zabezpečení a střežení objektů a prostor (SZSOP) je poměrně složitou záležitostí. Bývá sestaven z několika různých samostatných podsystémů, které musí být schopny vedle sebe nejen koexistovat, ale mnohdy spolu i vzájemně kooperovat.

Účelem této kapitoly je poskytnout komplexní přehled o prvcích používaných v jednotlivých dílčích podsystémech zabezpečovacího systému. Jsou zde zmíněny zejména komponenty používané pro realizaci systémů EZS, ACS, CCTV a EPS.

## 5.1 EZS – Elektronické zabezpečovací systémy

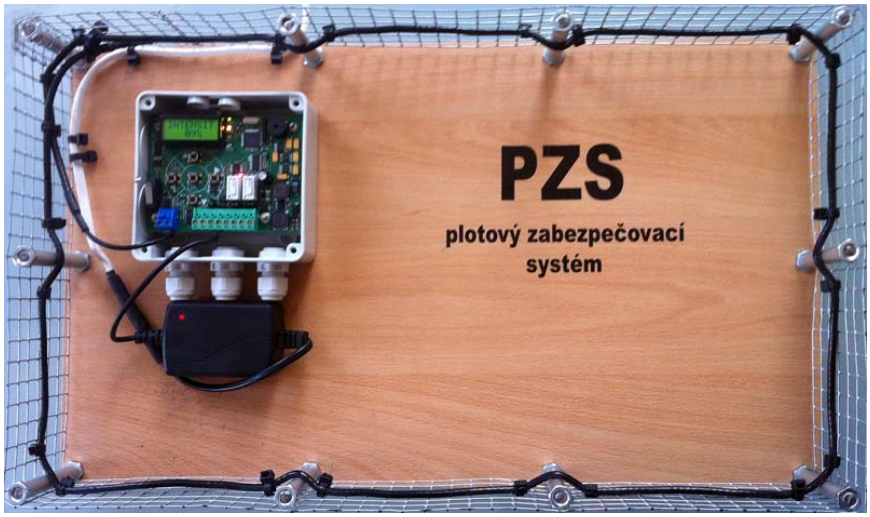
*Elektronické zabezpečovací systémy (EZS)* (v angličtině označované zkratkou IAS, *Intruder Alarm Systems*) slouží k akustické a/nebo optické signalizaci neoprávněného vniknutí do střeženého objektu (více viz kapitola 3.5). Požadavky kladené na systémy EZS a jejich dílčí prvky stanovuje rodina norem ČSN EN 50131-X. Jako zdroj vědomostí pro následující přehled komponent posloužila skripta [28].

### 5.1.1 Prvky obvodové (perimetrické) ochrany

Mají za úkol zajišťovat ochranu obvodu objektu, tedy většinou katastrálních hranic pozemku. K tomu se využívá mnoha různých typů detektorů. Ty musí být konstruovány pro použití ve venkovním prostředí a je třeba aby spolehlivě vykonávaly svoji činnost i při špatných povětrnostních podmínkách.

**Plotová vibrační čidla** – sestávají z perimetru, který je provlečen oplocením a může tvořit až kilometr dlouhé úseky. *Perimetr* (z řečtiny – „obvod“) je v tomto případě realizován dvouvodičovou linkou s vibračními čidly. Někdy bývá nazýván též jako *senzorický kabel*, nebo *detekční vedení*. Řídící jednotka do něj posílá krátké impulsy a zároveň vyhodnocuje odražené signály. Podle jejich charakteru je možné rozeznat stav detekčního vedení a při narušení pak dokonce s přesností na 20 metrů určit místo, kde k němu došlo [28].

**Mikrofonní koaxiální kabely** – generují při mechanickém namáhání (pohyb, vibrace) na svém výstupu elektrický signál. Ten je dále zpracováván a na základě jeho průběhu lze rozeznat i přesný typ narušení (nadzvednutí, přelézání, nebo přestřihnutí pletiva).




Obrázek 5.1: Model plotového zabezpečovacího systému (PZS)

**Diferenciální tlaková čidla** – jsou tvořena dvojicí v zemi paralelně uložených pružných hadic naplněných nemrznoucí kapalinou. Hadice bývají natlakovány na hodnotu okolo 250 kPa, zakopány zhruba 30 cm hluboko a rozteč mezi nimi by měla být asi 1 metr. Tlak je neustále monitorován a vyhodnocován a v případě jeho náhlé změny je vyhlášen poplach. Díky souběhu páru hadic se vyruší případné negativní vlivy, protože působí na obě hadice současně a stejnou měrou. Negativními vlivy se myslí například tlak od kořenů stromů vlivem jejich pohybů ve větru, nebo vibrace od aut projíždějících po blízké silnici.

**Perimetrická PIR čidla** – jsou prakticky totožná s bariérovými čidly se *záclonovou* charakteristikou používanými v plášťové ochraně. Vysílaný paprsek má v horizontální rovině velice malý úhel záběru (do 10 °) a jeho dosah bývá typicky 50 - 150 metrů.

**Štěrbinové kabely** – jsou opět instalovány v páru do země do hloubky zhruba 30 cm a vzdálenosti 2 metry od sebe. Po celém povrchu vodiče jsou pravidelně rozmístěny otvory („štěrbiny“) tvaru kosočtverce. Jeden kabel nimi vyzařuje vysokofrekvenční energii a druhý ji přijímá. Prostor detekce má tvar elipsy a je široký zhruba 3 metry a vysoký 1,25 m. Vniknutí cizího tělesa do tohoto elektromagnetického pole (jedno jakou rychlostí) vyvolá změnu amplitudy signálu a řídící jednotka vyhlásí poplach.

**Infračervené závory a bariéry** – jsou realizovány vždy jako set dvou detektorů. Vysílací část na jedné straně a přijímací na straně druhé. Vysílač vysílá přes optiku přesně zaměřený a kódovaný (z důvodu zamezení vzájemného ovlivňování se více soustav) infračervený paprsek, který je neustále vyhodnocován přijímačem. Pokud dojde k jakémukoli přerušení tohoto paprsku (například pachatelem), je vyhlášen poplach. Dosah závor je desítky až stovky metrů.

Infračervené bariéry jsou tvořeny soustavou více IR závor (na vysílací i přijímací straně stejný počet) umístěných nad sebou do podoby jakéhosi sloupku.

**Laserové závory** – pracují na stejném principu jako IR závory a bariéry. Rozdíl je jen v použití neviditelného laserového paprsku vlnové délky 850 nm namísto IR záření. Dosah tohoto řešení v přehledném terénu je až 1 km.

**Mikrovlnné závory** – používají obdobný způsob detekce jako MW detektory pro prostorovou ochranu (viz kapitola 5.1.3). Liší se především odolnějším provedením a vyzařovací charakteristikou ve tvaru rotačního elipsoidu s rotací okolo osy, kterou tvoří pomyslná spojnice obou částí závory. Stejně jako u IR závor totiž sestávají ze setu dvou detektorů. Vysílací části na jedné straně a přijímací na straně druhé.

### 5.1.2 Prvky plášťové ochrany

Slouží k ochraně pláště objektu (okna, dveře, vrata) před vniknutím neoprávněné osoby.

**Kontaktní čidla** – jednoduché rozpínací kontakty různého provedení. Jsou to nejrůznější mikrospínače (sabotážní kontakty v EZS komponentách), dveřní magnetické kontakty (2 části – jazýčkové relé na neotevíratelné části dveří, permanentní magnet na dveřích) a koncové spínače.

**Destrukční čidla** – jsou založena na nevratné destruktivní činnosti. Při detekci je tedy čidlo zničeno a poté musí být nahrazeno nebo opraveno. Jako příklad lze uvést tenkou vodivou vrstvu nanesenou na skleněné výplni okna. Při rozbití skla dojde k jejímu přerušení a tím k vyhlášení poplachu.

**Čidla destrukčních projevů** – reagují na vibrace vznikající při pokusu o destrukci chráněných ploch (rozbití skla, proražení zdi). Používají se čidla otřesová a na ochranu skleněných ploch. Ta mohou být pasivní kontaktní (piezočidla nalepená na skle), pasivní bezkontaktní (vyhodnocování akustického projevu při destrukci) případně aktivní kontaktní. Posledně jmenované jsou nejkvalitnější a mají nejmenší procento podílu planých poplachů. Vysílací část detektoru vysílá do skleněné výplně ultrazvukový a/nebo optický signál, který je přijímací částí trvale vyhodnocován. Při destrukci skla dojde pochopitelně ke změně přenosových vlastností a tím k vyhlášení poplachu.

**Akustická (infrazvuková) čidla** – citlivé snímače akustického vlnění o frekvenci jednotek Hz. Ta vznikají při pohybu velkých ploch, nebo při změně objemu vzduchu v místnosti (otevření dveří, rozbití okna).

**Bariérová čidla** – jsou zastoupena pasivními i aktivními infračervenými detektory s tzv. „záclonovou“ (úzkou v horizontální rovině, širokou ve vertikální) vyzařovací charakteristikou. Čidlo se umístí na zeď do blízkosti okna tak, aby s ním infračervené IR paprsky byly rovnoběžné.

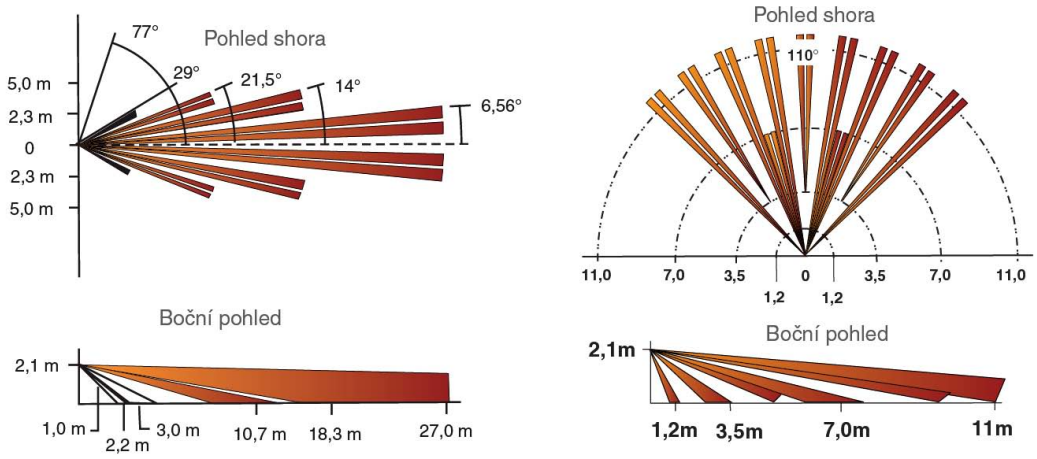
### 5.1.3 Prvky prostorové ochrany

Jedná se zejména o detektory pohybu určené pro montáž na zeď nebo strop ve vnitřních částech objektu. Jejich úkolem je sledovat vymezený prostor a detekovat v něm případný pohyb.

Některé detektory jsou vybaveny tzv. funkcí *antimasking*, což je ochrana proti vyřazení čidla z provozu překrytím nějakým předmětem, či přestříkáním barvou. Detektory si tak neustále (i v klidovém stavu EZS systému) hlídají prostor před sebou a v případě zastínění pak není možné uvést zabezpečovací systém do stavu střežení. Uživatel je o této skutečnosti informován a obdrží i informaci o tom, které čidlo je zastíněno. Potenciálnímu narušiteli je tak znemožněno „předpřipravit“ si objekt pro vloupání v době, kdy je EZS systém vypnut (resp. není ve stavu střežení).

**Pasivní infračervené detektory** – (PIR, *passive infrared sensors*) vyhodnocují změny infračerveného spektra elektromagnetického vlnění. Zdrojem vlnění je každé těleso, jehož teplota je vyšší než absolutní nula (–273, 15 °C) a nižší než 560 °C. Teplotě lidského těla (průměrně 36 – 37 °C) odpovídá vlnová délka 9,4 $\mu m$ [15].

Snímacím prvkem je polovodičová součástka (zvaná „pyroelement“) která snímá IR (infračervené) záření. Před ní je umístěna optika (většinou plastová Fresnelova čočka), jenž rozděluje snímaný prostor střídavě na aktivní a neaktivní zóny. Pohyb tělesa s odlišnou teplotou od okolí (člověk) mezi těmito zónami způsobí na pyroelementu změny, které jsou řídící elektronikou vyhodnoceny jako narušení. Provedení Fresnelovy čočky ovlivňuje velikost zorného úhlu a dosah detektoru. Na obrázku 5.2 jsou znázorněny detekční charakteristiky čidla s velkým dosahem (vlevo) a velkým zorným úhlem (vpravo). Je zřejmé, že tyto parametry jsou protichůdné.




Obrázek 5.2: Detekční charakteristiky 2 rozdílných PIR detektorů (zdroj: [30])

**Aktivní mikrovlnné detektory** – (MW, *Microwave senzors*) využívají k detekci pohybu *Dopplerova jevu*. Mikrovlnné čidlo vysílá paprsky o frekvenci $f_0$ a přijímá jejich odrazy o frekvenci $f$ pro níž platí:

$$f = \frac{f_0}{1 - \left(\frac{v}{c}\right)^2} \tag{5.1}$$

kde $v$ je rychlost pohybujícího se tělesa, $c$ rychlost pohybu vysílaného vlnění.

Rozdíl fází těchto frekvencí je vyhodnocován řídící elektronikou čidla. Vysílací kmitočet je obvykle 2,5 GHz, 10 GHz nebo 24 GHz. Oproti PIR čidlům detekují nejlépe pohyb ve směru k a od detektoru a mohou se vzájemně negativně ovlivňovat. Problém představují rovněž kovové a hladké plochy.

**Aktivní ultrazvukové detektory** – (US) využívají stejně jako MW čidla Dopplerova jevu. Liší se prakticky jen tím, že vysílají ultrazvukové vlny o kmitočtu 40 kHz. Opět platí, že jsou nejcitlivější na pohyb směrem k a od detektoru.

**Aktivní infračervené detektory** – (AIR, *active infrared detectors*) vysílají infračervené paprsky a vyhodnocují jejich odraz. Narozdíl od PIR čidel jsou schopny detekovat pomalý pohyb, nebo pohyb tělesa nevyzařujícího teplo a mohou být použity i v objektech

s rychlými teplotními změnami (výrobní procesy). Další výhodou je možnost změny detekční charakteristiky pouhým přeprogramováním (bez nutnosti měnit čočku). Nevýhodou je větší spotřeba a možnost sledování aktivity čidla pachatelem.

**Kombinované detektory (duální)** – se používají z důvodu snahy o snížení množství planých poplachů a tím zvýšení spolehlivosti zabezpečovacího systému. Narušení je detekováno jen při současné aktivaci obou částí detektoru založených na odlišných principech detekce. Nejčastěji se kombinují PIR a MW čidla.

### 5.1.4 Prvky předmětové ochrany

Používají se k ochraně nejrůznějších cenných předmětů jako jsou například trezory, obrazy či jiná umělecká díla. Střežení těchto předmětů je většinou prováděno trvale, bez ohledu na stav, v jakém se EZS nachází.

**Kontaktní čidla** – jsou tvořena mikrospínači nebo různými tlakovými, tahovými a magnetickými kontakty.

**Kapacitní čidla** – si lze představit jako deskové kondenzátory, jejichž dielektrikum tvoří vzduch a elektrody kovové části předmětu a zem. Dotek, nebo jen pouhé přiblížení se k chráněnému předmětu, způsobí změnu kapacity, což je následně řídící jednotkou vyhodnoceno jako narušení.

**Tlaková akustická čidla** – snímají a vyhodnocují vibrace vznikající při destrukci (nebo pokusu o ní) chráněných ploch (např. skleněná vitrína s exponáty). Podrobněji byl tento typ detektoru popsán v kapitole 5.1.2.

**Bariérová čidla** – vysílají paprsky s „bariérovou“ vyzařovací charakteristikou a reagují na jejich narušení (viz 5.1.2). Takovouto charakteristiku mohou mít například laserová, PIR a AIR čidla, nebo infračervené závory..

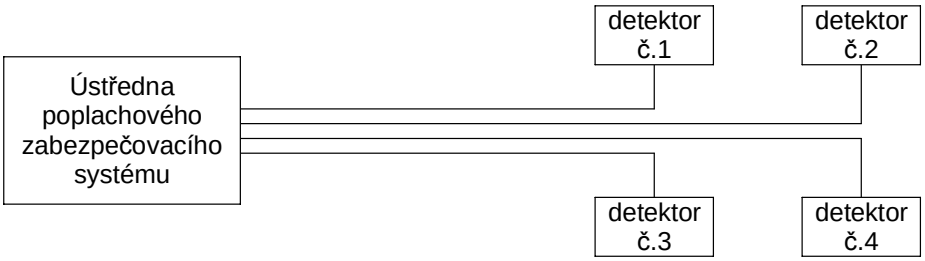
**Trezorová čidla** – jsou seismické detektory schopné rozpoznat všechny možné typy útoků na trezory. Dokáží detekovat použití ručního i elektrického nářadí (kladivo, vrtačka, rozbrušovačka), tepelného nářadí (kyslíko-acetylenový řezací hořák) a výbušnin. Princip činnosti je založen na analýze zvukových vln pořizovaných mikrofonem.

### 5.1.5 Ústředny EZS

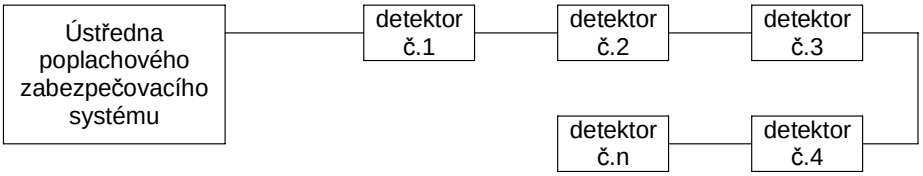
Z hlediska způsobu připojování detektorů se ústředny rozlišují na [28]:

**Analogové (smyčkové)** – každá poplachová smyčka má přiřazen samostatný vyhodnocovací obvod ústředny. Poplachovou smyčku tvoří jeden, nebo skupina detektorů (respektive jejich rozpínacích kontaktů). Nevýhodou takového řešení je potřeba velkého množství kabeláže, jelikož ke každému detektoru vedou minimálně vodiče pro napájení, poplachový a sabotážní kontakt.

**Sběrnicové (s přímou adresací čidel)** – mezi ústřednou a detektory probíhá digitální adresná komunikace po sběrnici. Využívá se tzv. *časového multiplexu*, kdy v daný okamžik komunikuje ústředna právě s jedním prvkem systému (detektor, siréna). Každá adresná komponenta musí mít tedy v rámci systému přiřazeno jedinečné ID (adresu). Výhodou je jednoduše realizovaná kabeláž (čtyřvodičové vedení – 2 vodiče pro napájení a 2 pro sběrnici) a vysoká odolnost systému proti sabotáži.

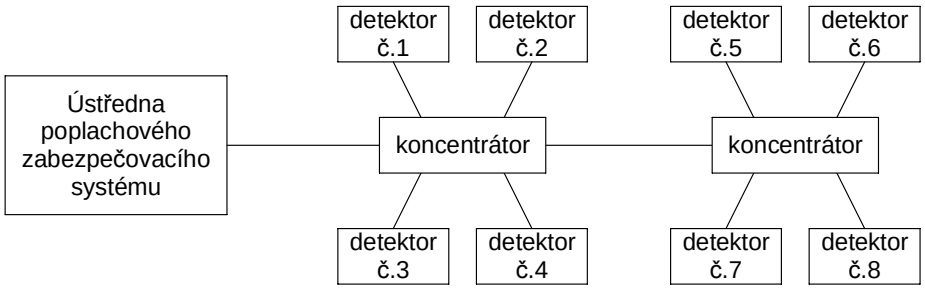



Obrázek 5.3: Blokové schéma smyčkové ústředny (převzato z [28])




Obrázek 5.4: Blokové schéma sběrnicové ústředny (převzato z [28])

**Koncentrátorové (smíšené)** – kombinují výhody obou předchozích typů. K ústředně jsou přes sběrnici připojeny takzvané *koncentrátory* plnící funkci smyčkových „podústředen“. Komunikace mezi nimi a ústřednou probíhá pomocí datové sběrnice. Detektory se ke koncentrátorům připojují již klasicky pomocí smyček (tedy stejně jako u analogových ústředen). Je-li ústředna vhodně dimenzována, je možné napojit na smyčku každého koncentrátoru právě jeden detektor a takto realizovat systém s až několika sty adresnými čidly (každá smyčka koncentrátoru je adresná). Tyto ústředny jsou velice vhodné pro instalaci do rozsáhlejších objektů.




Obrázek 5.5: Blokové schéma koncentrátorové ústředny (převzato z [28])

**Bezdrátové ústředny** – umožňují bezdrátové propojení s detektory a dalšími komponenty EZS systému. Díky tomu jsou užitečné všude tam, kde není vhodné nebo možné tahat kabeláž (historické a památkově chráněné objekty). Přenos probíhá nejčastěji na frekvencích 433 nebo 868 MHz a napájení je realizováno z baterií, které v detektorech vydrží až několik měsíců či roků.

**Hybridní** – kombinují výhody sběrnicových a bezdrátových ústředen. Všechny detektory jsou opět adresovatelné a mohou být připojeny buďto na sběrnici, nebo bezdrátově.

## 5.2 ACS - Systémy kontroly vstupů a docházkové systémy

Dle platné normy [3] ČSN EN 50133-1 je *systém kontroly vstupů (ACS)* definován jako: „Systém obsahující všechna konstrukční a organizační opatření včetně těch, která se týkají zařízení nutných pro řízení vstupu.“

Systémy kontroly vstupů (někdy zkráceně označované jako *vstupní systémy*) se tedy používají k řízení a kontrole přístupů do objektů, nebo jejich částí, na základě přidělených přístupových práv. Speciálním případem přístupových systémů jsou docházkové systémy. Ty jsou určeny ke sběru a následnému zpracování informací (evidence docházky) o čase a účelu průchodu kontrolním místem (např. hlavní vchod do budovy firmy). Oba systémy bývají mnohdy propojeny a tvoří spolu jeden funkční celek [29].

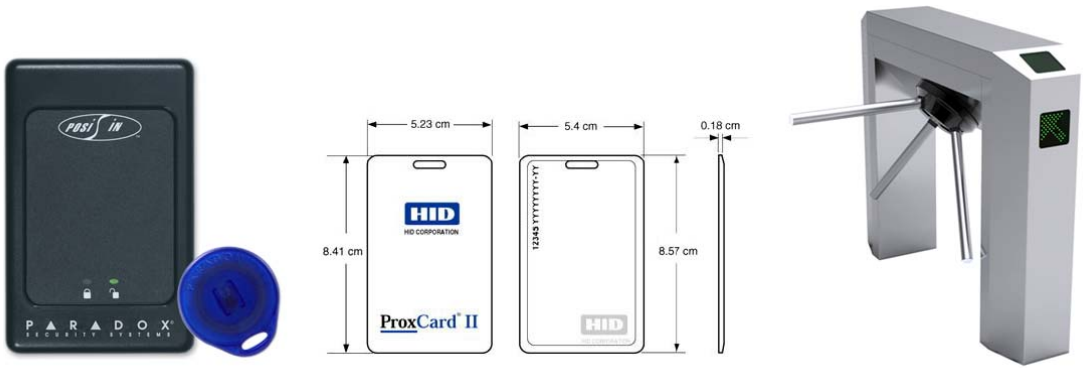
**Identifikační prvky** – se dělí podle toho, zda přistupující osoba vlastní identifikační prvek (magnetické či čipové karty a přívěšky), disponuje znalostí kódu (každá oprávněné osoba má přidělen PIN kód), případně biometrickými rysy.

**Snímací zařízení** – jsou volena podle použitých identifikačních prvků. Existují snímače kódové informace (klávesnice), biometrických rysů osob (otisk prstu, geometrie ruky, oční sítnice, analýza lidského hlasu), identifikačních prvků (karty, čipy) a kombinované (kombinace předchozích pro zvýšení bezpečnosti). V praxi se nejčastěji používají snímače kombinující čtečku karet/čipů a klávesnici.

**Řídící jednotky** – (terminály) rozhoduji na základě databáze s oprávněními jednotlivých osob a informací od snímacího zařízení o umožnění nebo zamítnutí vstupu.

**Centrální jednotka** – je propojena s řídícími jednotkami a monitoruje a řídí celý přístupový/docházkový systém. Tvoří ji nejčastěji PC s nainstalovaným příslušným softwarem jenž je s řídícími jednotkami propojen pomocí počítačové sítě. Hlavním úkolem centrální jednotky je sběr, uchovávání a analýza informací z terminálů. Možným výstupem analýzy je například seznam procházejících osob a evidence docházky.

**Blokovací zařízení** – slouží k fyzickému zablokování nebo umožnění vstupu. Nejčastěji se k tomuto účelu používají elektrické zámky, nejrůznější turnikety a závory.




Obrázek 5.6: Čtečka, přívěšek a karta HID (Proximity 125 kHz), turniket

## 5.3 CCTV - kamerové systémy

*Kamerové systémy (CCTV – Closed Circuit Television, systémy uzavřených televizních okruhů)* slouží k monitorování a zaznamenávání dění v místě jejich instalace. Název *uzavřený televizní okruh* je odvozen od skutečnosti, že obraz z kamer je zde narozdíl od televizního vysílání dostupný jen v rámci kamerového systému, tedy určitého malého území (objektu). Veškeré požadavky kladené na systémy CCTV stanovují normy z rodiny ČSN EN 50132-X.

**Kamery** – Kamery jsou základem každého kamerového systému. Scéna (obrazová informace) je přes objektiv snímána CCD [1] čipem a převedena na elektrický signál (videosignál). Kamery lze dělit dle:

- **napájení** – 12 V DC, 12/24 V AC, 230 V AC,
- **videosignálu** – černobílé (B/W), barevné (COLOR),
- **druhu přenosu videosignálu** – analogové, IP kamery,
- **objektivu** – výměnný, součástí kamery,
- **určení do prostředí** – pro vnitřní použití, pro venkovní montáž,
- **konstrukce** – klasické s vyměnitelným objektivem, kompaktní (objektiv součástí kamery), vodotěsné, stropní (tzv. DOME kamery), PTZ kamery (uživatelské otáčení ve vertikálním i horizontálním směru a plynulá změna ohniskové vzdálenosti objektivu), miniaturní, deskové (jen deska s elektronikou a objektivem) a skryté (např. v PIR čidle).

**Digitální záznamová zařízení** – označovaná jako DVR (z anglického *Digital Video Recorder*) zobrazují a ukládají videozáznam z analogových kamer (případně i audiozáznam z mikrofonů) pro jeho případné pozdější zprostředkování. Aktuálně používané videorekordéry jsou označovány jako *triplexní*. To znamená, že umožňují současné pořizovaní záznamů, jejich lokální prohlížení (na monitoru připojeném k DVR) a poskytování uživatelům připojeným přes počítačovou síť. Digitální videorekordéry jsou tvořeny specializovaným hardwarem provádějícím kompresi videa (dříve formát MPEG-4, nyní úspornější H.264) a audia. O správnou funkci se stará realtime operační systém (každý výrobce si vyvíjí svůj) a záznamy jsou ukládány na běžné počítačové 3,5"pevné disky. Existují i hardwarové karty do počítač, ze kterého se po nainstalování příslušného software defacto stane DVR. Takové řešení je sice levnější, ale zato méně spolehlivé a energeticky náročnější, než u digitálních videorekordérů.

**NVR** – (z anglického *Network Video Recorder*) slouží pro ukládání a zprostředkovávání záznamů z IP kamer. IP kamery jsou prakticky totožné s analogovými. Liší se hlavně tím, že obrazová informace je digitální a je přenášena přes síťové rozhraní (konektor RJ-45). Zařízení NVR stejně jako DVR obsahují realtime operační systém a záznamy ukládají na pevný disk. Opět platí, že počítač s nainstalovaným softwarem zastane podobnou funkci, ale toto řešení je méně spolehlivé a energeticky více náročné.

**IR přísvity** – Většina kamer disponuje mimo denního režimu ještě takzvaným nočním režimem, kdy se pro větší citlivost na zbytkové světlo přepne CCD čip do černobílého

[1] CCD – „Charge-Coupled Device“, nebo-li zařízení s vázanými náboji [31]. V současnosti se používá jako snímací prvek u většiny kamer a digitálních fotoaparátů.

snímání a předřadí se před něj IR filtr. Tato funkce se v menu kamer nazývá D/N (odvozeno od slov day a night). Přepínání se děje automaticky podle intenzity okolního osvětlení, případně lze ovlivnit tlačítkem, nebo se režim den či noc nastaví trvale. Při přechodu kamery do nočního režimu se zapne její IR [2] přísvit sestávající z několika desítek IR LED diod umístěných většinou v kruhu okolo objektivu. Ty emitují infračervené světlo o vlnové délce v rozsahu 810 - 940 nm (nejčastěji 850 nm) jenž je pro lidské oko neviditelné. Takovéto kamery mohou i v naprosté tmě „vidět" na vzdálenosti až desítek metrů. Pokud se navíc použije kvalitní externí IR přísvit, prodlouží se tato vzdálenost až na stovky metrů (200 - 300 m).

**Přenos videosignálu** – je možný několika různými způsoby. Při výběru nejvhodnějšího z nich záleží především na požadované vzdálenosti a ceně. Pro CCTV existují tyto přenosové prostředky:

**Koaxiální kabel** – s impedancí 75 Ω je nejrozšířenější způsob vedení videosignálu na vzdálenosti řádově několik stovek metrů.

**Symetrické vedení** – umožňuje přenos videosignálu na vzdálenosti až okolo 1500 metrů. Přenos je realizován po kroucené dvojlince, tedy například po UTP kabelu `Cat5E`, který se používá pro počítačové sítě. Nevýhodou je vyšší cena, protože mimo kabeláž je navíc třeba 2 převodníků ke každé kameře (1 pro převod videosignálu z kamery na kroucenou dvojlinku a 2. pro převod zpět na videosignál).

**Bezdrátový přenos** – lze použít všude tam, kde je obtížné nebo nemožné tahat kabeláž. Přenosová vzdálenost bývá v řádu jednotek kilometrů. Nevýhodou je vyšší cena a poměrně velká míra rušení (obvzvláště ve městech), jelikož pro přenos je využíváno pásmo 2,4 GHz, ve kterém jsou provozovány `WiFi` sítě. Přenášen může být jak videosignál z analogových kamer (převede se takzvaným webserverem na datový tok a na druhé straně zase zpět), tak datový tok z IP kamer.

**Optický kabel** – je nejdražší, ale zato nejspolehlivější způsob přenosu (nejen) videosignálu na vzdálenost až desítek kilometrů. Nevýhodou je cena a větší technické nároky na instalaci. Po optickém kabelu lze přenášet jak videosignál z analogových kamer, tak datový tok z IP kamer.

**Počítačová síť** – bývá realizována UTP kabelem `Cat5E` a umožňuje přenos videosignálu na vzdálenosti řádově stovek metrů. Opět je možné přenášet datový tok jak z IP kamer, tak z webserverů na které jsou napojeny analogové kamery.

**Automatické sledování pohybujícího se objektu** – je v oblasti CCTV hitem posledních měsíců. Základ tvoří PTZ [3] kamera poskytující obrazovou informaci. Ta je dále zpracována specializovaným zařízením označovaným jako *zařízení pro sledování pohybu* (anglicky *tracking box*). Jeho úkolem je rozpoznat v obraze pohybující se objekt, určit směr pohybu a na základě toho generovat řídící povely pro PTZ kameru. Výsledkem je skutečnost, že se PTZ kamera za tímto objektem otáčí a neustále jej tak udržuje v obraze [16].

[2] IR – (z angl. *infrared*) je označení pro infračervené záření o vlnové délce v rozsahu 760 nm - 1 mm [32].

[3] PTZ kamera – (z anglického *Pan-Tilt-Zoom*) je uživatelsky ovladatelná pohyblivá kamera umožňující pohyb v horizontální i vertikální rovině a plynulou změnu ohniska objektivu (tzv. zoom).

## 5.4 EPS - Elektrická požární signalizace

*Elektrická požární signalizace (EPS)* slouží k včasné detekci a signalizaci prvotních příznaků vznikajícího požáru. Díky tomu je možné požár zlikvidovat v počátečním stádiu dříve, než napáchá mnoho škod [26]. Veškeré náležitosti týkající se systémů EPS stanovuje série norem z rodiny ČSN EN 54-X.

**Požární hlásiče (detektory)** – reagují na jevy doprovázející zahoření (vznik požáru) změnou elektrického odporu, případně proudu protékajícího detektorem. Existují požární hlásiče manuální (tlačítkové), automatické, optické hlásiče plamene, hlásiče využívající detekce plynů, tepelné detektory a jiné [29].

Nejčastěji používané jsou optické detektory. Princip jejich činnosti je založen na odrazu infračerveného (IR) světla od částic kouře vnikajícího do komory detektoru. Odražené IR světlo je snímáno optočlenem (fotodiodou) a poté vyhodnocováno řídící elektronikou. Ta následně vyšle signál do ústředny EPS.

**Autonomní hlásiče požáru a plynu** – jsou detektory tvořící samostatný systém ochrany proti požáru. Principiálně jsou totožné s požárními hlásiči, od kterých se liší jen tím, že namísto napojení na ústřednu EPS (ta není vůbec přítomna) signalizují vznikající poplach samostatně. Napájení je mnohdy realizováno z baterie (9 V) a velkou výhodu představuje nízká cena. Mimo autonomní hlásiče požáru se hojně využívají i autonomní hlásiče plynu.

**Ústředny EPS** – sbírají a vyhodnocují informace od požárních hlásičů. Ty dále zpracovávají a v případě zahoření se postarají o vyhlášení požárního poplachu, případně aktivaci samočinných hasících zařízení (jsou-li přítomna). Existují ústředny:

**Konvenční neadresné** – na jedné proudově vyvážené smyčce je připojeno více hlásičů (až 32), nelze tedy rozeznat který hlásič byl aktivován.

**Konvenční adresné** – každý hlásič má jedinečné ID, lze tak zjistit který byl aktivován. Hlásiče rozlišují jen stavy *klid* a *poplach*.

**Analogové** – pomocí sběrnice s kruhovou topologií jsou připojeny adresné hlásiče (každý má jedinečné ID) dodávající analogovou vícestavovou informaci.

**Interaktivní** – využívají inteligentních adresných detektorů vybavených mikroprocesory, které samy vyhodnotí situaci a do ústředny zasílají jen informace o nastalém stavu. Výhodou je pak menší zátěž sběrnice.

**Přenosové prostředky** – zajišťují přenos poplachové informace do *ohlašovny požáru*. Ta může být buďto místní (vrátnice, vlastní požárním útvar - např. v jaderné elektrárně), nebo vzdálená. V obou případech je však důležitý co nejrychlejší zásah proti vznikajícímu požáru. Požární systémy bývají často napojeny na specializované pulty požární ochrany (např. Genova), popřípadě vybrané pulty centralizované ochrany (PCO), které tuto službu poskytují.

# Kapitola 6

# Specifikace požadavků kladených na systém zabezpečení a střežení

Před přistoupením k samotnému návrhu je třeba nejdříve znát všechny požadavky zákazníka (zadavatele) na zabezpečovací systém. Proces získávání těchto informací je většinou poměrně obtížný, protože zadavatelem bývá ve většině případů laik bez většího povědomí o možnostech a principech zabezpečovacích systémů.

## 6.1 Neformální slovní specifikace zvoleného SZSOP

Mějme tedy zákazníka, jenž je majitelem obchodní firmy a pojmenujme ho například pan Opatrný. Pro následující soupis požadavků je uvažována prohlídka objektu jeho firmy a fiktivní rozhovor mezi ním a projektantem.

Zabezpečovaným objektem je středně rozsáhlá 2 - podlažní budova. V 1. nadzemním podlaží sídlí administrativní část majitelovy firmy zabývající se obchodní činností, ve druhém patře jsou volné kanceláře určené k pronájmu. Z tohoto důvodu je třeba, aby zabezpečovací systém mohl být snadno rozdělen na několik podsystémů. Perimetrická ochrana není vyžadována, protože budova nemá oplocení a je součástí menší technologické zóny. Pan Opatrný nepožaduje napojení objektu na PCO, postačí mu přenos poplachové informace na jeho a manželčin GSM telefon. Jelikož je v budoucnu plánována přístavba dalšího patra, musí existovat možnost snadného rozšíření zabezpečovacího systému.

Ve firmě v současnosti pracuje zhruba 30 zaměstnanců, kteří budou podle oddělení rozděleni do několika různých skupin s rozdílnými oprávněními. Tím bude jasně stanoveno, které dveře smí daná konkrétní osoba otevírat a do jakých prostor tak vstupovat. Každý zaměstnanec bude vlastnit svůj PIN kód a přístupovou kartu (popřípadě bezkontaktní přívěšek) a u většiny dveří bude příslušná čtečka či klávesnice. Majitel požaduje rovněž integraci docházkového systému s možností exportu přehledných měsíčních výpisů. Do evidence docházky bude zahrnuta pouze čtečka umístěná u hlavního vchodu do budovy. Kvůli časté obměně zaměstnanců na některých pozicích (uklízečka, brigádníci) je požadován snadný způsob přidávání a změn uživatelských účtů. Velice užitečná by byla možnost vyhradit si určitou skupinu čipových karet se základním oprávněním pro případné návštěvníky a hosty.

Dalším přáním pana Opatrného je existence TCP/IP rozhraní umožňujícího spravovat zabezpečovací systém a uživatelské účty z počítače připojeného do podnikové počítačové sítě (LAN). Rovněž by se mu líbilo využití pohybových PIR čidel zabezpečovacího systému pro spínání světel na chodbě v nastavitelnou večerní dobu.

Jedním z požadavků je i kamerový systém sestávající z 8 - 16 ti barevných kamer schopných „vidět“ i ve tmě. Většina jich bude umístěných uvnitř objektu na chodbách a v některých kancelářích. Vně budovy by měl být rozmístěn rozumný počet přehledových kamer zabírajících hlavní vstup do objektu a na rozích budovy pak 4 otočné (PTZ) kamery monitorující okolí pláště budovy a parkoviště. U těchto kamer navíc zákazník požaduje schopnost automatického sledování případného pohybujícího se objektu (auto, postava) a možnost jejich ovládání z klávesnice ze svojí kanceláře. Tam bude rovněž umístěno digitální záznamové zařízení a monitor. Doba záznamu obrazu (zvuk není prý třeba) ze všech kamer musí být alespoň 30 dnů. Posledním požadavkem pana Opatrného je možnost přístupu na záznamové zařízení přes počítačovou síť a Internet. Ideální by byla kombinace variant přístupu pomocí software, webového rozhraní a mobilního telefonu (iPhone 4).

### Shrnutí požadavků

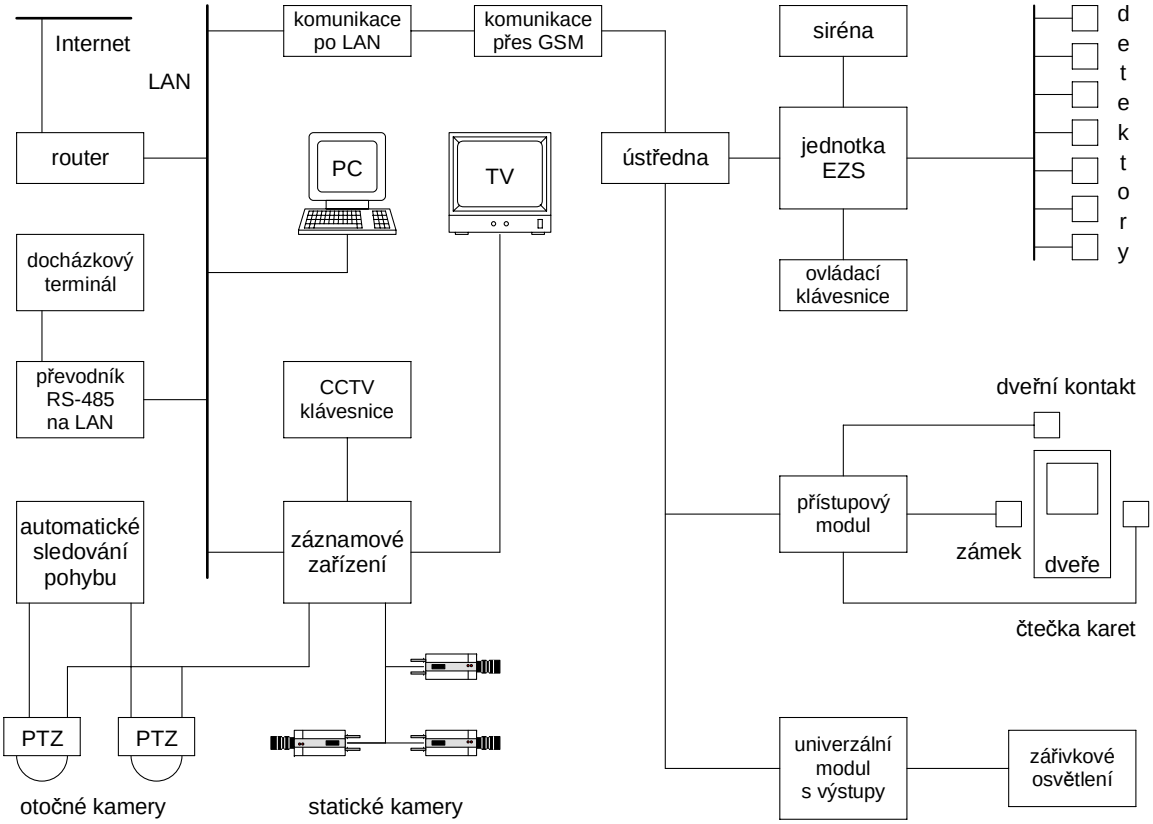
Smyšlený zákazník pan Opatrný jasně specifikoval požadavky kladené na zabezpečovací systém. V podstatě poptává kombinaci systémů EZS, ACS, docházkového systému a kamerového (CCTV) systému s automatickým sledováním pohybu. Pro přehlednost následuje stručná rekapitulace těchto požadavků:

- **Požadavky na zabezpečovací a přístupový systém (EZS a ACS)**
  - 2 - podlažní budova s prostory k pronájmu, potřeba použití mnoha podsystémů,
  - obvodová ochrana netřeba,
  - přenos poplachové informace po GSM síti,
  - možnost snadného budoucího rozšíření systému,
  - cca 30 zaměstnanců (PIN kód, přístupová karta), skupiny s rozdílnými právy,
  - u většiny dveří umístěna čtečka karet či klávesnice pro jejich otevírání,
  - docházkový systém (čtečka umístěná u hlavního vchodu),
  - snadný způsob přidávání a změn uživatelských účtů,
  - čipové karty pro návštěvníky a hosty (mají definovány základní práva),
  - spravování zabezpečovacího systému a uživatelských účtů po LAN,
  - využití PIR čidel pro spínání světel na chodbě.
- **Požadavky na kamerový systém (CCTV)**
  - 8 - 16 barevných kamer s IR přísvitem, většina ve vnitřním provedení,
  - několik přehledových kamer ve venkovním provedení,
  - na rozích budovy 4 otočné (PTZ) kamery,
  - schopnost automatického sledování pohybu,
  - možnost ovládání PTZ kamer z klávesnice,
  - digitální záznamové zařízení a monitor,
  - doba záznamu obrazu (bez zvuku) alespoň 30 dnů,
  - přístup přes LAN a Internet (software, webové rozhraní, sw pro mobilní telefon).

## 6.2 Blokové schéma specifikovaného SZSOP

Na základě požadavků specifikovaných zákazníkem je vytvořeno následující blokové schéma systému pro zabezpečení a střežení objektu a jeho okolních prostor.

Blokové schéma je znázorněno na obr. 6.1. Zde se patří podotknout, že čáry naznačují pouze tok informací a nikoli skutečné fyzické propojení jednotlivých komponent.




Obrázek 6.1: Blokové schéma specifikovaného SZSOP

## 6.3 Volba prostředků pro realizaci

Podrobný rozbor specifikovaných požadavků a volba prostředků pro realizaci bude provedena v následující kapitole.

Pro zajímavost je uveden přehled komponent, které mají ke specifikaci nejblíže a tak budou pravděpodobně použity:

**Pro elektronický zabezpečovací systém (EZS)** a přístupový systém (ACS) bude nejspíše použita ústředna `Concept 3000`, respektive její vylepšená verze `Concept 4000 ACCES`. Výhodou je obrovská modularita, snadné rozšiřování systému a snadné přidávání nových uživatelů. Tento systém umožňuje vytvářet velké množství podsystémů (až 250) a rovněž počet uživatelů může být poměrně vysoký (až 4000). Dále budou voleny takové komponenty systému `Concept`, které zajistí splnění všech požadavků.

**Docházkový systém** – bude pravděpodobně navržen jako řešení výrobce `ACS-line`, které je použitelné v součinnosti s přístupovým systémem a nabízí velké množství podrobných výstupů.

**Kamerový systém** – bude realizován sestavou kamer různých výrobců a digitálním záznamovým zařízením (DVR) výrobce `Pinetron`. Konkrétní modelová řada bude zvolena až při návrhu. Dále budou použity prvky umožňující automatické sledování pohybu. Zvolené řešení by mělo opět splňovat všechny požadavky specifikované zákazníkem.

## 6.4 Volba částí SZSOP které budou realizovány

Volba částí SZSOP jež budou následně realizovány je limitovaná možnostmi zapůjčení potřebných komponent. V tomto jsem však již podnikl všechny potřebné kroky a zapůjčení stěžejních prvků systému mám přislíbeno.

Snahou je realizovat pro demonstrační účely funkční prototyp zabezpečovacího a přístupového systému obsahujícího alespoň několik detektorů, čtečku karet a prvky docházkového systému.

Kamerový systém bude pro demonstrační účely realizován v celé míře, jen s omezeným počtem kamer. Prvky pro automatické sledování pohybujícího se objektu budou rovněž zahrnuty.

# Kapitola 7

# Návrh zabezpečovacího systému

Tato kapitola se zabývá kompletním návrhem systému SZSOP a volbou jeho dílčích komponent. Ty jsou vybírány s ohledem na požadavky plynoucí ze zadání diplomové práce a ze specifikace provedené v kapitole 6.

## 7.1 Analýza požadavků na zabezpečovací/přístupový systém

Podstatná část navrhovaného SZSOP bude tvořena zabezpečovacím (EZS) a přístupovým (ACS) systémem. Zvolený systém musí zajistit splnění minimálně všech těchto kritérií:

- Potřeba použití mnoha podsystémů,
- u většiny dveří umístěna čtečka karet či klávesnice pro jejich otevírání,
- přenos poplachové informace po GSM síti,
- možnost snadného budoucího rozšíření systému,
- cca 30 zaměstnanců (PIN kód, přístupová karta), skupiny s rozdílnými právy,
- snadný způsob přidávání a změn uživatelských účtů,
- čipové karty pro návštěvníky a hosty (mají definovány základní práva),
- spravování zabezpečovacího systému a uživatelských účtů po LAN,
- využití PIR čidel pro spínání světel na chodbě.

### 7.1.1 Ústředna zabezpečovacího (EZS) a přístupového (ACS) systému

Jádro zabezpečovacího systému představuje ústředna, proto je třeba jejímu výběru věnovat velkou pozornost. V tomto konkrétním případě volbu ústředny nejvíce ovlivní tato kritéria:

**Použití mnoha podsystémů:** Většina zabezpečovacích ústředen na trhu umožňuje rozdělení na 2 až 8 podsystémů. Jelikož v objektu, pro nějž je systém navrhován, se počítá s pronájmem volných kanceláří, mohla by být tato hodnota brzy limitující. Z tohoto důvodu je třeba vybrat ústřednu, která umožní rozdělení na více jak 8 podsystémů.

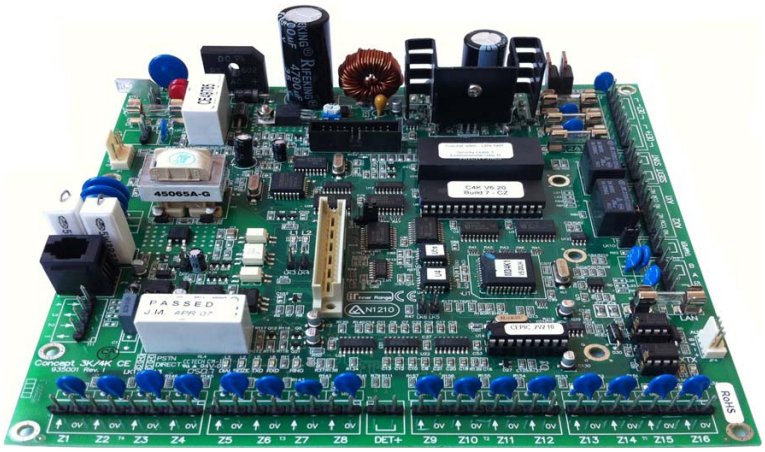
**Mnoho přístupových čteček:** Je třeba brát na vědomí, že ne všechny ústředny umožňují připojení čteček. Pokud umožňují, bývá jejich počet většinou omezen na 32. To by znamenalo kontrolu nad 16-ti dveřmi (dvě čtečky na jedny dveře, každá pro jeden směr), což by v našem případě stačilo.

**Snadné rozšíření systému:** U smyčkových ústředen nebývá pozdější rozšiřování systému nikterak snadné a někdy ani možné. Mnohdy potom nemusí dostačovat například počet zón a je tak nutné měnit velkou část systému. Pro splnění požadavku na snadnost budoucího rozšiřování je tedy lépe volit ústřednu sběrnicového nebo koncentrátorového typu (popis rozdílů viz kapitola 5.1.5).

**Jednoduchý způsob přidávání a změn uživatelských účtů:** V některých zabezpečovacích systémech lze přidávat či měnit uživatelské kódy jen pomocí klávesnice. V případě potřeby častých změn není toto řešení vhodné a je užitečnější použít takovou ústřednu, která umožňuje spravovat uživatelské účty pomocí počítače.

**Nároky na automatizaci:** Pro automatizaci mnohých činností v objektech se většinou používají nejrůznější specializované systémy. Trendem poslední doby je však přidávat část těchto funkcí i do systémů EZS. Ústředny jsou často vybaveny reléovými výstupy a umožňují připojení nejrůznějších snímačů (teploty, hladiny vody, apod.). Jelikož jedním z požadavků na navrhovaný systém je spínání světel při pohybu na chodbě (v nastavitelnou večerní dobu), bude třeba se při výběru vhodného typu ústředny zaměřit i na její schopnosti automatizace.

Na základě výše uvedeného rozboru a po pečlivém zvážení všech požadavků *se jako nejvhodnější jeví použití zabezpečovacího a přístupového systému* `Concept 4000` od australské společnosti `Inner Range`. Konkrétně bude použita ústředna `Concept IRC4000 EU`, která v sobě kombinuje prvky *zabezpečovacího (EZS)* a *přístupového (ACS)* systému.



Obrázek 7.1: Ústředna zabezpečovacího a přístupového systému Concept 4000

`IRC4000 EU` je ústředna koncentrátorového typu umožňující sestavení modulárního systému pro správu a zabezpečení budov a pro řízení přístupu osob.

Celkový *počet připojitelných modulů je až 250*, přičemž maximálně *99* jich může být *stejného typu*. Díky tomu lze realizovat systém obsahující až *250 nezávislých podsystémů* s celkovým počtem *2000 zón (detektorů)*. Pomocí velkého množství klávesnic a čteček (dle použitých modulů řádově stovky) lze oboustranně řídit přístup až do *250 dveří*. *Počet uživatel* systému `Concept 4000` může být *až 50 000* (z toho 4 000 s PINem, ostatní s čipovou kartou či přívěškem). *Uživatelské účty* s příslušnými oprávněními lze snadno *vytvářet či měnit z počítače* pomocí dodávaného software. Z hlediska automatizace a správy budov nechybí možnosti od *měření teploty* a *spínání* nejrůznějších zařízení až po *řízení výtahů* [11].

### 7.1.2 Návrh komponent systému Concept 4000

Jak již bylo uvedeno, systém `Concept 4000` je velice modulární a umožňuje tak uspokojit nejrůznější nároky kladené na zabezpečovací a přístupový systém.

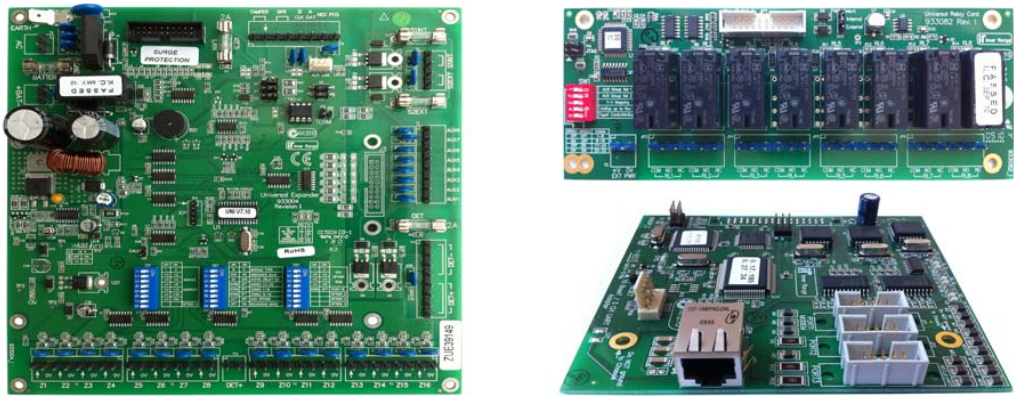
Splnění většiny požadavků ze specifikace zajistí samotná ústředna. Pro realizaci ostatních je však třeba provést výběr vhodných komponent (modulů). Zejména je nutné dodržet minimální počty podsystémů, zón a ovládaných dveří. Dále musí být přidána schopnost přenosu poplachové informace po GSM síti a využití PIR čidel pro spínání světel na chodbě. Do volby vhodných modulů musí být rovněž zahrnuty i požadavky na snadnost přidávání či změny uživatelských účtů.

Následuje přehled zvolených komponent se stručným popisem jejich činnosti a se zdůvodněním výběru. Veškeré informace byly čerpány z webu [34] a materiálů výrobce [11].

**Univerzální expandér IRZ3004 EU EXP/16:** K ústředně `IRC4000 EU` je možné připojit 16 zón (detektorů). Tento počet zhruba vystačí na zabezpečení jednoho patra budovy menší firmy. Proto je třeba navíc použít i tento rozšiřující modul (expandér), ke kterému lze připojit dalších 16 detektorů, 2 sirény a 8 reléových výstupů. Maximálně může být připojeno až 99 těchto expandérů. V našem případě však postačí jeden, který bude sloužit pro zabezpečení, kontrolu přístupů a ovládání světel ve druhém patře budovy (ústředna zajistí tyto funkce v prvním nadzemním podlaží).

**Univerzální expandér IRZR3082-C:** Tato verze se připojuje datovým kabelem přímo k ústředně (existuje i verze pro připojení k univerzálním expandérům). Slouží pro rozšíření systému o 8 releových výstupů (250 V / 5 A) umožňujících spínání libovolných zařízení (klimatizace, zámky dveří, osvětlení, apod.). V tomto případě poslouží pro ovládání zářivkového osvětlení v prvním nadzemním podlaží budovy.

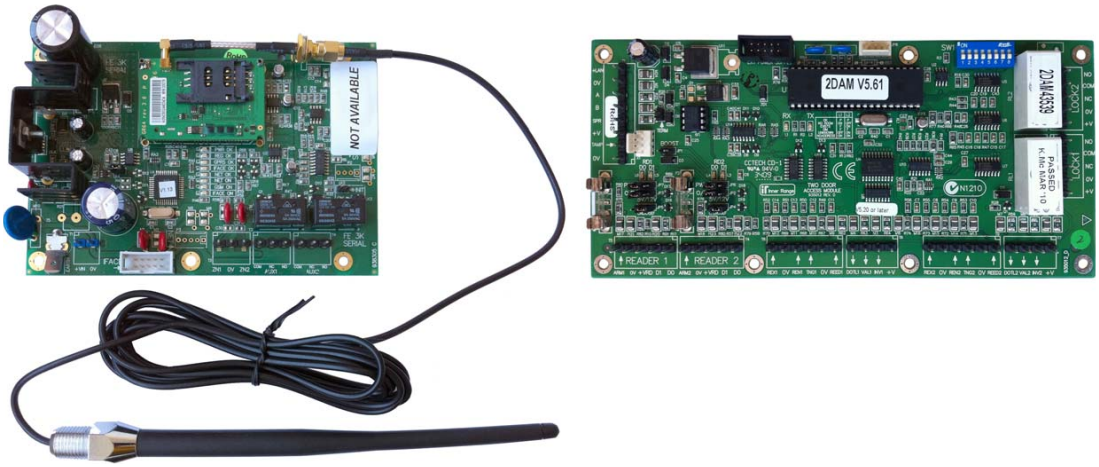
**Komunikační deska IRPX13BaseT (1x LAN a 3x RS-232):** Pomocí zabudovaného konektoru se připojí přímo k ústředně, kterou tak rozšíří o 3 porty sériového rozhraní RS-232 a jeden ethernetový port. Přes sériové rozhraní lze provádět komunikaci s počítačem, nebo připojovat další periferie. V našem případě bude jeden sériový port použit pro komunikaci s GSM modulem a ethernetové rozhraní zajistí propojení ústředny do místní počítačové sítě LAN. Jedná se tedy o důležitou komponentu z hlediska požadavků na zasílání informací přes GSM sít a na snadnou správu uživatelských účtů.



Obrázek 7.2: Rozšiřující desky systému Concept (v pořadí dle popisu)

**GSM modul FE3000-S:** Slouží jako komunikační rozhraní mezi ústřednou a mobilními telefony až 32 uživatelů. Umožňuje zasílání krátkých textových zpráv (SMS) s informací o nastalém poplachu. Pomocí příkazů ve formě SMS zpráv z definovaných telefonních čísel je navíc možné celý systém kompletně ovládat. GSM modul komunikuje s ústřednou prostřednictvím sériového rozhraní na desce `IRPX13BaseT`.

**Přístupový modul pro dvoje dveře IRR3000:** Zajišťuje kompletní řízení jednostranného přístupu ke dvěma dveřím, případně oboustranného přístupu k jedněm dveřím. K modulu lze tedy připojit dvě čtečky přístupových karet a přívěšků. Dále jsou na něm umístěna relé pro spínání elektrických dveřních zámků a výstupy pro signalizační LED či bzučáky. Prostřednictvím dveřních kontaktů lze v případě potřeby rozeznávat stav zda jsou dveře otevřeny či zavřeny a zda například nedošlo k jejich násilnému otevření. V našem případě bude tento modul pracovat v režimu oboustranného řízení dveří na základě jasně daných přístupových práv pro jednotlivé uživatele.




Obrázek 7.3: GSM modul FE3000 S a přístupový modul pro dvoje dveře IRR3000

**LCD klávesnice IRT3000-E:** Slouží pro programování i kompletní obsluhu zabezpečovacího a přístupového systému `Concept`. Je vybavena zeleně podsvíceným monochromatickým LCD displejem a dvaceti tlačítky. Maximální povolený počet klávesnic v jednom systému je 99, což je v našem případě více než dostačující a klávesnice tak mohou být umístěny na všech užitečných místech (zpravidla vstupně-výstupní cesty do klíčových prostor/podsystémů v objektu).

**Čtečka Inner Range Dual-Format Proximity Reader:** Jedná se o dvou formátovou čtečku Proximity karet a čipů. Konkrétně jsou podporovány formáty *Inner Range Secure 40*, *HID* (125 kHz FSK Proximity formát 26 - 40 bitů) a *EM Marine* (125 kHz ASK) [10]. Čtečka je kompaktních rozměrů a se slušným čtecím dosahem (do 150 mm). Díky rozsahu pracovních teplot od –35 °C do +65 °C a kvalitní konstrukci je vhodná i pro použití do venkovních prostor. Propojení s přístupovým modulem pro dvoje (`IRR3000`) nebo jedny (`IRR3000/1`) dveře je realizováno pomocí rozhraní Wiegand. Následná komunikace pak probíhá pomocí stejnojmenného komunikačního protokolu (podrobnější popis rozhraní a protokolu Wiegand bude proveden v kapitole 7.2).

**Přístupová média - karty a čipy HID:** Uživatelé zabezpečovacího a přístupového systému `Concept`, mající příslušná oprávnění, mohou do jednotlivých prostor (podsystémů) přistupovat pomocí zadání PINu na klávesnici. Druhou možností je přiložení bezkontaktní přístupové karty nebo čipu ke čtečce. V našem konkrétním případě se počítá s využitím čipů a karet `HID ProxCard II` [10].


Obrázek 7.4: LCD klávesnice IRT3000 E a čtečka s kartou HID ProxCard II

### 7.1.3 Detektory a ostatní prvky zabezpečovacího systému

Aby byl zabezpečovací systém navržen kompletně, zbývá ještě zvolit vhodné detektory, a další drobné, ale o to více potřebné komponenty.

Výrobce zabezpečovacího a docházkového systému `Concept` (společnost `Inner Range`) detektory ani jiné doplňkové periferie (sirény, akumulátory) nedodává. Celý systém je naopak navržen tak, aby nebyl problém použít komponenty jiných, v dané oblasti zkušenějších, výrobců. Pro navrhovaný SZSOP se jako vhodné jeví následující detektory a komponenty.

**PIR detektor PARADOX 476 Pro:** Je velice odolný proti vysokofrekvenčnímu rušení a falešným detekcím. Součástí je i ochranný kontakt (takzvaný *tamper*) pro rozpoznání nežádoucího otevření. Dosah detektoru je 11 metrů při montážní výšce 2,5 m. Rozsah možných rychlostí pobybujícího se objektu je 0,2 - 7 metrů za sekundu.

**Stropní PIR detektor PARADOX DG466 Paradome:** Jedná se o stropní detektor se schopností určení směru pohybu (díky dvěma zabudovaným PIR senzorům). Je tak vhodný pro případy, kdy chceme zastřežit prostor s otevřenými dveřmi. Tedy například balkón, kdy zevnitř ven a zase zpět je možné projít bez narušení, naopak je vyvolán poplach. Detektor lze navíc použít i v klasickém režimu. Doporučená montážní výška je 2,1 - 3,6 metrů a detekce je zaručena při rychlostech pohybujícího se objektu v rozsahu 0,2 - 3,5 metrů za sekundu.

**Dveřní PIR záclona PARADOX 460 Paradoor:** Je detektor s detekční charakteristikou typu záclona (více viz kapitola 5.1.2). Používá se pro signalizaci otevření oken a dveří, případně i pro ochranu uměleckých děl (například detekce pohybu před obrazem na zdi). Díky automatické teplotní kompenzaci má konstantní citlivost a velkou odolnost proti rušení. Instalační výška by pro přístupové aplikace (monitorování dveří) měla být 2 - 2,7 m. Pro bezpečnostní aplikace (střežení uměleckých děl) pak dle potřeby může být až 6 m (při větší výšce je zabírána větší plocha, ale s menší citlivostí).

**Magnetický dveřní kontakt SA-200A:** Jedná se o plastový magnetický rezpínací kontakt se svorkovnicí pro připojení kabelů z ústředny. Je určený pro povrchovou montáž jak na vodivé, tak i nevodivé materiály. K rozepnutí magnetického kontaktu dojde při oddálení obou částí na vzdálenost větší než 20 milimetrů (tato mezera se nazývá takzvaná *detekční vzdálenost*).

Obrázek 7.5: Zvolené detektory (v pořadí dle popisu v textu)

**Venkovní zálohovaná siréna PARADOX PS-128:** Jedná se o odolnou sirénu určenou pro akustickou a optickou signalizaci poplachu (narušení objektu). Velice efektivní reproduktor o akustickém výkonu 40 W vydává pronikavý zvuk o frekvenci 900 - 2400 Hz a intenzitě až 128 decibelů. Pod krytem z plastu se nachází odolná železná konstrukce bránící snadném zneškodnění. Siréna je napájena napětím 12 V DC a pro případ výpadku napájení je vybavena vlastním akumulátorem.

**Vnitřní siréna Jablotron SA-913F:** Je nezálohovaná plastová siréna pro vnitřní použití vybavená LED majákem a vydávající zvuk o intenzitě až 104 decibelů.

**Transformátor TRN16/30 JBC-E20302-038:** O napájení všech modulů a periferií zabezpečovacího a přístupového systému `Concept` se stará ústředna (v případně rozsáhlé instalace navíc i podpůrné napájecí zdroje). Ústřednu je třeba napájet střídavým napětím 16 V. Pro tento účel bude použit jednofázový transformátor 230 V / 16 V o výkonu 30 VA. Jedná se o pasivně chlazený transformátor uzpůsobený pro nepřetržitý provoz. Jako ochranný prvek je použita tavná trubičková pojistka.

**Akumulátor Alarmguard CJ12-18 (12V/18Ah):** Jedná se o bezúdržbový uzavřený akumulátor určený pro zálohu zabezpečovacího systému po dobu výpadku napájení.


Obrázek 7.6: Zvolené sirény, transformátor a záložní akumulátor (v pořadí dle popisu)

## 7.2 Evidence docházky

Další část požadovaného zabezpečovacího systému bude tvořena podsystémem evidence docházky zaměstnanců. Měl by splňovat tyto požadavky:

- Pro evidenci docházky poslouží čtečka u hlavního vchodu,
- export přehledných měsíčních výpisů.

Z důvodu integrace do celkového SZSOP je však třeba navrhnout takové komponenty, které budou nejen splňovat potřebná kritéria, ale zároveň budou kompatibilní i se zabezpečovacím a přístupovým systémem `Inner Range Concept 4000`.

**Docházkový terminál ACS-line RT-300W:** Jedná se o poměrně rozšířený terminál pro evidenci docházky a kontrolu přístupu. V tomto případě je jeho umístění situováno do prostoru hlavního vchodu do budovy a slouží čistě pro hlídání docházky. Ve vnitřní paměti může (*off-line*) uchovávat mnoho událostí jako je příchod, odchod, přestávka, služební cesta apod. Tato data jsou jednou za určitý čas načtena do počítače pomocí dodaného software. Pro komunikaci slouží průmyslová sériová sběrnice RS-485. Terminál `RT-300W` sám o sobě neobsahuje žádnou čtečku. Tu je nutné připojit přes vnitřní *rozhraní Wiegand* [1], přičemž podporovány jsou všechny čtečky umožňující komunikaci přes *komunikační protokol Wiegand* [2].

**Čtečka Inner Range Dual-Format Proximity Reader:** Jedná se o shodnou čtečku která je již popsána v kapitole 7.1.2. Jelikož obsahuje rozhraní *Wiegand* a podporuje stejnojmenný komunikační protokol, lze ji snadno propojit s docházkovým terminálem `ACS-line RT-300W`.

**Přístupová média - karty a čipy HID:** Jako přístupová média budou v navrhovaném systému použity *bezkontaktní přívěšky a karty HID* (125 kHz Proximity, formát FSK, 26 - 40 bitů) a *EM Marine* (125 kHz, formát ASK) [10].


Obrázek 7.7: Navržený docházkový terminál, čtečka, přívěšek a karta

[1] Rozhraní Wiegand – je realizováno třemi vodiči. Dva jsou datové (Data 0, Data 1) a jeden představuje zem (GND). Na datových vodičích je v klidu napěťová úroveň 5 V (tedy logická 1) [5].

[2] Komunikační protokol Wiegand – je založen na sekvenčním přenosu jednotlivých bitů s jednoduchou časovou synchronizací. Komunikace se provádí pomocí impulsů na datových vodičích. Je-li třeba zaslat hodnotu logická 1, je na vodič data 1 generován puls trvající 50 $\mu$s (puls představuje hodnota logická 0). Při přenosu logické 0 je vyslán puls na vodič data 0. Prodleva mezi komunikačními impulsy je 2 ms [5].

### Převodník e-NET E-P132-X

Slouží pro přenos sběrnic RS-485/422/232 po Ethernetu (10/100BaseTX). Díky tomu je možné k libovolnému zařízení se sériovým rozhraním RS-485/422/232 přistupovat po síti LAN či z Internetu. Na klientském PC je možné nainstalovat virtuální sériový port a komunikace se vzdáleným sériovým zařízením pak bude probíhat úplně stejně, jako by byla prováděna lokálně. V navrhovaném systému evidence docházky tento převodník poslouží pro propojení terminálu `RT-300W` (majícího sériové rozhraní RS-485) s počítačem, na kterém bude nainstalována aplikace pro evidenci docházky.

Na zařízení se nachází konektor `Cannon 9 pin D-Sub` pro rozhraní RS-232, svorkovnice pro připojení průmyslové sériové sběrnice RS-485/RS-422, síťový konektor RJ-45, konektor pro napájení (9 - 12 V DC) a LED diody pro indikaci stavu. Převodník je osazen 32-bitovým procesorem ARM-7 s pracovní frekvencí 33 MHz a 2 MB paměti RAM. Podporuje režimy TCP server/klient, UDP klient a protokoly ARP, IP, ICMP, HTTP a DHCP [34].


Obrázek 7.8: Pohled na odkrytovaný převodník e-NET E-P132-X

### Docházkový software ADS 4

Pro zpracování údajů o docházce z terminálu `RT-300W` poslouží software `Docházka 4` od společnosti `RON Software` (dále v textu uváděný pod označením `ADS 4`).

Jedná se o placenou aplikaci určenou pro OS Microsoft® Windows® umožňující konfiguraci a následné načítání dat z docházkových terminálů. Komunikace s nimi probíhá přes LAN, přičemž v našem případě je třeba ještě zařadit převodník LAN → RS-485/422/232 (viz kapitola 7.2). Načtená data jsou uložena do databáze na lokálním serveru (podporovány jsou například Microsoft SQL, Oracle, MSDE, Sybase) a poté dále zpracovávána. Dlužno podotknout, že komunikace s terminály neprobíhá neustále, ale údaje z jejich paměti jsou načítány jen při požadavku obsluhy. V případě potřeby je však možné k software dokoupit modul s názvem „Služba“, který pracuje na pozadí OS a zajišťuje periodické načítání dat z terminálů v nastavitelných intervalech a případné další plánované činnosti.

Data načtená z terminálů jsou v software `ADS 4` zobrazována v přehledném grafickém rozhraní. Jejich vyhodnocení může probíhat po libovolných intervalech, avšak nejčastěji užívané období je jeden měsíc. Uživatelé mající příslušná oprávnění mohou automaticky zpracovanou docházku dále ručně editovat a upravovat. Takto je možné přidávat například události, které zaměstnanec zapomněl (odchod k lékaři), nebo nemohl (náhlá nemoc) na terminálu zadat. Editovat je možné i časy příchodů a odchodů, přičemž původní data z terminálů zůstávají v databázi zachována. Veškeré prováděné změny jsou graficky odlišeny a u každé takové úpravy je navíc evidováno jméno uživatele, který ji provedl.

Každý zaměstnanec má přidělen model pracovní doby (například ranní 8 hod. směna, noční 12 hod. směna). Program umožňuje automatické počítání přesčasů a příplatků za víkendy, svátky či noční směny. Oprávněná osoba má poté možnost rozhodnout, zda a kolik přesčasů bude proplaceno, převedeno do dalšího měsíce, či ignorováno.

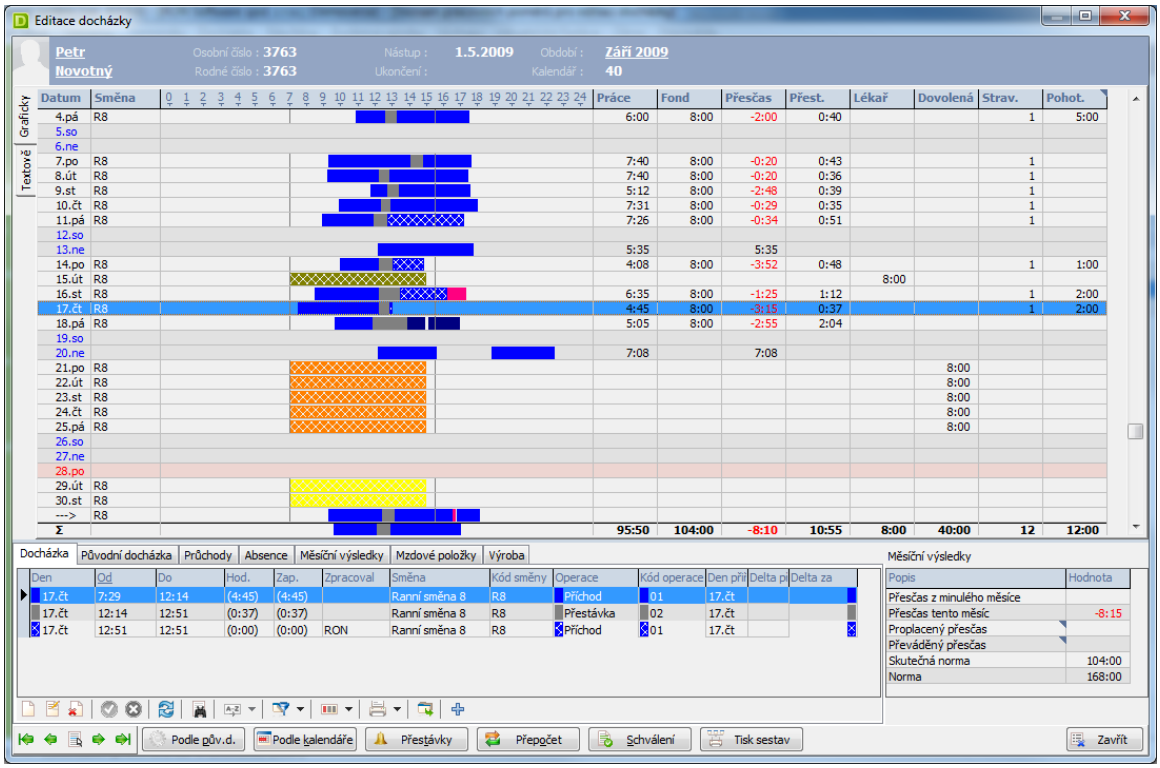
Užitečnou funkcí je export dat do mnoha mzdových a personálních systémů. Nechybí ani možnost tisku velkého množství vlastních nebo předdefinovaných výstupních sestav. Těmi jsou například: seznam zaměstnanců s rozdělením, měsíční rozpis docházky, grafický výkaz odpracovaných směn a přehled časových složek mzdy [25].

### Použité rozšiřující moduly software ADS 4

Jedním z požadavků na navrhovaný SZSOP je přístup přes webové rozhraní. Aby toto bylo splněno i u docházkového systému, je potřeba použít jistého rozšíření software `ADS 4`. Dostupných modulů je více, ale pro navrhovaný systém jsou podstatné jen tyto:

**Intraweb:** Jedná se o webovou aplikaci, nebo-li tenkého klienta. Pomocí internetového prohlížeče lze přistupovat k údajům v databázi a dle přidělených oprávnění nad nimi provádět nejrůznější operace. Takto je možné například sledovat docházku zaměstnanců, prohlížet denní a měsíční přehledy, plánovat směny či dovolenou a vykonávat spoustu dalších užitečných činností.

**Služba:** Pracuje na pozadí operačního systému jako systémová služba a slouží k automatickému spouštění naplánovaných úloh. V našem případě zajistí periodické načítání dat z docházkového terminálu a následné zpracování docházky.




Obrázek 7.9: Ukázka vzhledu software Docházka 4 (ADS 4) (převzato z [25])

## 7.3 Návrh kamerového systému

Další podstatnou část zabezpečovacího systému bude tvořit kamerový systém CCTV se schopností automatického sledování pohybu zvolenými kamerami. Navrhovaný systém musí splňovat následující podmínky:

- 8 - 16 barevných kamer s IR přísvitem - vnitřní i vnější,
- 4 otočné (PTZ) kamery zajišťující automatické sledování pohybu,
- digitální záznamové zařízení uchovávající záznam alespoň 30 dnů,
- klávesnice pro ovládání PTZ kamer,
- přístup přes LAN a Internet.

### 7.3.1 Volba mezi analogovým či IP kamerovým systémem

Před samotným návrhem kamerového systému je třeba učinit rozhodnutí, zda bude CCTV systém sestaven z analogových či IP kamer. Pro IP kamery hovoří vyšší kvalita obrazu a snadnost instalace. Proti nim je pak cena, a co je zásadní, tak i legislativa. Dle vyjádření Asociace technických bezpečnostních služeb Gremium Alarm nelze kamerový systém sestavený čistě z IP kamer považovat za plnohodnotný kamerový systém z hlediska požadavků pojišťoven. Národní bezpečnostní úřad (NBÚ) totiž pro IP kamery zásadně nevydává certifikaci, která by zajistila realizaci CCTV systému v požadovaném stupni zabezpečení chráněného objektu (viz kapitola 3.4.4).

Z přihlédnutím k těmto faktům bude kamerový systém navržen a následně realizován za použití analogových kamer a příslušného záznamového zařízení.

### 7.3.2 Výběr kamer

Výběru kamer je třeba věnovat zvláštní pozornost, protože jejich špatná volba může poměrně značně degradovat celkovou kvalitu kamerového systému.

Na základě požadavků zákazníka bude pro vnitřní prostory použito 5 stropních („Dome“) kamer a 5 boxových kamer s varifokálním objektivem (umožňuje manuální změnu ohniska při instalaci). Pro monitorování vchodu do objektu a parkoviště pak poslouží 2 venkovní kamery s IR přísvitem. Na rozích budovy budou dále umístěny 4 otočné (PTZ) kamery, které bude obsluha moci ovládat z klávesnice a zároveň budou řízeny moduly pro automatické sledování objektu.

**Kamera LG L332-BP:** Je barevná kamera s automatickým přepínáním režimů den/noc určená do vnitřních prostor. Díky modernímu DSP procesoru (výrobce ho označuje `XDI II`) dosahuje rozlišovací schopnosti až 650 televizních řádků a přestože není vybavena IR přísvitem je schopna snímat obraz už při osvětlení o intenzitě od 0,00003 lux. Nechybí ani pokročilá digitální redukce šumu v obraze a kompenzace protisvětla[3]. Na těle kamery je závit (typu CS-mount) pro uchycení objektivu. Napájecí napětí může být 12 V DC nebo 24 V AC.

[3] BLC – (Back Light Compensation) neboli kompenzace protisvětla je funkce kamer, která eliminuje silné světlo v zadní části záběru. Bez přítomnosti této funkce by např. osoba stojící proti oknu byla příliš tmavá. Vylepšené varianty této funkce se někdy označují jako WDR, či HSBLC.

**Objektiv Computar TG4Z-2813-IR:** Je varifokální objektiv (s manuálně měnitelnou ohniskovou vzdáleností) a automatickým řízením clony (DC Auto Iris). Ohniskovou vzdálenost je možno plynule měnit v rozsahu 2,8 - 12 mm, což při rozměru CCD snímače 1/3 "představuje zorné pole o úhlu 23 ° až 82 °. Díky zabudovanému IR filtru je možné jej použít i s kamerami umožňujícími automatické přepínání režimu den/noc [4]. Závit je typu CS-mount a objektiv je tedy bez problémů kompatibilní s kamerou `LG L332-BP`.

**Stropní kamera LG L6323-BP:** Má prakticky totožné parametry s výše uvedenou kamerou `LG L332-BP`. Liší se jen vzhled a provedení, které je uzpůsobeno pro stropní montáž.

**Venkovní kamera KT&C KPC-N680QPH:** Jedná se o masivní venkovní kameru se stupněm krytí IP67. Zobrazovací jednotka je tvořena 1/3 "barevným CCD čipem `Sony` s rozlišovací schopností 550 televizních řádků. Součástí odolného kompaktního krytu je varifokální objektiv s plynule měnitelnou ohniskovou vzdáleností $f = 2,8 - 12$ mm. Okolo něj se nachází 35 IR LED (vlnové délky 850 nm) zajišťujících dosvit až na vzdálenost 40 m. Díky tomu je kamera schopna pracovat i za naprosté tmy. Přepínání mezi režimy den/noc se děje automaticky. Nechybí ani běžné funkce jako je kompenzace protisvětla (BLC, WDR), vyvážení bílé barvy (AWB) a automatické řízení úrovně videosignálu (AGC). Napájecí napětí je 12 V DC, proudový odběr zhruba 650 mA a doporučený rozsah pracovních teplot -10 °C až +50 °C.

**Venkovní PTZ kamera LG LT903PB:** Je venkovní otočná PTZ kamera v odolném plechovém krytu. Optická část je tvořena CCD čipem velikosti 1/4 "s rozlišovací schopností 540 TV řádků. Kamera je vybavena motorovou optikou s 37-mi násobným optickým zoomem umožňující plynulou změnu ohniskové vzdálenosti v rozsahu $f = 3,5 - 129$ mm. Díky pokročilému DSP procesoru může pracovat i za velmi špatných světelných podmínek (od 0,0001 lux) i bez přítomnosti IR přísvitu. Režim den/noc je přepínán automaticky na základě vyhodnocení intenzity světla ve snímané scéně. Modul optiky umožňuje otáčení o 360 ° v horizontálním směru a o 180 ° ve vertikálním. Jako komunikační rozhraní je použita sériová linka RS-485, přičemž kamera podporuje komunikační protokoly Pelco D, Pelco P a LG Multix. Vnitřní paměť postačuje na uložení až 128-mi prepozic. Mimo BNC konektor video-výstupu je přítomno ještě 8 alarmových vstupů a 4 alarmové výstupy. Napájecí napětí je 24 V AC, spotřeba energie do 20 W a rozsah pracovních teplot je díky integrovanému vyhřívání -25 °C až +55 °C. Pro montáž na zeď se používá držák s označením `LSO-101WA`.

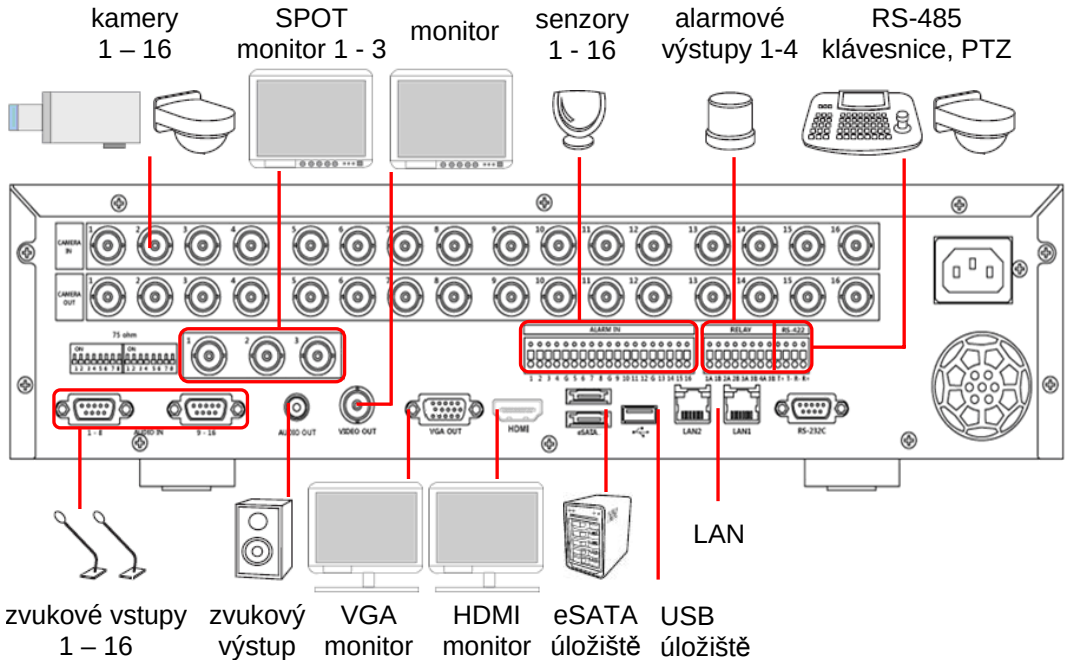
Obrázek 7.10: Zvolené kamery (v pořadí dle popisu)

[4] Pokud by se u takové kamery použil objektiv bez IR filtru, obraz by byl při snímání v nočním režimu rozmazaný. To je dáno jinou vlnovou délkou denního a IR světla.

### 7.3.3 Digitální záznamové zařízení (DVR)

Hlavní prvek kamerového systému představuje digitální záznamové zařízení, neboli DVR (viz kapitola 5.3). To umožňuje živé prohlížení obrazu z kamer a pořizování, přehrávání, či export záznamů. Ovládání je možné přímo prostřednictvím tlačítek na čelním panelu, dálkovým ovladačem nebo pomocí myši připojené v předním USB portu. Díky přítomnosti LAN rozhraní je možná i obsluha z počítače vybaveného příslušným softwarem.

Pro navrhovaný kamerový systém se jako nejvhodnější volba jeví použití rekordéru `Pinetron PDR-X7016`. Jedná se o kvadruplexní (umožňuje současně živé zobrazení, přehrávání záznamů, export záznamů a připojení po LAN) zařízení se 16 video a 16 audio vstupy. Dále obsahuje rozhraní pro připojení až 16 senzorů (např. PIR detektorů), 4 alarmové výstupy (např. pro bzučáky), sériové rozhraní RS-485 pro připojení klávesnice a PTZ kamer, 2 ethernetové konektory RJ-45 pro připojení do LAN, USB 2.0 a eSATA. Dále je zde zvukový výstup a konektory BNC, VGA a HDMI pro výstup na příslušné monitory. Specialitou jsou pak další 3 BNC konektory pro připojení takzvaných SPOT monitorů.




Obrázek 7.11: Možnosti zapojení DVR zařízení Pinetron PDR-X7016

Na zařízení běží *real-time operační systém* (RTOS) unixového typu. Záznamy mohou být ukládány až na 4 interní 3.5"pevné SATA II disky (na 4. konektoru je připojena DVD-RW mechanika, kterou lze odpojit). Přes 2 rozhraní eSATA lze navíc připojit disková pole čítající dalších 10 pevných disků. Celkem je tedy možno pracovat až se 14 pevnými disky o celkové kapacitě až 28 TB. Použitý systém souborů je JFS[5]. Zařízení podporuje práci s disky v režimech RAID 0, kdy dojde k jejich zřetězení (linear) a RAID 1, kdy se vždy na 2 disky zrcadlí stejná data pro jejich větší bezpečnost (mirroring).

[5] JFS – je žurnálovací 64-bitový souborový systém (file system). Vyvinula jej počátkem 90. let firma IBM a je šířen pod licencí GPL. Jelikož byl navržen pro použití na serverech, je vysoce spolehlivý a výkonný z hlediska propustnosti dat [33].

Analogový zdroj videa v PAL rozlišení (720x576) je v reálném čase komprimován hardwarovým kodérem s kompresí H.264. Oproti starším typům DVR, které používaly kompresi MPEG-4, je tento kodek zhruba o 1/3 úspornější a na úložný prostor se tak vleze více záznamů. Jen pro zajímavost, pro ukládání zvuku se využívá komprese audiokodekem G.722.

`Pinetron PDR-X7016` je v současnosti (rok 2011) jeden z nejvyšších modelů záznamových zařízení DVR na trhu. Umožňuje současně nahrávat záběry až ze šestnácti kamer se snímkovací frekvencí 25 snímků za sekundu v plném PAL rozlišení (720x576, v CCTV často označováno jako „*full D1 resolution*“). Zvládá tedy komprimovat 400 ($16 \times 25$) video snímků za sekundu v reálném čase! Úroveň kvality komprese a počet snímků za sekundu (*frame rate*) lze nastavit zvlášť pro každý kanál. Zařízení podporuje rovněž nastavení odlišné (zpravidla nižší) kvality videa pro přenos po počítačové síti LAN (výrobce tuto funkci nazývá jako *dual streaming*).

Nahrávání je možné buďto trvale, na základě detekce pohybu v obraze, při sepnutí senzorů připojených na vstupy, či podle plánovacího kalendáře. Velmi užitečná funkce je spínání alarmových výstupů a volitelně k tomu i odesílání e-mailů při nejrůznějších událostech. Těmi mohou být například detekce pohybu, sepnutí alarmového vstupu, ztráta videosignálu a systémové události jako je porucha HDD, přehřívání, porucha větráků apod. Pro případy kdy je třeba opravit chyby nebo přidat nové funkce je dostupná možnost upgrade firmware. To lze provést jak pomocí USB flash disku, tak přes počítačovou síť. Pro vzdálenou správu DVR zařízení přes LAN (potažmo Internet) lze využít webové rozhraní (kvůli použití *ActiveX* je funkční jen v prohlížeči *Internet Explorer*), či software pro PC a mobilní telefony. Podporovány jsou operační systémy *Microsoft Windows* a *MAC OS*. Z mobilních platforem pak *iOS* (Apple), *Android* a *Windows Mobile*.

Nastavení a konfiguraci záznamového zařízení `Pinetron PDR-X7016` lze provádět buďto pomocí tlačítek na čelním panelu, dálkovým ovladačem nebo přes software či webové rozhraní. Většina informací v této kapitole byla čerpána z oficiálního manuálu výrobce [24].

Obrázek 7.12: Digitální videorekordér PDR-X7016 (převzato z [24])

**Pevné disky:** Jako nejvhodnější z hlediska výkonu, spolehlivosti a ceny byly zvoleny 2 TB pevné disky `Western Digital WD20EURS`. Jedná se o 3,5”HDD s rozhraním SATA II určené k nepřetržitému provozu. Dle výrobce jsou přímo určeny pro použití v digitálních videorekordérech. Počet disků bude upřesněn později.

**Diskové pole DAT Optic sBOX-R:** Jedná se o externí box vybavený rozhraním eSATA. Umožňuje tak rychlé připojení až pěti 3,5”pevných disků se SATA II rozhraním. Ty jsou pro lepší chlazení umístěny v hliníkových rámečcích, které navíc monitorují a na displeji zobrazují teplotu a stav příslušného disku.

**Ovládací klávesnice Pinetron PSD-CJ1000:** Slouží k pohodlnému ovládání PTZ kamer a digitálních záznamových zařízení (DVR). Je vybavena konektorem pro připojení ke sběrnici RS-485. Podporuje komunikační protokol Pelco D a Pelco P. Nastavení se provádí přímo tlačítky klávesnice. Pro zobrazení stavových informací slouží velký modře podsvícený display. Napájecí napětí je 12 V DC, přibližný odběr 0,5 A [8].

**Monitor Samsung BX2431:** Je vybaven rozhraním HDMI a lze jej tedy bez problémů propojit se zvoleným záznamovým zařízením. Maximální povolená délka kabelu je 10 m, což bude v našem případě bohatě stačit. Nativní rozlišení monitoru je 1920 x 1080.

Obrázek 7.13: Zvolené periferie pro záznamové zařízení (v pořadí dle popisu)

### 7.3.4 Modul pro automatické sledování pohybu

Jedním z požadavků zákazníka jsou 4 otočné PTZ kamery se schopností automatického sledování pohybu. Nejvhodnějšími kamerami se v tomto případě jeví `LG LPT-LT903PB` (viz kapitola 7.3.2). Tyto kamery samy o sobě pohyb sledovat neumí a pro tuto funkci je tedy CCTV systém třeba doplnit ještě o 4 moduly s označením `MF-AT100`, nebo-li *tracking box*.

*Tracking box* je zařízení sloužící k automatickému ovládání otočné PTZ kamery s cílem neustále sledovat pohybující se objekt ve snímané scéně. Nahrazuje tak činnost, kterou by jinak musel vykonávat člověk. Jeden *tracking box* může řídit jen jednu kameru. Jeho funkce je založena na detekci pohybu v obraze. Vyhodnocuje rychlost a směr pohybujícího se objektu a na základě těchto analýz generuje příslušné řídící povely pro PTZ kameru. Snaží se tak vždy o udržení objektu zájmu ve středu záběru [16].

Z popisu činnosti je zřejmé, že videosignál i řídící sběrnice RS-485 musí být v tracking boxu zapojeny průchozím způsobem. Díky tomu je možné i běžné ovládání kamery přes klávesnici či záznamové zařízení. Řídící povely z *tracking boxu* mají nejnižší prioritu a člověk (operátor kamerového systému) tak vždy může převzít nad ovládáním kamer kontrolu. Mimo vstupní a výstupní konektory pro videosignál a sběrnici RS-485 obsahuje *tracking box* ještě 4 alarmové vstupy umožňující rychlý přesun kamery na předem definované prepozice.

K tomu, aby otočná PTZ kamera dokázala komunikovat s řídícím zařízením (klávesnice, DVR, atd.) je třeba užití jednotného komunikačního protokolu. *Tracking box* `MF-AT100` i zvolené kamery (`LG LPT-LT903PB`) podporují shodně protokoly Pelco D a Pelco P.


Obrázek 7.14: Čelní a zadní pohled na tracking box MF-AT100 (převzato z [16])

### 7.3.5 Přenosové prostředky a ostatní prvky CCTV systému

Při návrhu je třeba se zaměřit i na ostatní, na první pohled možná méně důležité, prvky kamerového systému. Těmi jsou myšleny zejména napájecí zdroje, kabeláž a přepěťové ochrany. Jejich špatný výběr může mít podstatný vliv na kvalitu celého systému.

**Koaxiální kabel a konektory:** Pro vedení videosignálu je samozřejmě třeba použít co nejkvalitnější koaxiální kabel s malým útlumem signálu a dobrým stíněním. Konkrétně je vhodný koaxiální kabel `RG-6U/32CA` (průměr vnitřního vodiče 0,90 mm, vnější průměr 6,50 mm, impedance 75 Ω, rozsah pracovních teplot -20 °C až +70 °C). Na jeho oba konce se přišroubují konektory F a na ně potom konektory BNC sloužící pro připojení na DVR a kamery.

**UTP kabel Cat.5E:** Jedná se o nestíněný kabel kategorie 5e obsahující 4-kroucené (twisted) páry. Kabel splňuje standardy EIA/TIA568-B.2 pro kategorii 5E. V navrhovaném CCTV systému bude použit jak pro počítačovou síť LAN, tak pro přenos videa z otočných PTZ kamer (pomocí twist převodníků) a pro realizaci sběrnice RS-485.

**Set twist převodníků Metel TW-500:** Obsahuje vysílací (`TW-Tx`) a přijímací (`TW-Rx`) stranu. Převodník umožňuje přenos videosignálu po krouceném páru vodičů až na vzdálenost 500 metrů. Výstupní úroveň videosignálu je regulovatelná. Jelikož se jedná o aktivní zařízení, je vyžadováno napájení (12 V DC).

**Přepěťová ochrana Metel BREAK-COP-VD24-IP55:** K venkovním otočným PTZ kamerám je vhodné jako doplněk použít ochranu proti přepětí (vzniklým například vlivem blesku). V takovém případě sice pravděpodobně dojde k poškození kamery, ale zabrání se tak alespoň dalším škodám na záznamovém zařízení. Těmi bývají nejčastěji spálené video vstupy a sběrnice RS-485. Přepěťová ochrana `Metel BREAK-COP-VD24` chrání videokanál, sběrnici RS-485 i napájecí vedení (maximálně do 24 V AC / 5 A). Funkce této přepěťové ochrany je vratná, provedení je venkovní s krytím IP55.

**Napájecí zdroje:** Pro napájení kamer a twist převodníků poslouží zdroje `MW DR-120`, které jsou určeny pro montáž na DIN lištu. Napájecí napětí je 12 V DC, zatížitelnost až 10 A. Napájení otočných PTZ kamer zajistí transformátor s výstupním napětím 24 V AC. Ostatní komponenty (klávesnice, tracking box) mají své napájecí adaptéry.

**Výstražné samolepky:** Upozorňují návštěvníka objektu a případného pachatele na přítomnost kamerového systému. V případě, že do objektu budou přistupovat i jiné osoby než zaměstnanci (například návštěvy, kontroly), je použití samolepek na viditelném místě nutné i z legislativních důvodů.

Obrázek 7.15: Ostatní prvky CCTV systému (v pořadí dle popisu)

# Kapitola 8

# Realizace

Tato kapitola si klade za cíl stručné popsání způsobu realizace jednotlivých dílčích podsystémů SZSOP. Realizace je provedena na základě návrhu z kapitoly 7 a v souladu se specifikací provedené v kapitole 6.

## 8.1 Zabezpečovací a přístupový systém

Jako hlavní prvek realizovaného zabezpečovacího a přístupového systému byla zvolena zabezpečovací ústředna `Concept IRC4000 EU`. Jejímu výběru je věnována kapitola 7.1.1. K ústředně jsou připojeny další komponenty, jejichž výběr, zdůvodnění a popis činnosti je proveden v kapitolách 7.1.2 a 7.1.3.

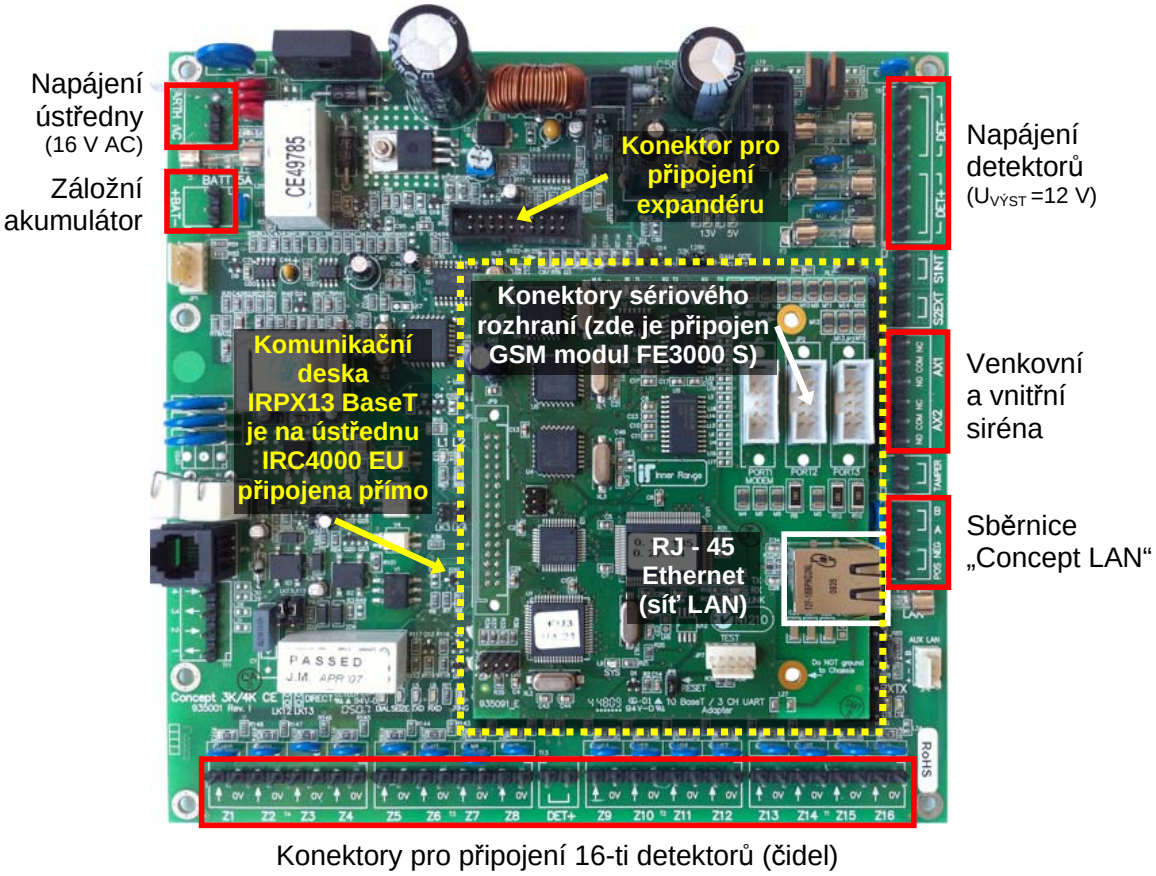
Následuje popis realizovaného zapojení zabezpečovací a přístupové ústředny, zvolených komponent a periferií. Většina uváděných informací byla čerpána z instalačních manuálů [22] [23] a programovacích příruček [20] [21].

### Popis způsobu zapojení desky ústředny

Způsob zapojení ústředny `IRC4000 EU` je znázorněn na obrázku 8.1. Do svorek `AC` vlevo nahoře je připojeno střídavé napájecí napětí 16 V AC dodávané transformátorem `TRN16/30 JBC-E20302-038` (viz kapitola 7.1.3). Přímo na ústředně se nacházejí obvody, které toto napětí dále usměrní a stabilizují na hodnotu 12 V DC. Tím jsou napájeny vnitřní obvody ústředny a napětí je vyvedeno i na svorky `DET+` a `DET-` (vpravo nahoře), určené pro napájení detektorů. Pod svorkami `AC` je umístěn konektor pro připojení záložního akumulátoru dodávajícího napětí 12 V DC po dobu výpadku hlavního napájení. Sem se tedy připojí akumulátor `Alarmguard CJ12-18 (12V/18Ah)` popsaný v kapitole 7.1.3. Na pravé straně ústředny se dále nachází vývody relé `AX1` a `AX2`, které v našem případě slouží pro spínání vnitřní a venkovní sirény. Pod nimi jsou pak vývody sběrnice `Concept LAN`, na kterou se připojuje většina dalších komponent systému `Concept`. Popis této sběrnice a způsob zapojení bude proveden v kapitole 8.1.2.

Veškeré detektory a magnetické dveřní kontakty se připojí ke svorkám `Z1 - Z16` na spodní straně desky ústředny. Podrobný popis způsobu zapojení detektorů bude následovat v kapitole 8.1.1. Dalším přítomným připojovacím rozhraním je černý, 20-ti pinový konektor určený pro propojení s expandérem. V našem případě je sem plochým kabelem zapojen univerzální expandér `IRZR3082-C`, který je nakonfigurován pro ovládání osvětlení na chodbě (podrobnější popis bude následovat v kapitole 8.1).

Důležitou součástí realizovaného systému je komunikační deska `IRPX13BaseT`, která zajišťuje komunikaci s GSM modulem a zároveň obsahuje rozhraní pro připojení ústředny do počítačové sítě. Tato deska se k ústředně připojuje přímo pomocí zabudovaného konektoru, jehož protikus se nachází na desce ústředny. Vznikne tak jednotný celek rozšiřující ústřednu o tři sériová a jedno ethernetové rozhraní. Způsob zapojení je dobře patrný z obrázku 8.1. Komunikační deska `IRPX13BaseT` je zde označena žlutou přerušovanou čárou.




Obrázek 8.1: Zapojení ústředny IRC4000 EU (včetně komunikační desky IRPX13BaseT)

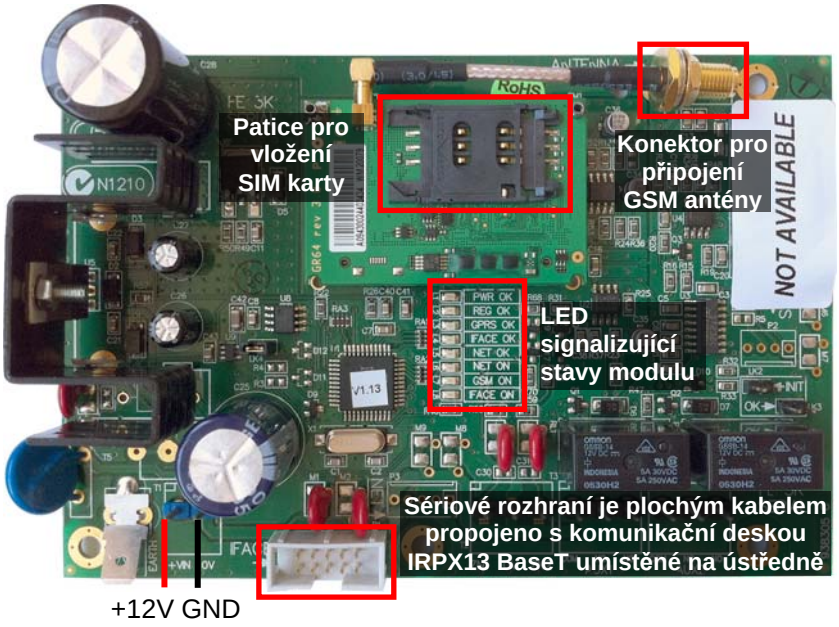
### Zapojení GSM modulu a jeho propojení s ústřednou

Způsob zapojení GSM modulu `FE3000-S` je znázorněn na obrázku 8.2. Pro napájení modulu je na svorky označené jako `+VN` a `0V` a umístěné v levé spodní části desky přivedeno napětí 12 V DC. Hned vedle napájecích svorek se nachází bílý konektor sériového rozhraní. Pro propojení s komunikační deskou `IRPX13BaseT` se používá plochý 20-ti žilový kabel, který je na komunikační desce zapojen do druhého konektoru sériového rozhraní (viz obrázek 8.1). Je tomu tak proto, že první konektor slouží pro případné propojení ústředny s počítačem, čehož se využívá například při provádění diagnostiky a servisních úkonů.

Na desce GSM modulu jsou i dva vstupní konektory a dva reléové výstupy. Díky tomu lze v případě potřeby realizovat jednoduchý autonomní zabezpečovací systém se dvěma detektory, sirénami a s možností zasílání SMS o poplachu a stavu systému. V našem případě zůstávají konektory nevyužity, proto nejsou možnosti jejich zapojení ani dále popisovány.

V horní části GSM modulu je umístěna patice, do které se vkládá SIM karta mobilního operátora s vhodným datovým tarifem. Vedle ní se pak nachází konektor GSM antény, kterou je třeba umístit v místech s kvalitním signálem. Z těchto důvodů je kabel antény poměrně dlouhý. Součástí desky GSM modulu jsou i LED diody signalizující stavy ve kterých se modul nachází:

- **LED PWR OK** – svícením indikuje přítomnost napájecího napětí 12 V DC. Pokud bliká, je napájecí napětí nedostatečné, případně špatně připojeno.
- **LED REG OK** – signalizuje úspěšnost přihlášení k GSM síti. Měla by se rozsvítit zhruba do minuty od zapnutí GSM modulu. Poté každých 5 sekund několikrát problikne, čímž ukazuje míru kvality signálu.
- **LED IFACE OK** – slouží pro indikaci stavu komunikace mezi GSM modulem a ústřednou (respektive komunikační deskou). Pokud bliká, případně vůbec nesvítí, jedná se o chybu komunikace.




Obrázek 8.2: Způsob zapojení GSM modulu FE3000-S

### Zapojení univerzálního expandéru IRZR3082-C řídícího osvětlení

Ústředna systému `Concept` obsahuje dva releové výstupy, které jsou použity pro spínání sirén. Pro rozšíření počtu releových výstupů o dalších 8 je k ústředně připojen univerzální expandér `IRZR3082-C`. Způsob zapojení je naznačen na obrázku 8.3.

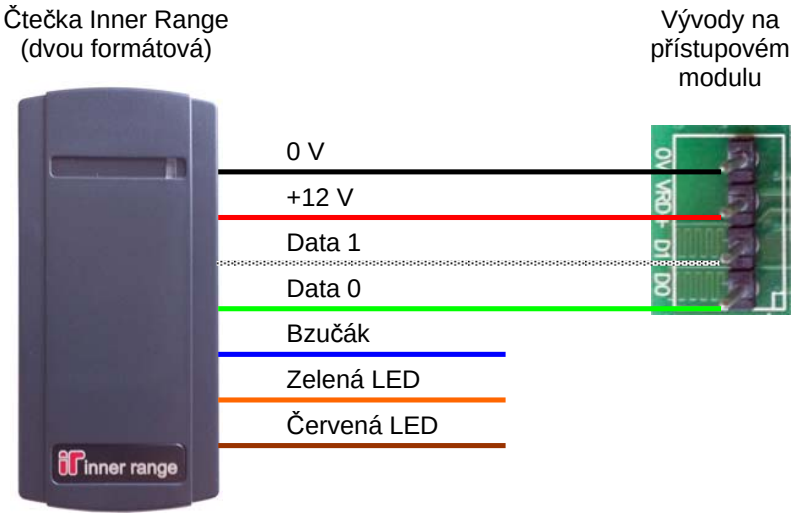
Přes svorky označené jako `+V` a `0V` je do modulu univerzálního expandéru přivedeno napájecí napětí 12 V DC. Dále se na modulu nachází (v jeho horní části) bílý 20-ti pinový konektor, který se plochým kabelem propojí s obdobným konektorem umístěným přímo na desce ústředny (viz obrázek 8.1). K ústředně lze takto připojit jen jeden expandér `IRZR3082-C`. Je-li potřeba více než deseti releových výstupů, je možné použít expandéry

IRZR3082-E, které se připojují na sběrnici Concept LAN. Pro naše účely 10 releových výstupů dostačuje (2 pro sirény a 8 pro ovládání osvětlení). Samotná relé jsou umístěna ve spodní části desky expandéru. Každé z nich umožňuje spínání zátěže až do velikosti 250 V / 5 A. Návrh zapojení konkrétního zářivkového osvětlení není součástí této práce. Releové výstupy budou pro daný účel pouze příslušně nakonfigurovány.


Obrázek 8.3: Způsob zapojení univerzálního expandéru IRZR3082-C

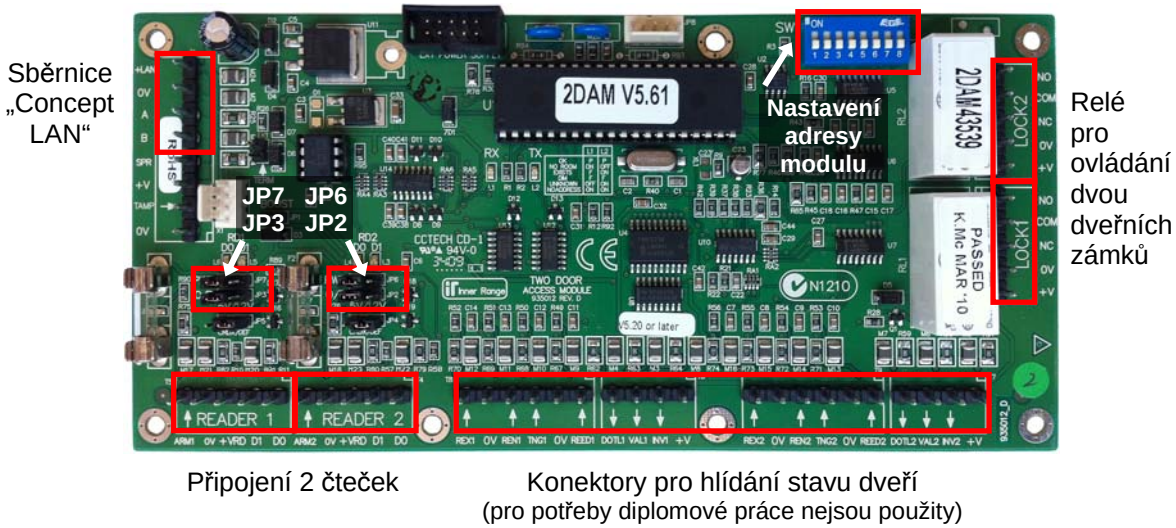
### Připojení čteček a zámků dveří k přístupovému modulu

Na obrázku 8.4 je naznačen způsob připojení čtečky Inner Range k přístupovému modulu s rozhraním Wiegand (to je podrobněji popsáno v kapitol 7.2). Použité barvy odpovídají barevnému značení vodičů u skutečné čtečky. Červený a černý vodič slouží pro přivedení napájení (12 V DC), bílý a zelený pak představují datové vodiče rozhraní Wiegand. Ostatní tři vodiče se používají v případech, kdy potřebujeme ovládat ve čtečce vestavěný bzučák a LED diody. Pro naše účely jsou tedy v tomto případě nevyužity.




Obrázek 8.4: Propojení čtečky s přístupovým modulem

Přístupový modul IRR3000 umožňuje pomocí dvou čteček řídit jednostranně přístup do dvou dveří, nebo oboustranně do jedněch dveří. Způsob zapojení přístupového modulu IRR3000 je patrný z obrázku 8.5.




Obrázek 8.5: Způsob zapojení přístupového modulu IRR3000

Na levé straně přístupového modulu IRR3000 se nachází vývody pro připojení čtyřvodičové sběrnice Concept LAN (podrobněji bude popsána v kapitole 8.1.2). Pod nimi jsou čtyři vývody pro případ potřeby napájení z externího napájecího zdroje. Tyto svorky jsou v našem případě nevyužity, protože bez problémů postačí napájení ze sběrnice. V horní části modulu je dále umístěno 8 DIP přepínačů pro nastavení adresy (čísla) modulu. Adresa se nastavuje jako osmi bitové binární číslo, přičemž její skutečná hodnota je vždy o 1 vyšší než nastavená. Má-li tedy mít modul adresu „1“, nastavíme na DIP přepínačích hodnotu „0“ (respektive „00000000“).

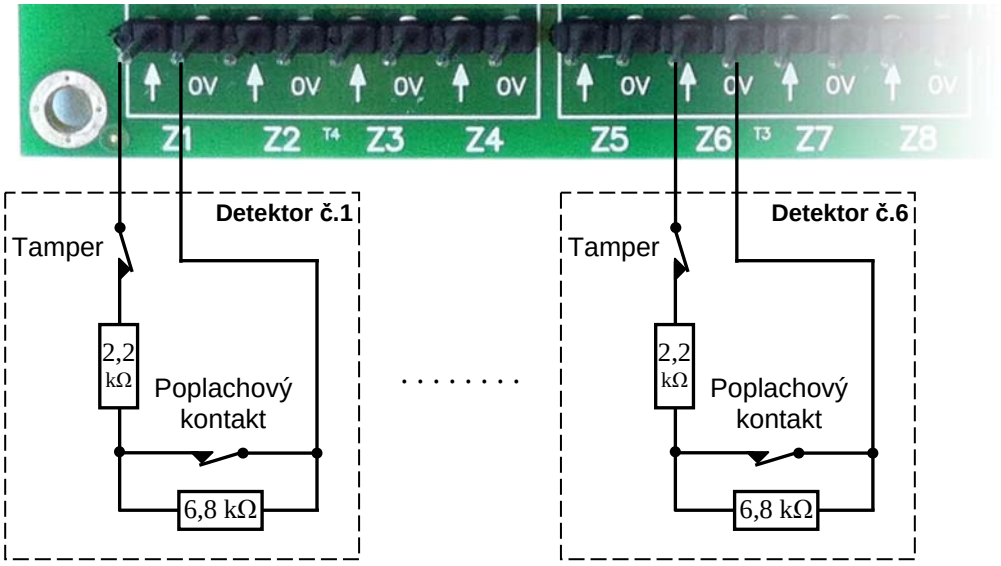
V pravé části přístupového modulu jsou umístěna dvě relé s vývody pro ovládání a napájení dvou dveřních zámků. V režimu, kdy přístupový modul řídí oboustranně jedny dveře, se využívá jen vývodů určených pro první zámek (na desce označeny jako LOCK1). Vlevo ve spodní části modulu se pak nachází svorky pro připojení dvou čteček (na desce označeny jako READER 1 a READER 2). Způsob připojení je detailně popsán a znázorněn na obrázku 8.4 na předchozí straně (56).

Důležitou součástí desky přístupového modulu IRR3000 jsou jumpery JP2, JP3, JP6 a JP7, pomocí nichž se nastavují napájecí a čtecí úrovně napětí na čtečkách. Konkrétně se pomocí jumperů JP2 a JP3 nastavuje velikost komunikačního (čtecího) napětí, které je pro duální čtečku Inner Range třeba nastavit na hodnotu 5 V. Pomocí jumperů JP6 a JP7 se pak nastavuje napájecí napětí. To je pro použitý typ čteček potřeba nastavit na 12 V.

Ve spodní části desky přístupového modulu se mimo svorky pro připojení dvou čteček nachází ještě několik dalších vstupních a výstupních konektorů. Ty sice nejsou pro potřeby této práce použity, ale přesto je vhodné alespoň zmínit možnosti jejich využití. Ze vstupních konektorů jsou to: REX (pro připojení odchodového tlačítka), REN (pro vstupní tlačítko namísto čtečky), TNG (stav západky dveřního zámku), REED (stav otevření/zavření dveří). Dále jsou dostupné výstupní svorky: DOTL (indikuje příliš dlouhé otevření dveří), VAL (signalizuje načtení platné karty) a INV (přiložení neplatné karty).

### 8.1.1 Zapojení detektorů (zón) a sirén

K desce ústředny `IRC4000 EU` a univerzálního expandéru `IRZ3004 EU EXP/16` je možné připojit až 16 detektorů (zón). Způsob jejich zapojení je naznačen na obrázku 8.6, přičemž pro ústřednu i univerzální expandér je naprosto shodný.

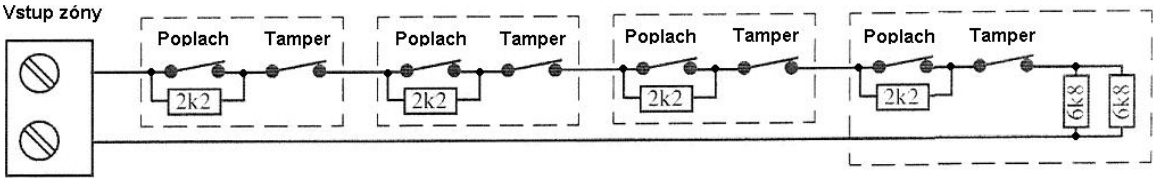



Obrázek 8.6: Připojení detektorů s NC kontakty k ústředně či expandéru

Hodnota elektrického odporu zóny v klidu je 2,2 kΩ, což odpovídá velikosti vřazeného `EOL` rezistoru. Při detekci pohybu dojde k rozpojení poplachového kontaktu v příslušném čidle a hodnota celkového odporu vzroste na 9 kΩ. Vzniklý stav je ústřednou vyhodnocen jako narušení a s touto informací je pak dále nakládáno na základě nastavení dané zóny. Jedná-li se o zpožděnou zónu, začne běžet příchodový čas. V případě okamžité zóny je ihned vyhlášen poplach. Při pokusu o násilné vniknutí do detektoru dojde k rozpojení ochranného kontaktu nazývaného `tamper` (v jenom čidle jich může být i více) a velikost odporu zóny tak vzroste k $\infty\,\Omega$. V takovém případě je vyhlášen okamžitý poplach. Obdobně je tomu i v případě vyzkratování detektoru (například kleštěmi při stříhání kabeláže útočníkem).

#### Vícenásobné zóny

Systém `Concept` umožňuje připojení až čtyř detektorů do jedné zóny způsobem jak je znázorněno na obrázku 8.7. Toto řešení sice vede ke zvýšení počtu připojitelných detektorů, ale nedoporučuje se jej používat z důvodu nemožnosti rozlišit, který detektor způsobil poplach. Počet zón je vhodnější rozšířit pomocí univerzálních expandérů `IRZ3004 EU EXP/16`.



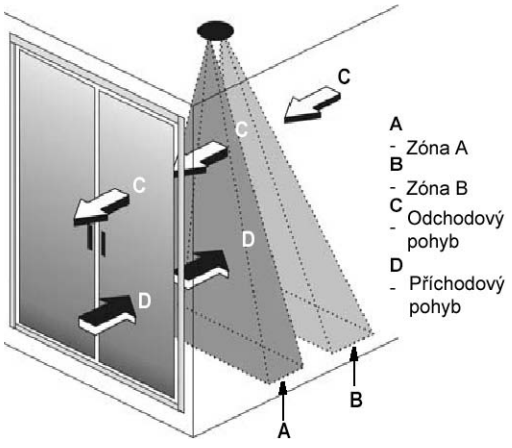

Obrázek 8.7: Způsob zapojení čtyř detektorů do jedné zóny (převzato z [34])

### Popis zapojení a nastavení zvolených detektorů

K zabezpečovací a přístupové ústředně `Concept IRC4000 EU` a k univerzálnímu expandéru `IRZ3004 EU EXP/16` jsou připojeny detektory, jejichž volba byla provedena v kapitole 7.1.3. Pro jejich napájení je použito napětí 12 V dostupné na svorkách `DET+` a `DET-` ústředny (viz kapitola 8.1) a univerzálního expandéru.

**PIR detektor PARADOX 476 Pro:** Optimální montážní výška je 2,1 m a v zorném poli detektoru by se neměly nacházet žádné lesklé plochy, ventilátory, horkovzdušná topení a předměty s rychle se měnící teplotou (lednička, netěsnící okno). Oblast detekce je potom ve vzdálenosti od 1,2 m do 9 m. Na desce detektoru se nachází dva jumpery (`J1` a `J2`). První určuje, zda bude aktivní LED dioda signalizující pohyb, druhý pak rychlost detekce (od výroby je nastaven rychlý režim, tedy `J2` je spojen). Samotné připojení detektoru k desce ústředny či expandéru se provede způsobem popsaným na začátku této kapitoly (obrázek 8.6).

**Stropní PIR detektor PARADOX DG466 Paradome:** Obsahuje dva PIR snímače pohybu a díky tomu dokáže rozlišovat směry průchodů. Na ústředně je pak tento detektor zapojen do dvou zón. Způsob, jakým probíhá rozlišování odchodového a příchodového pohybu dobře vystihuje obrázek 8.8. Pro správnou činnost je třeba provést instalaci do prostor poblíž vstupních dveří, červenou LED diodou směrem ke vstupu. Opět platí potřeba vyvarovat se předmětům s rychle se měnící teplotou v zorném poli detektoru. Na desce čidla se nachází 5 jumperů (označených `J1` až `J5`) sloužících pro nastavení všech potřebných funkcí. Jumper `J1` povolí nebo zakáže indikaci detekce pohybu LED diodou. Jumper `J2` umožňuje nastavit větší odolnost proti rušení (ovšem za cenu snížení citlivosti). Pomocí jumperů `J3`, `J4` a `J5` pak lze nakonfigurovat zvláštní odchodový režim a velikost příchodového zpoždění. Pro běžné účely a pro potřeby této diplomové práce postačí ponechat všechny jumpery v továrním nastavení.




Obrázek 8.8: Typy pohybů rozlišovaných detektorem DG466 (převzato z [9])

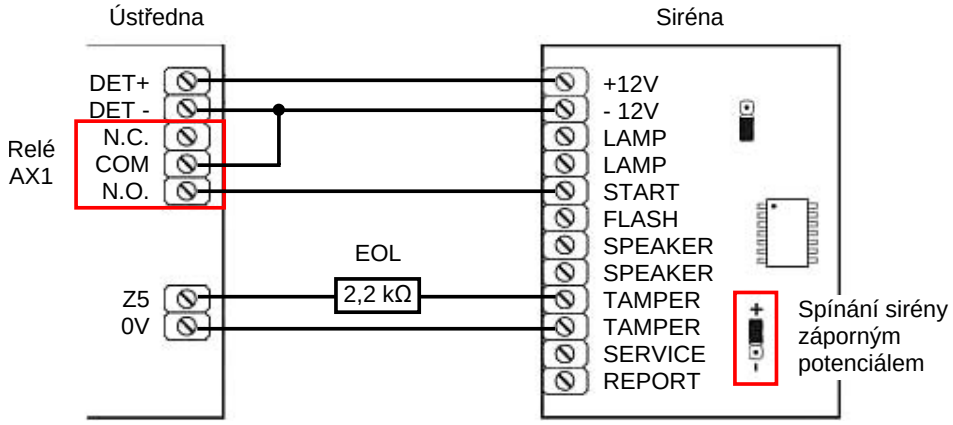
**Dveřní PIR záclona PARADOX 460 Paradoor:** Se nainstaluje nad okno nebo předmět, jenž má být střežen. Vhodná instalační výška je v rozmezí od 2,1 m (detekuje i malý pohyb ruky) do 6 m (detekuje pohyb osoby). Jumper `J1` určuje, zda bude aktivní LED dioda signalizující pohyb. Pomocí jumperu `J2` se definuje typ výstupu (továrně N.C.) a `J4` určuje napájecí napětí (nechat propojeno pro napětí 12 V).

**Magnetický dveřní kontakt SA-200A:** Je možné jej instalovat na vodivé i nevodivé materiály. Kontakt je určený pro povrchovou montáž, ale je-li to možné, je dobré jej zahloubit. Při instalaci je třeba dát pozor na to, aby vzdálenost mezi oběma částmi magnetického kontaktu byla při zavřených dveřích menší než 20 mm. Připojení k ústředně se realizuje shodně jako u ostatních detektorů.

### Popis zapojení a nastavení sirén

Pro napájení sirén jsou shodně jako u detektorů využity svorky `DET+` a `DET-` na desce ústředny `Concept IRC4000 EU`. Zapojení samotných sirén se mírně liší v závislosti na tom, zda se jedná o zálohované nebo nezálohované provedení.

**Venkovní zálohovaná siréna PARADOX PS-128:** Je uložena v masivním protipožárním krytu odolném proti odtržení a násilnému vniknutí. Je třeba ji umístit do dostatečné výšky a pokud možno tak, aby byla co nejhůře přístupná. Při instalaci se do sirény nejprve připojí akumulátor sloužící pro zálohu napájení po dobu případného výpadku. Propojení se zabezpečovací ústřednou je možné několika způsoby. V našem případě je použito zapojení jenž je naznačeno na obrázku 8.9. Napájení sirény je realizováno ze svorek `DET+` a `DET-` na ústředně. Poplach je vyhlášen buďto při výpadku napájení, nebo při sepnutí relé `AX1` na ústředně (čímž dojde k přivedení nulového potenciálu ze svorky ústředny `DET-` na svorku sirény `START`). Tamper sirény (spínač monitorující otevření krytu) je k ústředně připojen přes `EOL` rezistor velikosti 2,2 kΩ jako okamžitá zóna. Při násilném otevření sirény pak dojde ihned k vyhlášení poplachu, a to bez ohledu na stav, v jakém se zabezpečovací systém nacházel.




Obrázek 8.9: Způsob zapojení venkovní sirény PARADOX PS-128

**Vnitřní siréna Jablotron SA-913F:** Montáž provedeme přišroubováním na libovolný povrch ve vnitřních prostorách. Siréna by měla být umístěna dostatečně vysoko, aby nebylo snadné ji rychle zneškodnit. Zapojení je velice jednoduché. Postačí připojit příslušné vodiče na napájecí napětí 12 V přes spínací kontakt relé na ústředně. Ze sirény vedou celkem tři vodiče: hnědý, červený a bílý. Hnědý představuje napájecí zem a připojí se na svorku `DET-` na ústředně. Ke svorce `DET+` se přes kontakty `NO` a `COM` relé, označeného na ústředně jako `AX2`, připojí červený vodič. Při poplachu relé `AX2` sepne a siréna provádí akustickou (houká) i optickou (bliká) signalizaci. Pokud by se místo červeného vodiče použil bílý, siréna by pouze blikala.

### 8.1.2 Sběrnice Concept LAN a připojení ostatních komponent

Doposud byl popsán způsob zapojení komponent, které se k ústředně připojují přímo přes její vývody, nebo přes specifická rozhraní (sériový port, port pro připojení expandéru `IRZR3082-C`). Pro propojení všech ostatních prvků se využívá sběrnice označované jako `Concept LAN`. Na ni jsou v našem případě napojeny klávesnice `IRT3000-E`, přístupové moduly pro dvoje dveře `IRR3000` a expandér pro rozšíření systému o dalších 16 zón `IRZ3004 EU EXP/16`. Sběrnice `Concept LAN` je tvořena čtyřmi vodiči s následujícím označením a významem [23]:

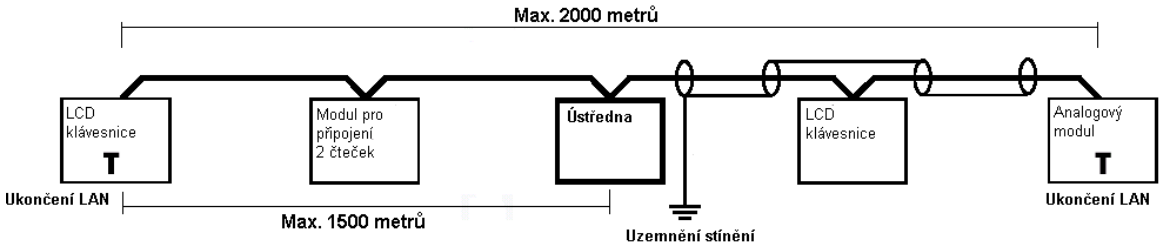
- `NEG` (na modulech často značeno jako `GND`) představuje záporný pól napájecího napětí.
- `LAN+` (na deskách modulů většinou značeno jako `POS`) představuje kladný pól napájecího napětí. Díky tomu lze po sběrnici napájet moduly bez vlastního zdroje (například klávesnice `IRT3000-E`). V případě, že daný modul má svůj napájecí zdroj (například expandér `IRZ3004 EU EXP/16`), tento vodič se nepřipojuje (vodič `NEG` musí být naopak připojen vždy).
- `A` a `B` jsou datové vodiče. Pro správou funkci musí být pro vedení dat použit jeden kroucený (twisted) kabelový pár.

O integritu sběrnice se stará ústředna, která provádí pravidelné dotazování se (tedy „pooling“) na stav jednotlivých modulů. Díky tomu lze snadno měnit a přidávat jednotlivé moduly i za běhu systému. Data přenášená po sběrnici jsou pro větší bezpečnost šifrována.

Na sběrnici `Concept LAN` je možno připojit až 250 modulů, z toho až 99 jich může být stejného typu. Pro realizaci je třeba použít strukturovanou kabeláž kategorie alespoň Cat. 5E. Při realizaci kabeláže na velmi dlouhé vzdálenosti, kde by již docházelo k výrazným úbytkům napětí na vedení, je vhodné pro napájecí část sběrnice (vodiče `NEG` a `LAN+`) použít samostatný kabel s vodiči větších průřezů.

Maximální povolená délka kabeláže (bez použití takzvaného „LAN izolátoru“ `IRI3000`) je 2 000 metrů. Navíc musí být dodrženo, aby délka kabelů mezi ústřednou a nejvzdálenějším modulem byla menší než 1 500 metrů a maximální počet takto připojených modulů byl 64. Datovou část sběrnice (vodiče `A` a `B`) je nutné na obou koncích zakončit zakončovacím rezistorem (takzvaným „terminátorem“) o hodnotě 470 ohmů. Rezistor se vkládá mezi vodiče `A` a `B`. Na většině modulů k tomu postačí pouhé přepnutí příslušného DIP přepínače.

Jsou-li výše uvedené vzdálenosti limitující (například při velmi rozsáhlých realizacích), je možno do systému doplnit LAN izolátor `IRI3000`. Tento modul umožní rozdělení sběrnice na další dvě oddělené části, přičemž každá z nich tvoří novou samostatnou sběrnici (platí pro ni stejná pravidla jako byla uvedena výše). Pro účely této diplomové práce není LAN izolátor třeba a tak není v textu podrobněji popisován.



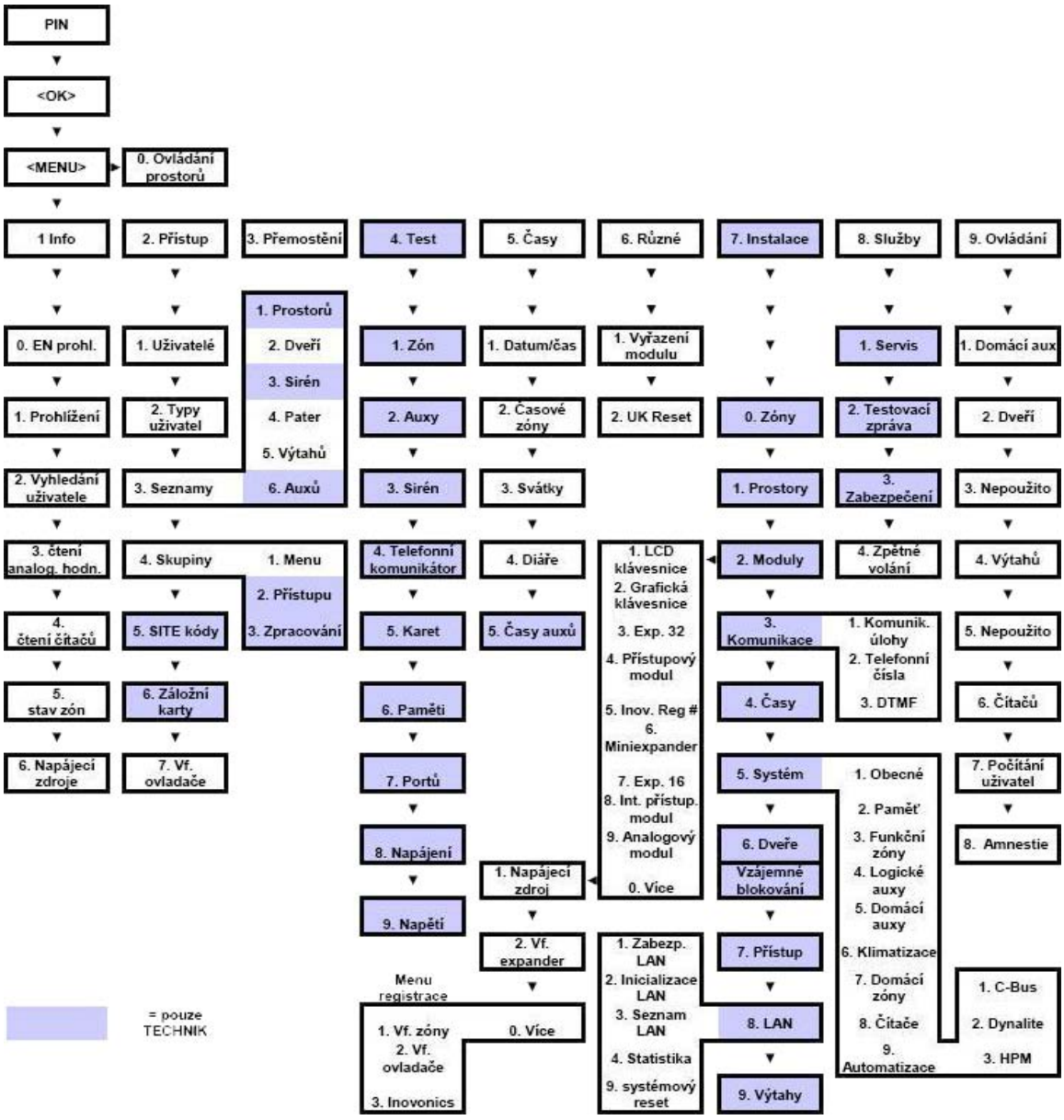

Obrázek 8.10: Způsob zapojení sběrnice Concept LAN bez LAN izolátoru (převzato z [23])

### 8.1.3 Programování pomocí klávesnice

Jednou z možností jak programovat *přístupový a zabezpečovací systém* `Concept` je zadávání požadovaných voleb pomocí klávesnice (`IRT3000-E`).

Možnost programování má pouze uživatel s názvem `TECHNIK`, pro kterého je v systému od výroby přednastaven uživatelský PIN „01“. Tento uživatel má největší práva a vyjma změny PIN kódu se u něj nedoporučuje nic upravovat.

Uživatel `TECHNIK` vstoupí do *programovacího menu* zadáním PIN kódu „01“, potvrzením tlačítkem `OK` a následně stiskem tlačítka `MENU`. Zde se v příslušných sekcích zadávají potřebné údaje a parametry. Struktura programovacího menu je znázorněna na obrázku 8.11.

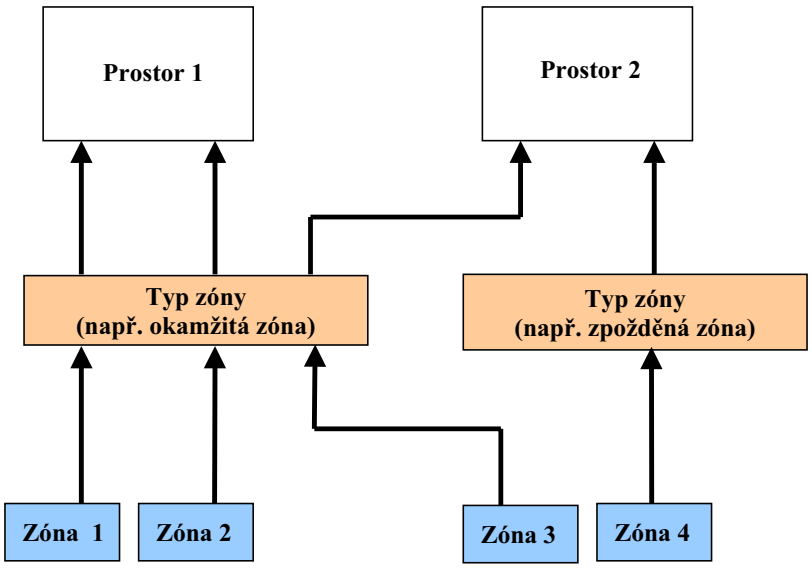



Obrázek 8.11: Struktura programovacího menu systému Concept (převzato z [21])

### Programovací volby zabezpečovacího systému

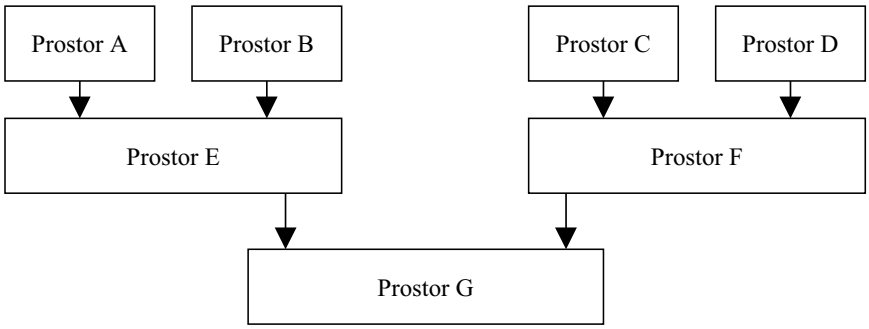
Základními programovacími entitami zabezpečovacího systému jsou *zóny*. Pro každou je možné nastavit její název a typ použitého detektoru (zda je s N.O. nebo N.C. kontakty). Nadřazenými prvky nad zónami jsou takzvané *typy zón*, které určují pravidla chování a způsoby reakce vlastních zón na vstupní podněty. Sem patří například nastavení stavů, na které bude zabezpečovací systém reagovat, konfigurace sirén a zobrazení zpráv na klávesnici. Zóny je možno sdružovat do větších celků, nazývaných *prostory*.

Grafické znázornění vazeb jednotlivých programových voleb zabezpečovacího systému vyjadřuje obrázek 8.12.




Obrázek 8.12: Schematické vyjádření programových vazeb u zón (převzato z [21])

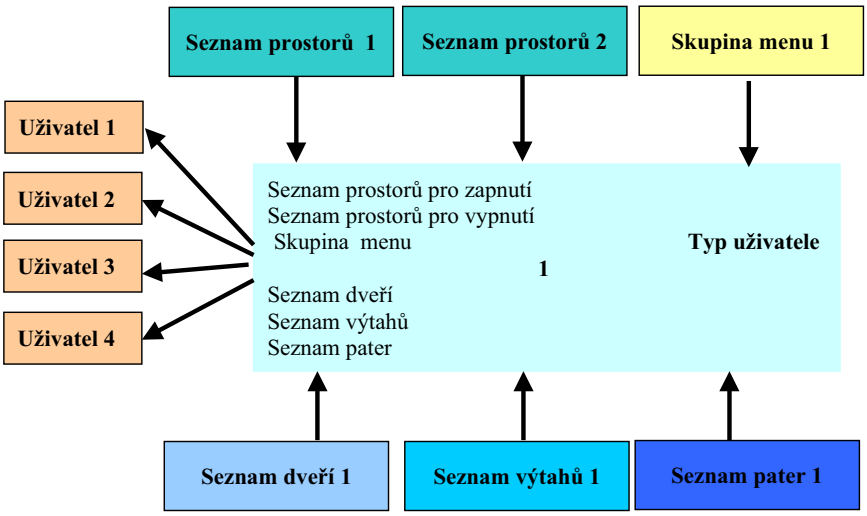
Velice důležitou funkcí je vytváření takzvaných *společných prostor*, kdy se některé již existující prostory v systému sdružují do logických celků. Zastřežení (případně odstřežení) takového prostoru uživatelem poté vede i k zastřežení (případně odstřežení) všech dílčích podprostorů. Ukázka principu tvoření *společných prostor* je na obrázku 8.13. Prostory A a B mohou představovat kanceláře a prostor E pak chodbu v daném patře. Prostory C, D a F mohou představovat totéž, jen v jiném patře. Prostor G poté reprezentuje celou budovu.




Obrázek 8.13: Způsob tvoření společných prostor (převzato z [21])

### Programovací volby správy uživatelů

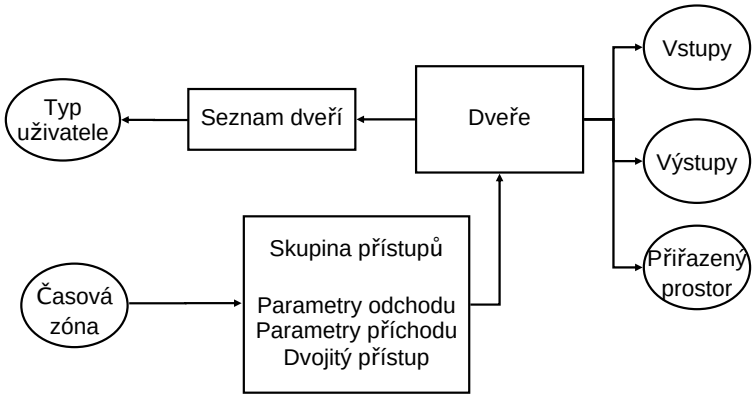
Pro usnadnění práce s uživatelskými právy jsou v systému `Concept` zavedeny profily určující *typ uživatele*. Nově vytvářeného či editovaného uživatele pak postačí zařadit do příslušné skupiny a není pro něj nutno zvlášť definovat uživatelská oprávnění. Každé skupině je možno přiřadit prostory, které budou moci její členové ovládat, povolit nebo zakázat určité funkce a definovat výčet dveří s povoleným průchodem. Opět platí, že se tato nastavení nepřiřazují přímo, ale pomocí příslušných seznamů (*seznam prostor*, *seznam dveří*, *seznam pater*) [21]. Hierarchie programovacích voleb správy uživatel je znázorněna na obrázku 8.14.




Obrázek 8.14: Schematické znázornění uživatelských programových voleb (převzato z [21])

### Programovací volby přístupového systému

Základní prvek pro programování přístupového systému představují *dveře*. Každým dveřím lze přiřadit název, dveřní elektrický zámek a prostor, do kterého spadají. Lze je dále sdružovat do *seznamů dveří* a pomocí nich pak určovat přístupová oprávnění jednotlivým skupinám uživatelů. *Skupina přístupů* pak pro každé dveře definuje provázání se zabezpečovacím systémem a určuje, které klávesnice a přístupové moduly je mohou otevírat.




Obrázek 8.15: Schéma programovacích voleb přístupového systému (převzato z [21])

### 8.1.4 Programování a vzdálená správa pomocí software

Pro programování a vzdálenou správu zabezpečovacího a přístupového systému Concept lze použít software Insight vyvíjený výrobcem. Ten je dostupný v několika verzích, a to Lite, Installer a Express, přičemž poslední dvě jmenované verze jsou placené.

Pro účely diplomové práce byla použita verze Insight Lite, která má omezení na současné připojení k maximálně jedné ústředně, což plně postačuje. Ve verzi „Lite“ nejsou dále dostupné některé moduly jako je například Insight Foto ID (doplňující fotografie k uživatelským účtům) nebo Insight Schéma (umožňující grafickou vizualizaci stavů systému na mapce či výkresu objektu) [19].

#### Připojení ústředny Concept do počítačové sítě

Připojení systému Concept do počítačové sítě je realizováno přes ethernetový port komunikační desky IRPX13BaseT. Aby bylo možné navázat komunikaci mezi ústřednou a softwarem Insight Lite, je nejprve třeba provést určitá nastavení ústředny. Software Insight je ve své podstatě serverová aplikace, naslouchající na síťovém portu 17 185. Z tohoto důvodu je vhodné mít IP adresu serveru na kterém tento software běží nastavenu jako statickou.

Následně je třeba v ústředně aktivovat takzvanou *komunikační úlohu* Insight (vyvoláním menu 7-3-1 na LCD klávesnici). V rámci této komunikační úlohy se poté nastaví IP adresa ústředny, maska sítě, IP adresa výchozí brány (routeru) a IP adresa Insight serveru. Konkrétní síťové adresy použité při realizaci jsou uvedeny v tabulce 8.1.

| | **Server se SW Insight** | **Ústředna Concept** |
|---|---|---|
| IP adresa | 192.168.001.201 | 192.168.001.230 |
| Výchozí brána | 192.168.001.001 | 192.168.001.001 |
| Maska sítě | 255.255.255.000 | 255.255.255.000 |
| IP adresa serveru | - - - - | 192.168.001.201 |

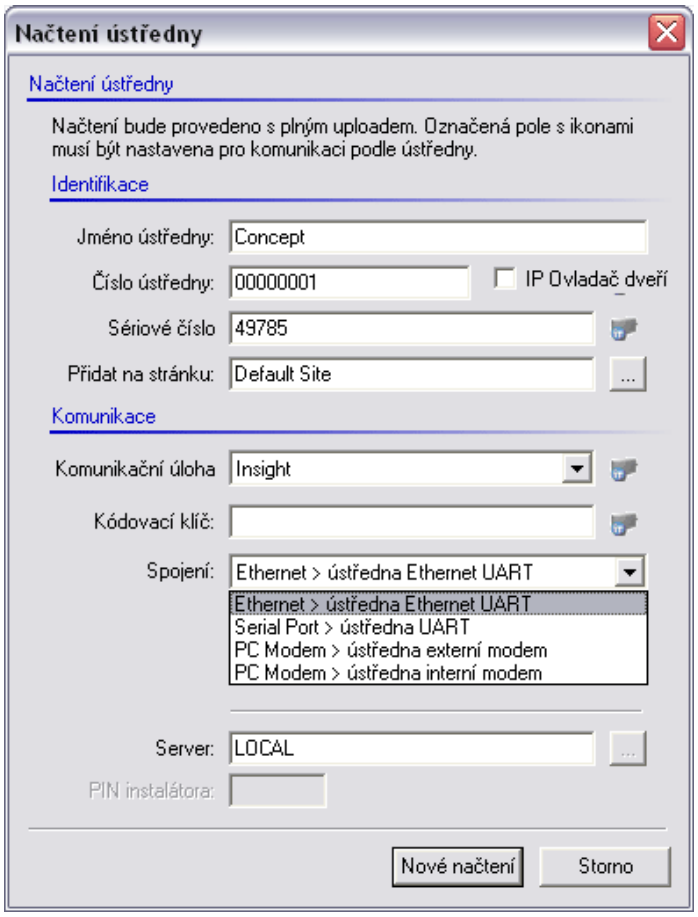
Tabulka 8.1: Nastavení počítačové sítě na serveru a v ústředně Concept

#### Načtení ústředny do software Insight Lite

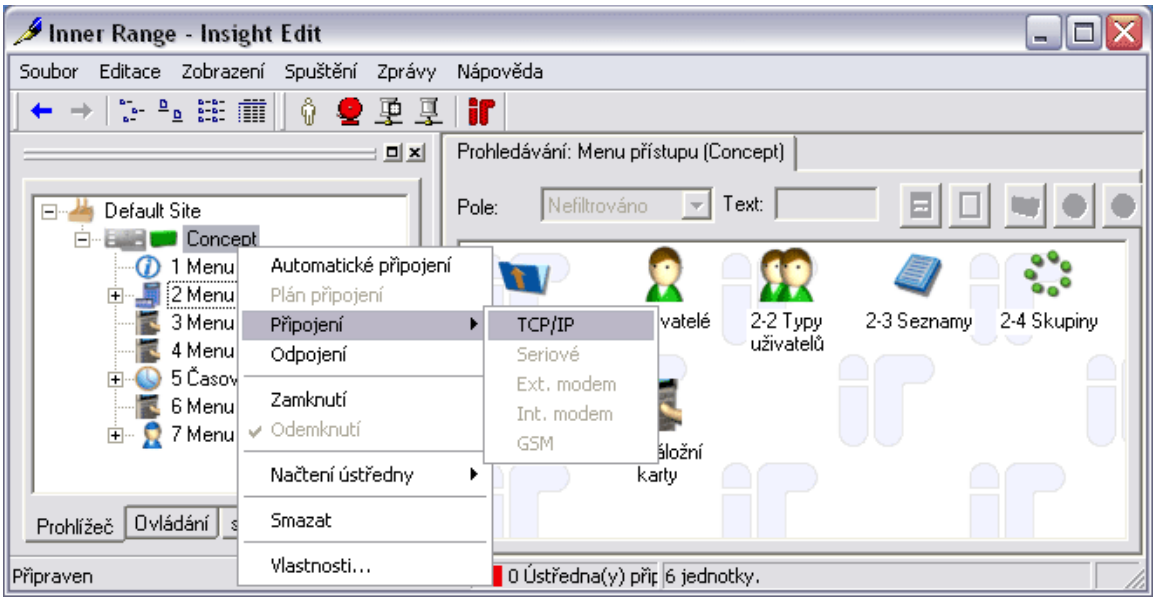
V momentě, kdy jsou parametry počítačové sítě správně nastaveny a v ústředně je úspěšně spuštěna *komunikační úloha* Insight, je možné zahájit komunikaci mezi ústřednou a softwarem Insight Lite.

Před tím je však třeba ještě nastavit ID ústředny a zjistit její sériové číslo. ID ústředny se nastavuje pomocí LCD klávesnice v menu 7-3-1 (Instalace - Komunikace - Komunikační úlohy). Sériové číslo je dostupné spolu se spoustou dalších informací o systému v menu 2 (Menu přístupu).

Načtení ústředny se poté provede pomocí modulu Insight Načtení ústředny. Po přihlášení (defaultní login a heslo je „admin“) pak v dialogovém okně postačí zvolit libovolné jméno relace, zadat ID ústředny, její sériové číslo a vybrat položku „ethernet“ v sekci „typ spojení“. Následným kliknutím na tlačítko „Nové načtení“ dojde ke spojení s ústřednou a k ověření komunikace. Popisovaný postup načtení ústředny je znázorněn na obrázku 8.16. Posledním krokem je vyvolání procedury propojení s ústřednou a načtení její konfigurace. To se provede v modulu Insight Edit postupem znázorněném na obrázku 8.17.




Obrázek 8.16: Dialogové okno pro načtení ústředny Concept




Obrázek 8.17: Připojení k ústředně Concept z programu Insight Lite

### 8.1.5 Programování ústředny

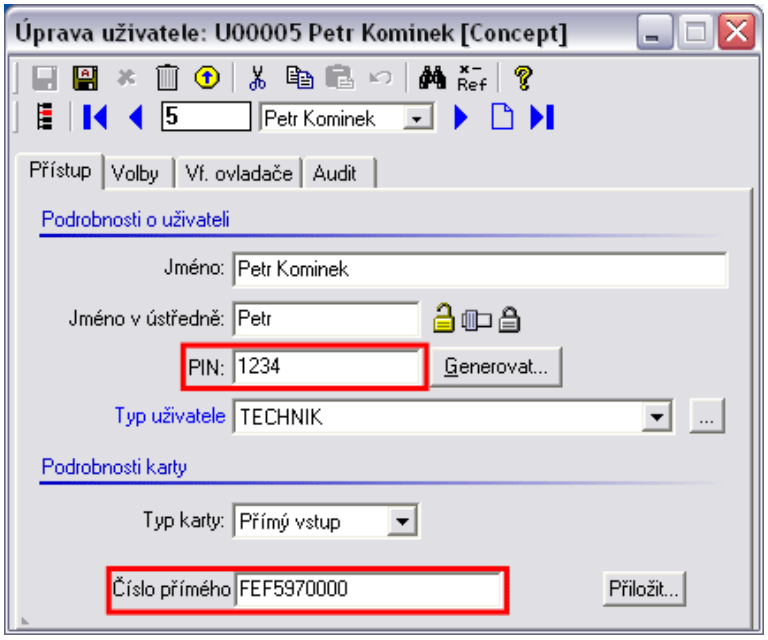
Konfigurace a naprogramování zabezpečovacího a přístupového systému `Concept` byly provedeny na základě požadavků plynoucích ze specifikace (kapitola 6) a v souladu s návrhem provedeným v kapitole 7.1.

Na následujících stranách bude stručně popsán způsob nastavení systému pro realizaci některých z požadovaných funkcí. Kompletní konfigurace zabezpečovacího a přístupového systému je uložena na datovém nosiči DVD přiloženém k této diplomové práci.

#### Definice nového uživatele, ukázka načtení přístupové katy a čipu

Jedním ze základních kroků při programování zabezpečovacího a přístupového systému `Concept` je definice nového uživatele. Ta se provádí v menu 2-1 („Uživatelé“) buďto z klávesnice, nebo pomocí software `Insight Lite`.

Vzhled dialogového okna pro přidání či změnu uživatelského účtu je zachycen na obrázku 8.18. Každému uživateli je zde možné přiřadit jméno, PIN kód a číslo karty nebo čipu pro ovládání zabezpečovacího systému a pro přístupové funkce. Důležité je rovněž zvolit příslušný *typ uživatele*, což je v podstatě skupina uživatel s právy pro ovládání a přístup do definovaných prostor. Více informací o *typech uživatelů* bylo již uvedeno v kapitole 8.1.3.



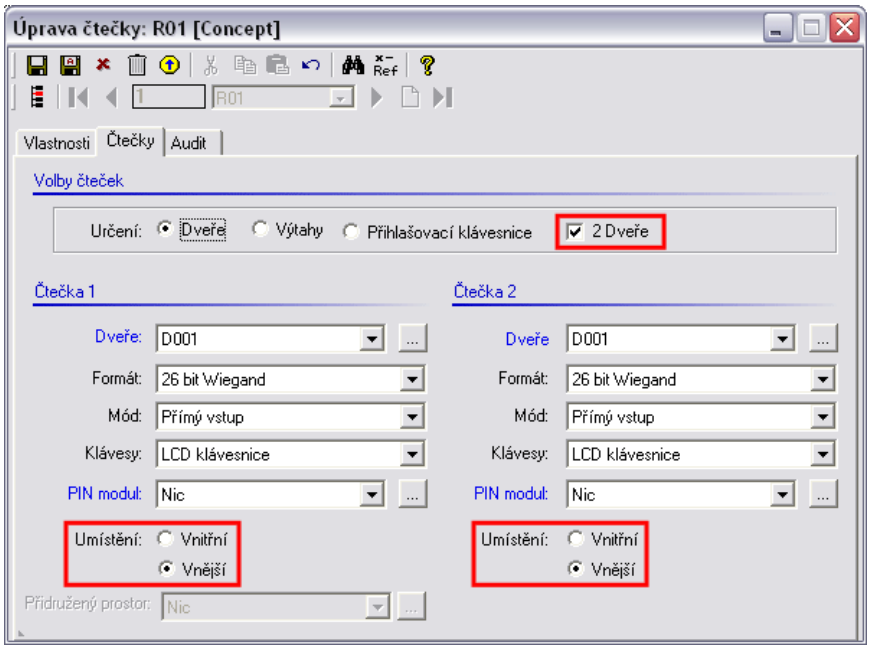

Obrázek 8.18: Dialogové okno pro vytvoření uživatele v systému Concept

Před přiřazením čísla karty nebo čipu danému uživateli je nejprve třeba u položky „Typ karty“ zvolit položku „Přímý vstup“ (viz obrázek 8.18). O řádek níže se pak zadává vlastní číslo karty. To lze nejrychleji zjistit pomocí LCD klávesnice, v menu 4-5 (*Testování čteček*). Po přiložení karty nebo čipu na čtečku se na LCD displeji klávesnice objeví jejich číslo v hexadecimálním formátu (například 039AFEF5970000). První čtyři hexadecimální znaky určují formát karty a počet bitů čísla (více o tomto viz [10]). Jelikož již byla provedena volba kompatibilních karet a čtečky (`HID Proximity Card II`, 26-bitů), můžeme je ignorovat a do příslušného políčka zadáme číslo karty o tyto 4 znaky kratší (tedy FEF5970000).

### Konfigurace přístupových modulů

Pro otevírání dveří prostřednictvím elektrických zámků slouží přístupové moduly `IRR3000` a `IRR3000-1`. K prvně jmenovanému je možné připojit dvě čtečky a řídit tak jednosměrně průchod dvěmi dveřmi, případně obousměrně jedněmi dveřmi. Druhý pak umožňuje připojení pouze jedné čtečky.

Konfigurace přístupového modulu se provádí v menu 7-2-4 (*Menu instalace - Moduly - Modul čtečky*) na klávesnici nebo v software `Insight`. Příslušné dialogové okno pro nastavení parametrů přístupového modulu je zobrazeno na obrázku 8.19.




Obrázek 8.19: Dialogové okno konfigurace přístupového modulu

Na záložce „Čtečky“ je třeba zatrhnout volbu „2 Dveře“, čímž definujeme, že k modulu jsou připojeny 2 čtečky. Následně se každé čtečce přiřadí příslušné dveře (v našem případě budou obě čtečky řídit přístup do jedněch dveří „D001“) a nastavit formát karet a čipů (v našem případě *26 bit Wiegand*). V sekci „umístění“ ve spodní části okna se ještě nastaví, která čtečka je umístěna vně a která uvnitř daného prostoru.

Další užitečnou funkcí jež byla nastavena je možnost zastřežit definované prostory trojím přiložením přístupové karty nebo čipu na čtečku. Toho docílíme zatrhnutím volby „Vstupní prostor při 3x přiložení“ u položky „Ovládací mód“ na záložce „vlastnosti“ dialogového okna z obrázku 8.19.

### Spínání osvětlení na základě detekce pohybu PIR detektory

Další požadovanou funkcí systému bylo spínání světel na základě detekce pohybu PIR čidly v nastavitelnou večerní dobu.

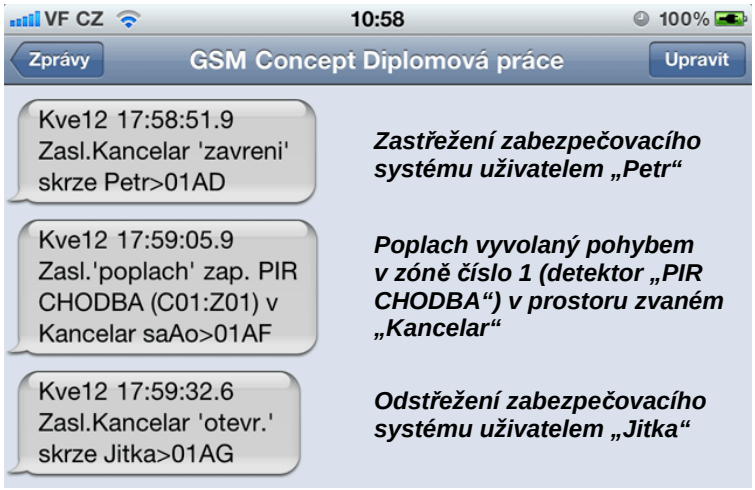
Pro tento účel si v menu 5-2 (*Časování - Časové zóny*) vytvoříme *časovou zónu* nazvanou „světla“ a definujeme časové intervaly a dny, kdy má být tato zóna aktivní (v našem případě je definována pro každý den od 00:00 do 08:00 hodin). Na záložce „Nastavení“ potom tuto *časovou zónu* přiřadíme prostoru jménem „světla“.

Prostor s názvem „světla“ nadefinujeme v menu 7-1 (*Menu instalace - Prostory*). Zde následně vybereme zóny (detektory), které mají sloužit pro spínání osvětlení. Nakonec je ještě třeba stanovit dobu sepnutí a označit ty releové výstupy (takzvané *auxy*), ke kterým je osvětlení fyzicky připojeno. V našem případě je použit výstup s označením `C01:X03`, kde řetězec `C01` značí ústřednu číslo 1 a `X03` pak příslušné relé. Jen pro doplnění, první releový výstup na expandéru `IRZR3082-C` je v systému číslován jako `X03`. Je tomu tak proto, že přímo na ústředně jsou dostupné 2 releové výstupy a jejich číslování v rámci celého systému je navazující.

### Konfigurace GSM modulu pro zasílání SMS zpráv

Před vlastní konfigurací GSM modulu `FE3000-S` pro zasílání SMS zpráv při zastřežení, odstřežení a poplachu je třeba nejprve definovat telefonní čísla, na která budou tyto zprávy zasílány. To se provede v menu 7-3-2 (M*enu instalace - Komunikace - Telefonní čísla*). Mimo uživatelská telefonní čísla (zadávají se v mezinárodním formátu 420123456789) je zde třeba vyplnit navíc i telefonní číslo centra pro odesílání SMS zpráv daného operátora (například pro Vodafone je to 420608005681).

Ostatní nastavení se provádí v menu 7-3-2 (*Menu instalace - Komunikace - Komunikační úlohy*). Zde zvolíme *komunikační úlohu* `CT002 (GSM)` a nastavíme port, do kterého je na komunikační desce `IRPX13BaseT` připojen GSM modul (tedy v našem případě *port 2*). Na záložce „Vlastnosti“ vybereme ze seznamu číslo SMS centra a uživatele, kterým mají být zasílány SMS. Na záložce „Konfigurace SMS“ pak zatrhneme, že SMS se mají zasílat při zastřežení a odstřežení systému a při poplachu.




Obrázek 8.20: Ukázky SMS zpráv zasílaných systémem Concept

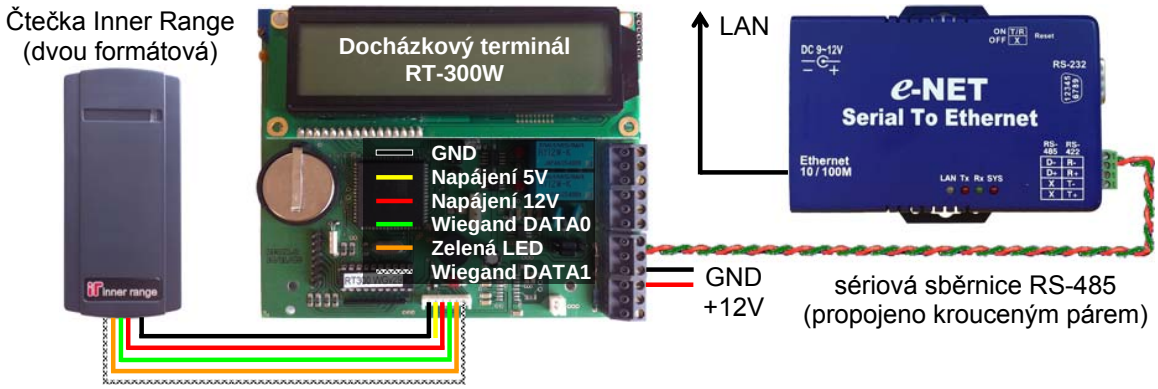
Na obrázku 8.20 je znázorněna forma a obsah skutečných SMS zpráv zaslaných realizovaným zabezpečovacím a přístupovým systémem `Concept` při *zastřežení*, *poplachu* a *odstřežení*. Na první pohled by se mohlo zdát, že některé textové řetězce ve zprávách obsažené nejsou zrovna dobře čitelné. Má to však svoje praktické důvody. Prostřednictvím zasílání SMS zpráv na telefonní číslo SIM karty umístěné v GSM modulu `FE3000-S` lze totiž celý systém ovládat. Více informací o syntaxi těchto příkazů a o možnostech ovládání zabezpečovacího a přístupového systému `Concept` je uvedeno v programovací příručce [20].

## 8.2 Realizace docházkového podsystému

Dalším dílčím realizovaným prvkem systému zabezpečení a střežení objektů a prostor je *podsystém pro evidenci docházky*. Realizace byla provedena v souladu s návrhem z kapitoly 7.2. Informace byly čerpány převážně z manuálu [6] a z webových stránek [34] a [25].

### 8.2.1 Propojení docházkového terminálu, čtečky a převodníku e-NET

Docházkový podsystém je tvořen docházkovým terminálem `ACS-line RT-300W` propojeným se čtečkou `Inner Range Dual-Format Proximity Reader` a převodníkem `e-NET E-P132-X`. Způsob propojení těchto komponent a připojení docházkového podsystému do počítačové sítě LAN je znázorněn na obrázku 8.21.




Obrázek 8.21: Způsob propojení docházkového terminálu se čtečkou a převodníkem e-NET

Čtečka je k terminálu `RT-300W` připojena přes rozhraní *Wiegand*. Vývody tohoto rozhraní jsou přímo na desce docházkového terminálu. Nachází se zde svorky `GND` a `+12V` pro napájení čtečky, vývody rozhraní Wiegand (`DATA0` a `DATA1`) a svorka pro připojení zelené LED diody signalizující úspěšné načtení přístupového média (karty nebo čipu).

V pravé části desky terminálu se nachází svorkovnice pro přivedení napájecího napětí 12 V (svorky `GND` a `+12V`). Dále jsou zde vývody sériové sběrnice RS-485, na kterou je připojen samostatně napájený převodník `e-NET E-P132-X`, který je dále přes integrovaný konektor `RJ-45` připojen do počítačové sítě.

#### Konfigurace převodníku e-NET E-P132-X

Pro zpřístupnění docházkového terminálu do počítačové sítě je velice důležitá správná konfigurace převodníku `e-NET E-P132-X`. Ta se provádí přes jeho webové rozhraní pomocí libovolného internetového prohlížeče. Převodník má od výroby nastaveno dynamické přidělování IP adresy (DHCP). Po připojení do počítačové sítě je tedy nejdříve třeba zjistit jeho IP adresu (například na routeru) a tu následně zadat do webového prohlížeče.

Konfigurační webové rozhraní převodníku je dostupné na portu 80 a jeho vzhled je znázorněn na obrázku 8.22. Zde je třeba nastavit IP adresu převodníku (v našem případě 192.168.1.250), pod kterou bude v docházkový terminál v počítačové síti dostupný. Dále se zde nastavuje síťová maska, IP adresa routeru, webový port a případné další parametry.

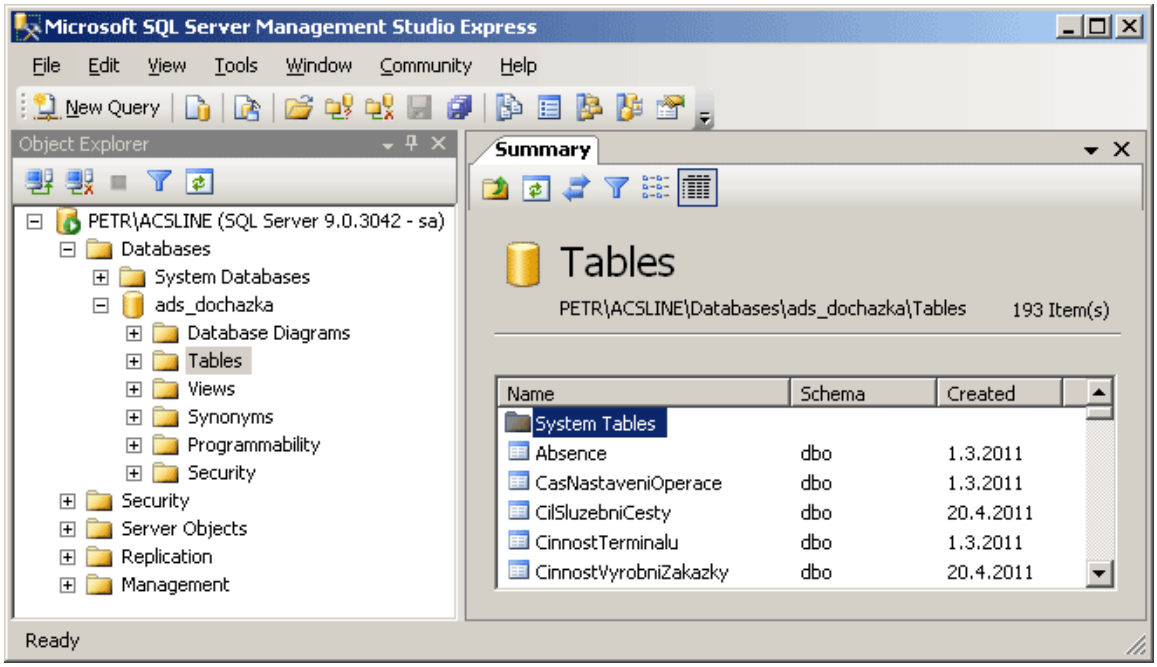
Pro správnou komunikaci s terminálem je velice důležitá volba „Device ID“ (nastavit na hodnotu 1 stejně jako je nastaveno v terminálu) a dále i veškerá nastavení v části „Serial Port 2“. Zde se definuje číslo síťového portu, na kterém bude dostupné sériové rozhraní převodníku (tedy sběrnice RS-485, na kterou je dále napojen docházkový terminál). Pro naše účely bylo ponecháno defaultní nastavení a terminál tak bude přístupný na portu 101. Poslední důležitou položkou je „Baud rate“ definující rychlost komunikace po sériové sběrnici (tedy mezi převodníkem a terminálem). Tato rychlost musí být nastavena shodně v převodníku i docházkovém terminálu (v našem případě zvolena hodnota 19 200 baud/sec).


Obrázek 8.22: Webové rozhraní pro konfiguraci převodníku e-NET E-P132-X

### 8.2.2 Instalace a konfigurace databázového a HTTP serveru

Jak již bylo uvedeno v kapitole 7.2, pro zpracování údajů o docházce z terminálu `RT-300W` poslouží software `ADS 4` od společnosti `RON Software`. Ten pro svoji činnost potřebuje přístup do SQL databáze, kam se ukládají veškerá data načtená z terminálu či vygenerovaná docházkovým softwarem.

Jako databázový server posloužil při realizaci této práce počítač s nainstalovaným softwarem `Microsft SQL Server Express` (IP adresa serveru 192.168.1.240). Z klientského počítače (IP adresa 192.168.1.201) byla pomocí software `Microsoft SQL Server Management Express` vytvořena SQL databáze s názvem „ads_dochazka“. Postup instalace a konfigurace databázového serveru včetně způsobu vytvoření nové SQL databáze je podrobně popsán v návodu [7]. Na obrázku 8.23 je ukázka vytvořené SQL databáze „ads_dochazka“ v software `Microsoft SQL Server Management Express`.




Obrázek 8.23: Správa SQL databáze v Microsoft SQL Server Management Express

Na serverovém počítači je dále nainstalována aplikace HTTP serveru Apache, pomocí nějž je zpřístupněno webové rozhraní (modul `Intraweb` popsaný v kapitole 7.2) docházkového software `ADS 4`. Pro správnou funkci webového modulu je třeba v PHP souboru s názvem „_appdbset.php“ vyplnit přihlašovací údaje k SQL databázi. V našem případě je vyplněno následující:

```
// odbc - mssql
$db_utils = "db/odbc.php";
$db_connectionstring = "ADS";
$db_user ="sa";
$db_password = "acslineadmin";
```

Veškeré konfigurační soubory HTTP serveru, modulu `Intraweb` a exportovaná SQL databáze „ads_dochazka“ jsou uloženy na DVD přiloženém k této práci.

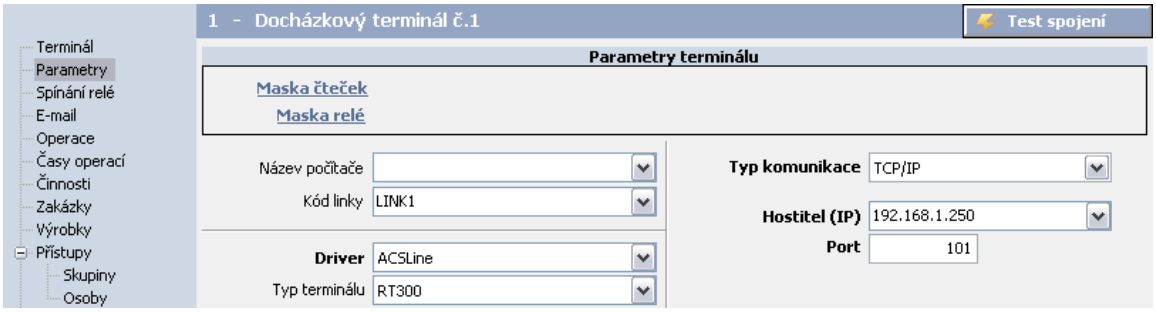
### 8.2.3 Instalace a nastavení docházkového software ADS 4

Při instalaci docházkového software `ADS 4` je třeba zvolit typ, cestu k databázi, její název a přihlašovací údaje. V našem případě se databáze s názvem „ads_dochazka“ nachází na počítači s IP adresou 192.168.1.240. Jako typ zvolíme „SQL server“ a přihlašovací údaje shodné jako byly zvoleny při vytváření databáze na serveru. Tedy uživatelské jméno je „sa“, heslo pak „acslineadmin“. Následně se provede inicializace databáze a software je připraven k použití.

Na základě návrhu provedeného v kapitole 7.2 jsou při realizaci použity doplňkové moduly s názvy „*Intraweb*“ a „*Služba*“. Tyto moduly jsou placené a je nutné je nejprve aktivovat zadáním licenčního čísla v příslušném menu software `ADS 4`.

### Konfigurace docházkového terminálu a definice uživatel

V docházkovém software ADS 4 v menu *Terminály* přidáme novou položku „Docházkový terminál č.1“. Zde nastavíme parametry pro spojení s docházkovým terminálem RT-300W, respektive převodníkem e-NET E-P132-X. Tedy v našem případě typ komunikace (TCP/IP), IP adresu (192.168.1.250) a číslo síťového portu (101).

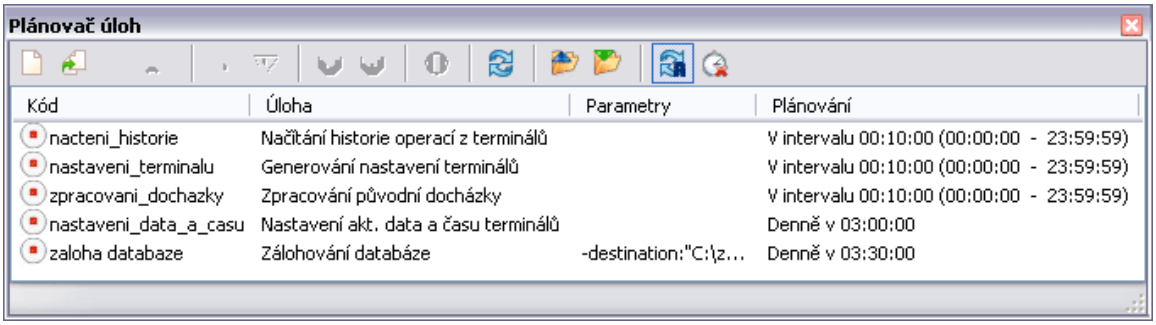



Obrázek 8.24: Nastavení parametrů komunikace s docházkovým terminálem

V software ADS 4 se následně definují uživatelé (menu *Seznamy - Zaměstnanci*), přiřadí se jim příslušný přístupový čip nebo karta (každému stejná jako pro zabezpečovací a přístupový systém Concept) a definují další parametry, jako je druh směny, pracovní pozice a podobně. Dále je možné změnit přiřazení operací tlačítkům na terminálu (příchod, přestávka, odchod, atd.) a provádět různá další nastavení. Nakonec se celá konfigurace pomocí menu *Terminály - Generování nastavení terminálů* odešle do docházkového terminálu RT-300W.

### Konfigurace modulů Intraweb a Služba

Pro konfiguraci zásuvných modulů (v našem případě *Intraweb* a *Služba*) slouží menu *Systém - Nastavení*. Zde se definuje viditelnost dílčích položek menu webového rozhraní pro jednotlivé uživatele a pro každou z nich navíc i detaily zobrazení (např. zda se v informacích o uživateli bude zobrazovat položka titul, adresa a podobně). V nastavení modulu *Služba* je možno definovat automatická spouštění úloh. V našem případě je nastaveno automatické načítání dat z terminálu, zálohování databáze a synchronizace uživatel, data a času.




Obrázek 8.25: Přehled naplánovaných automatických úloh v modulu Služba

Způsob ovládání docházkového software ADS 4 není v této práci z důvodu prostorového omezení dále popisován. Ovládání je však velice intuitivní a vše je podrobně popsáno v dodávaném uživatelském manuálu. Ukázky vzhledu webového rozhraní (modul *Intraweb*) a výstupní tiskové sestavy jsou uvedeny v příloze C.

## 8.3 Kamerový systém

Posledním podsystémem realizovaného SZSOP je kamerový systém s otočnými PTZ kamerami a s možností automatického sledování pohybujícího se objektu. Realizace byla provedena v souladu se specifikací a návrhem z kapitoly 7.3.

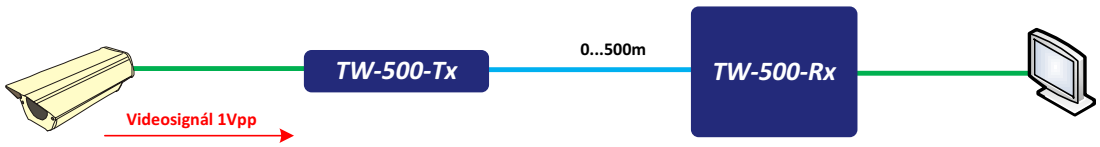
### 8.3.1 Připojení kamer a periferií k záznamovému zařízení

Propojení všech komponent (kamery, klávesnice, HDMI monitor, externí diskové pole) s digitálním záznamovým zařízením `Pinetron PDR-X7016` je realizováno obdobně jako bylo naznačeno na obrázku 7.11.

#### Připojení kamer pomocí twist převodníků Metel TW-500

Vnitřní kamery jsou se záznamovým zařízením propojeny koaxiálním kabelem zakončeným na obou stranách BNC konektory. Pro připojení venkovních kamer, které jsou ve větší vzdálenosti jak 300 metrů je vhodné použít twist převodníky `Metel TW-500` (podrobnější popis byl proveden v kapitole 7.3.5). Způsob zapojení je dobře patrný z obrázku 8.26.

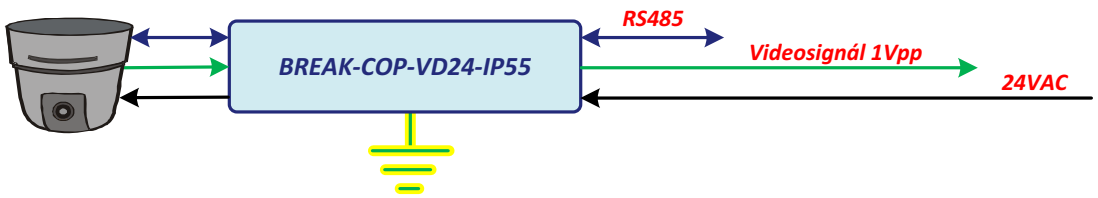
Zelené čáry reprezentují koaxiální kabel (mezi kamerou a vysílací částí převodníku a mezi záznamovým zařízením a přijímací částí převodníku) a modrá pak UTP kabel. Vzdálenost mezi oběma částmi převodníku (tedy v podstatě délka UTP kabelu) může být až 500 metrů a je třeba je napájet napětím 12 V (toto na obrázku není pro zjednodušení znázorněno). Na přijímací části se navíc nachází trimr, kterým je možné vyladit potřebnou úroveň zesílení tak, aby obraz byl i při přenosu na velkou vzdálenost v pořádku.




Obrázek 8.26: Způsob zapojení twist převodníků Metel TW-500 (převzato z [18])

#### Zapojení přepěťové ochrany Metel BREAK-COP-VD24-IP55

Mezi otočné venkovní PTZ kamery a záznamové zařízení jsou zařazeny přepěťové ochrany `Metel BREAK-COP-VD24-IP55`. Ty chrání před případným přepětím sběrnici sériové linky RS-485, napájecí vedení i přenosovou cestu pro video (koaxiální kabel). Více o této přepěťové ochraně bylo napsáno v kapitole 7.3.5. Způsob zapojení je naznačen na obrázku 8.27. Přepěťová ochrana se jednoduše vřadí do příslušných kabeláží, které jsou poté přes ni průchozí. Pro správnou funkci je navíc velice důležité provést řádné uzemnění.




Obrázek 8.27: Ukázka zapojení přepěťové ochrany (převzato z [18])

#### Připojení pevných disků a externího diskového pole

Do záznamového zařízení `Pinetron PDR-X7016` je možno připojit až 4 pevné disky se SATA rozhraním, pokud se odpojí vnitřní DVD mechanika. V našem případě je DVD mechanika ponechána a ke zbývajícím SATA rozhraním uvnitř záznamového zařízení jsou připojeny tři pevné disky. Pro zvýšení celkové záznamové kapacity je navíc přes rozhraní e-SATA připojeno externí diskové úložiště `DAT Optic sBOX-R`, které je osazeno dalšími pěti disky.

Pro záznam je tedy použito celkem 8 pevných disků `Western Digital WD20EURS` o souhrnné kapacitě 16 TB. Parametry záznamu jsou nastaveny následujícím způsobem:

- Je-li na některém videokanálu detekován pohyb, spustí se nahrávání obrazu z příslušné kamery v nejvyšší (*ULTRA*) kvalitě a se snímkovací rychlostí 25 snímků za sekundu.
- V ostatních případech probíhá nepřetržitý záznam videa v kvalitě *HIGH* a se snímkovací rychlostí 6 snímků za sekundu.

Při uvažovaném nastavení způsobu a kvality záznamu tak DVR zařízení umožní zaznamenat od 44 dnů (nejhorší případ, kdy neustále dochází k pohybu) po zhruba 250 dnů (nejlepší případ, kdy nedochází k pohybu před kamerami) nepřetržitého záznamu. Při reálné úvaze, že po souhrnnou dobu 1/3 dne bude docházet k pohybu před kamerami, postačí disková kapacita na nepřetržitý záznam zhruba šesti měsíců videa!

Toto řešení, kdy se nahrává nepřetržitě v menší kvalitě a při pohybu dojde k jejímu navýšení, je velice výhodné. Zaznamenává se tak naprosto vše v dostatečné kvalitě a při zásadní události (jakýkoli pohyb) je kvalita automaticky zvýšena na nejvyšší možnou.

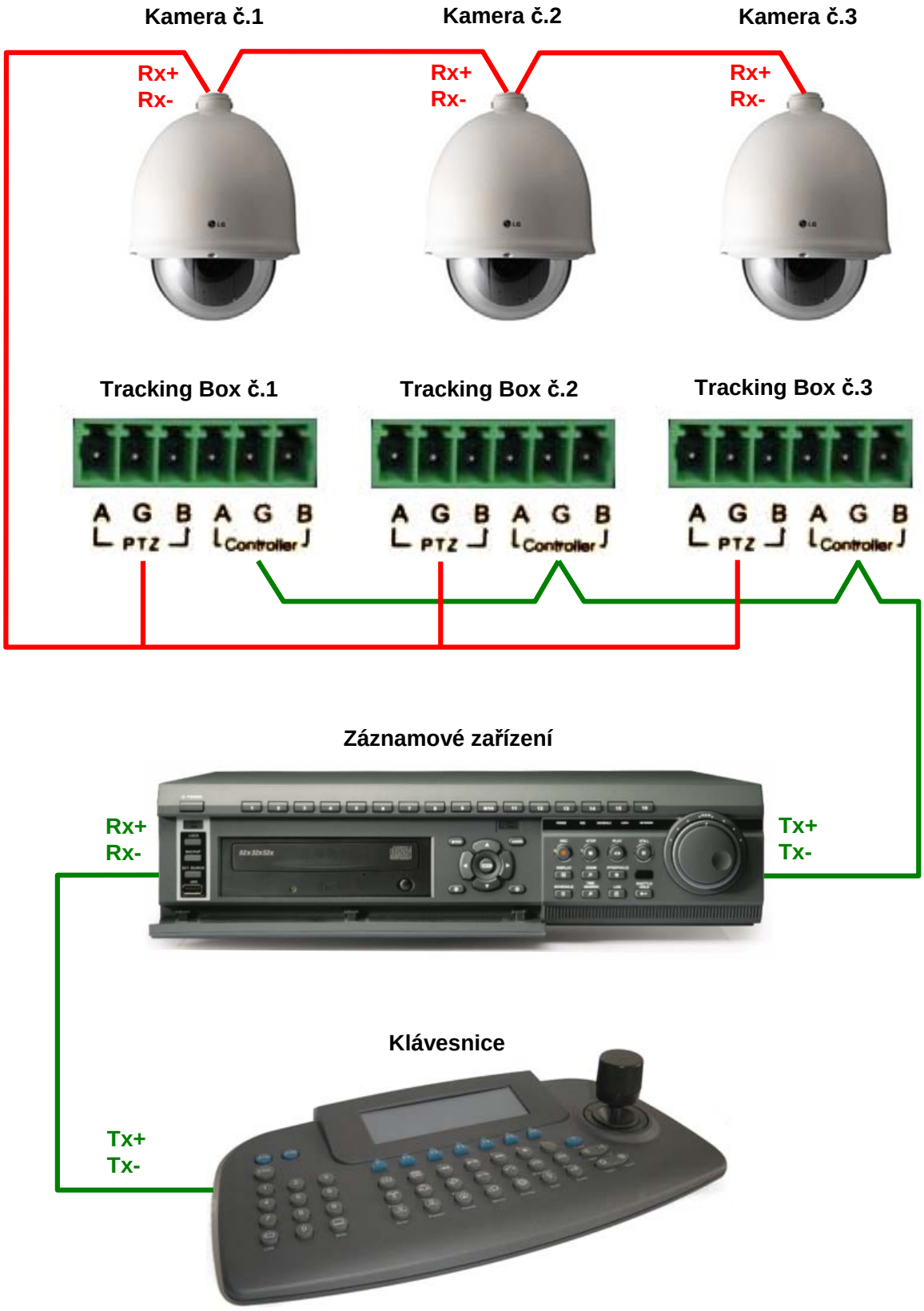
Výše uváděné doby záznamu jsou teoretické a pro jejich odhad byla použita softwarová utilita `HDD Calculator` získaná od výrobce záznamového zařízení. Uvedený software je k dispozici i na DVD přiloženém k této práci.

### 8.3.2 Způsob zapojení otočných PTZ kamer a tracking boxu MF-AT100

Velkou pozornost je třeba při realizaci kamerového systému věnovat zapojení modulů pro automatické sledování pohybu. Jak již bylo podrobně popsáno v kapitole 7.3.4, modul pro automatické sledování pohybu (takzvaný *tracking box*) analyzuje pohyb v obraze z kamery a na základě toho generuje příslušné řídící signály na sběrnici RS-485. Z tohoto je tedy zřejmé, že videosignál z kamery musí být přiveden do *tracking boxu* a z něj dále zapojen na video vstup záznamového zařízení. Stejně tak i sériová linka RS-485 musí být zapojena průchozím způsobem. Díky tomuto zapojení se otočná PTZ kamera která je připojena přes *tracking box* chová v základu jako každá jiná obyčejná PTZ kamera.

Na základě specifikace a následného návrhu je pro ovládání záznamového video rekordéru `Pinetron PDR-X7016` a venkovních otočných PTZ kamer použita i ovládací klávesnice `Pinetron PSD-CJ1000`. Ta se k záznamovému zařízení připojuje opět pomocí sériové linky RS-485. Výsledné zapojení je pak takové, že otočné PTZ kamery (a *tracking boxy*) jsou řízeny záznamovým zařízením a to je ovládáno pomocí klávesnice (samozřejmě je zachována možnost ovládat i napřímo pomocí tlačítek nebo dálkového ovladače).

Naznačení způsobu propojení všech výše zmiňovaných komponent je provedeno na obrázku 8.28. Zelená a červená čára představují kroucené dvojlinky po kterých je vedena komunikace mezi klávesnicí a *tracking boxem* (potažmo *tracking boxem* a kamerami).




Obrázek 8.28: Způsob propojení klávesnice, videorekordéru, tracking boxů a PTZ kamer

#### Nastavení komunikačních parametrů v jednotlivých zařízeních

Aby mohla klávesnice komunikovat se záznamovým zařízením a to potom dále s kamerami či *tracking boxy*, musí mít všechny tyto komponenty nastaven shodný komunikační protokol a přenosovou rychlost. Zároveň platí, že veškerá zařízení připojená na sběrnici RS-485 musí mít nastaveno jedinečné ID v rámci celé sběrnice. Výjimku v tomto ohledu tvoří modul pro automatické sledování pohybu, který naopak musí mít shodné ID s tou PTZ kamerou, kterou má řídit.

Nastavení osmibitového identifikátoru ID, komunikačního protokolu a přenosové rychlosti se na kamerách a *tracking boxech* provádí pomocí DIP přepínačů. Ty se na kamerách `LG LPT-LT903PB` nacházejí na desce s elektronikou a je tak třeba demontovat spodní část krytu. Na modulech `MF-AT100` jsou DIP přepínače umístěny na čelním panelu (viz obrázek 7.14). Nastavení komunikačních parametrů pro záznamové zařízení a klávesnici se provádí v příslušných menu těchto zařízení. Postup nastavení pro DVR je podrobně popsán v manuálu [24], pro klávesnici pak v manuálu [8]. V našem případě mají jednotlivé otočné PTZ kamery (potažmo k nim přiřazené *tracking boxy*) nastaveny *ID 1 až 4*, komunikační protokol *Pelco D* a přenosovou rychlost *9 600 baudů za sekundu*.

Nakonec je ještě třeba vyplnit v záznamovém zařízení v menu „*Kamera*“ pro každý kanál, na který je připojena PTZ kamera, parametry, které jsou v této kameře nastaveny. Poté je možné po maximalizaci zobrazení dané kamery na celou obrazovku a volbě ovládacího PTZ menu kameru ze záznamového zařízení ovládat.

### 8.3.3 Definice prepozic a nastavení modulu MF-AT100

Jak již bylo uvedeno, PTZ je zkratka slov (*Pan-Tilt-Zoom*) a vyjadřuje možnosti pohybu kamery. Konkrétně je tedy možné pohybování ve směru horizontálním, vertikálním a zoomování (plynulá změna ohniskové vzdálenosti objektivu). Při realizovaném zapojení může uživatel s kamerou pohybovat jak pomocí joysticku na ovládací klávesnici, tak prostřednictvím tlačítek na čelním panelu videorekordéru. Dalšími možnostmi je ovládání dálkovým ovladačem, pomocí software (ať už v PC či mobilním telefonu) a přes webové rozhraní.

Před vlastním popisem způsobu nastavení prepozic v kameře a konfigurací *tracking boxu* si vysvětlíme některé důležité pojmy:

**Prepozice** – (*preset*) je uložená pozice PTZ kamery. Obsahuje informace o souřadnicích ve vodorovné a svislé rovině a hodnotu zoomu (zaostření kamery je při libovolném zoomu automatické). Prepozice se ukládají v paměti kamery a zachovávají se i při výpadku napájení.

**Tour** – (*trasa, trasování*) – pomocí ovládacích prvků (DVR, klávesnice, software) lze spustit takzvanou *tour*, nebo-li *pravidelné nepřetržité obíhání presetů*. PTZ kamera se bude tedy neustále v definovaných časových prodlevách (například 10 sekund) přesouvat postupně mezi uloženými presety. Takto lze tedy realizovat například neustálé monitorování prostor okolo celého objektu.

**Cruise** – je vylepšená *tour* (*trasa, trasování*) o schopnost sledování pohybu. Kamera se v každé prepozici zastaví na definovanou dobu stejně jako u *trasování* a v případě, že v obraze není modulem `MF-AT100` detekován pohyb, pokračuje následně dále v *trasování*. V případě pohybu ve snímané scéně je aktivována sledovací funkce *tracking*

*boxu* a ten pak řídí PTZ kameru a snaží se detekovaný pohybující se objekt sledovat. Po ukončení pohybu, nebo po vypršení definovatelného časového intervalu pokračuje kamera dále v *trasování (obíhání presetů)*.

### Uložení prepozic v otočných PTZ kamerách

Před nastavováním *tracking boxu* pro automatické sledování pohybu je třeba mít v kameře již uloženy presety. Nejjednodušším způsobem jak toho dosáhnout je použít ovládací klávesnici. Nejprve zadáme ID záznamového zařízení které chceme ovládat (v našem případě máme jen jedno DVR s ID „1“) a stiskneme tlačítko [DVR]. Následně zadáme ID kamery, kterou chceme ovládat a stiskneme tlačítko [Cam]. Pomocí joysticku poté nasměrujeme a zazoomujeme PTZ kameru tak, aby zabírala námi požadovanou scénu. Poté klávesami zadáme číslo presetu (od 1 do 49) a stiskneme postupně tlačítka [Shift] a [Preset]. Úspěšné uložení prepozice je v obraze kamery potvrzeno zobrazením OSD nápisu „Preset xx“ (kde xx je námi zvolené číslo). PTZ kameru můžeme na uloženou prepozici kdykoli natočit zadáním jejího čísla a stisknutím tlačítka [Preset].

Tímto způsobem si pro každou ze čtyř kamer uložíme potřebný počet presetů, přičemž platí, že plně dostačující počet je do deseti. Kompletní popis možností ovládání záznamového zařízení a kamer pomocí klávesnice `Pinetron PSD-CJ1000` lze nalézt v manuálu [8].

### Nastavení modulu MF-AT100 pro automatické sledování pohybu

Nastavení *tracking boxu* `MF-AT100` se provádí pomocí *OSD menu zobrazeném v obraze z kamery*, která je přes tracking box průchozím způsobem zapojena do záznamového zařízení. Menu se zobrazí po vyvolání presetu číslo 50 z klávesnice, přičemž postup je shodný jako při vyvolání jakékoli jiné prepozice. Prepozice číslo 50 (respektive 50 až 54) je tedy rezervována tracking boxem a v kameře již pak pod touto hodnotou nelze další uložit.

Struktura OSD menu je zobrazena na obrázku 8.29. Pro požadovanou funkci obíhání prepozic a sledování případného pohybu je třeba provést následující nastavení v příslušných částech menu. Informace o jednotlivých volbách byly čerpány z manuálu [16].

Hlavní menu „Main menu“:

**Park time:** Určuje dobu, po jejímž uplynutí dojde k automatickému provedení takzvané „Park action“ (viz dále). Prodlevu je možné nastavit v intervalu 15 sekund až 12 hodin. V našem případě postačí defaultní volba, tedy 15 sekund.

**Park action:** Po vypršení doby „Park time“ (tedy v našem případě 15 s po skončení pohybu, nebo 15 s po ukončení ovládání kamery uživatelem) provede *tracking box* definovanou činnost. V našem případě je požadováno, aby automaticky pokračovalo obíhání presetů se sledováním případného pohybu, což zajistí volba `CRUISE 1`.

Podmenu „Tracking setting“:

**Auto zoom:** Určuje, zda má být při automatickém sledování pohybu prováděno i zoomování. Ponecháme na defaultní volbě `ON`.

**Size sens:** Definuje na jak velký objekt bude *tracking box* reagovat. Jsou dostupné volby `LARGE/MEDIUM/SMALL`. Za velký se považuje objekt zabírající v záběru plochu větší než 1/4 obrazovky a za malý pak takový, jenž v záběru vyplňuje méně než 1/8 obrazovky. Ponecháme volbu `MEDIUM`.

**Gray sens:** Určuje úroveň citlivosti detekce pohybujícího se objektu. Dostupné volby jsou `HIGH/MEDIU/LOW`, ponecháme dobře fungující možnost `MEDIUM`.

**Tracking time (m):** Jedná se o konstantu určující maximální dobu sledování pohybu, bez ohledu na to, že stále probíhá. Je ji možné nastavit na volbu `AUTO`, nebo na hodnotu z intervalu 1 až 15 minut. Za vhodnou dobu lze pro naše účely považovat tři minuty.

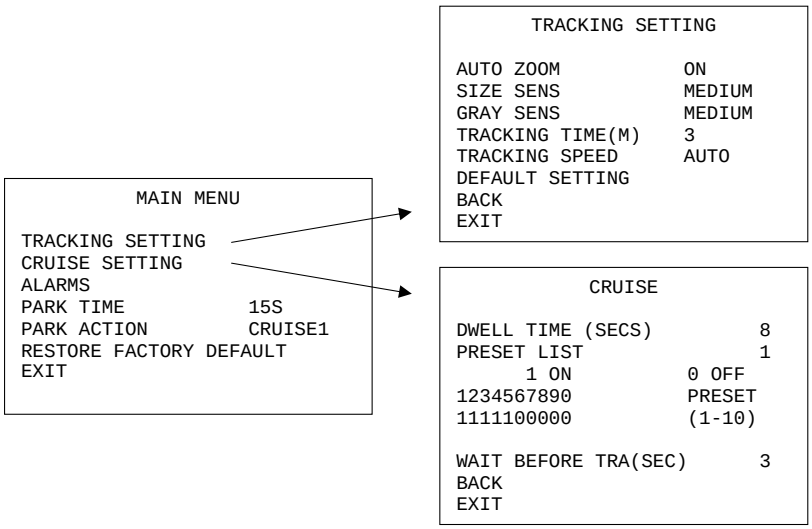
**Tracking speed:** Určuje prahovou rychlost objektu pro detekci pohybu. Možné nastavení je od 1 (pomalé děje) do 5 (rychlé děje) a dobře fungující volba `AUTO`.

Podmenu „Cruise“:

**Dwell time (sec):** Definuje dobu setrvání PTZ kamery na dané prepozici. Po jejím uplynutí přesune *tracking box* kameru na další preset.

**Preset list:** Jedná se o seznam třiceti prepozic, přičemž pro každou jde učit, zda má (nastavíme „1“) či nemá (nastavíme „0“) být zahrnuta do trasování (obíhání presetů).

**Wait before tra(sec):** Určuje časový úsek bezprostředně následovaný po zaslání příkazu k otočení PTZ kamery. Jedná se o dobu, kdy tracking box ignoruje pohyb, který vzniká přesunem kamery na požadovanou prepozici. Nastavíme volbu 3 sekundy, což je dostatečná doba k přesunu mechanismu kamery `LG LPT-LT903PB` o celých 360 °.




Obrázek 8.29: Struktura OSD menu tracking boxu MF-AT100

Tímto způsobem se nastaví každý ze čtyř *tracking boxů*. Následně je třeba u nich trasovací funkci s automatickým sledováním pohybu ještě aktivovat. To se provede vyvoláním presetu číslo 54. Poté každá z PTZ kamer provádí trasování (obíhá presety), přičemž v každé prepozici setrvá 8 sekund. Není-li po tuto dobu detekován *tracking boxem* pohyb, pokračuje PTZ kamera dále na následující preset. Nastane-li v obraze kamery na libovolné prepozici pohyb, *tracking box* jej analyzuje a prostřednictvím řídících povelů zasílaných na sběrnici RS-485 natáčí kameru v jeho směru. Po patnácti sekundách od ukončení pohybu, případně po uplynutí doby 3 minut (viz volba *Tracking time* v podmenu *Tracking setting*) se kamera opět vrátí k trasování se sledováním případného pohybu. Celý proces ovládání PTZ kamer a sledování pohybujících se objektů je tímto způsobem plně automatizován.

### 8.3.4 Nastavení digitálního videorekordéru Pinetron PDR-X7016

Veškerá nastavení digitálního videorekordéru (DVR) `Pinetron PDR-X7016` se provádějí v OSD menu prostřednictvím tlačítek na čelním panelu nebo pomocí dálkového ovladače. Vzhled tohoto OSD menu je zachycen na obrázku 8.30.

Menu je rozděleno celkem do osmi částí, z nichž každá má svoji specifickou roli:

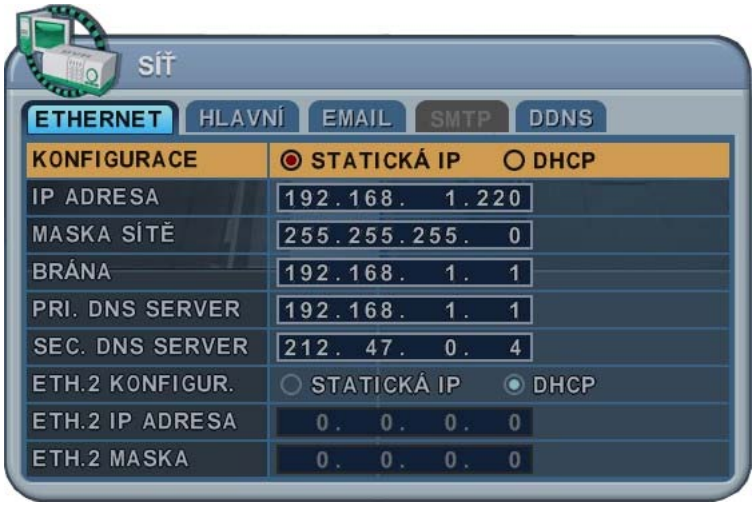
- **Displej** – nastavení způsobu zobrazení, barvy a pozice OSD menu.
- **Kamera** – nastavení jasu, kontrastu, sytosti a komunikačních parametrů PTZ kamer.
- **Záznam** – kvalita a typ záznamu (trvalý, na základě detekce pohybu apod.)
- **Plán** – podrobný týdenní plán způsobů nahrávání.
- **Disk** – formátování a správa disků, monitoring stavu.
- **Síť** – nastavení parametrů počítačové sítě (IP adresa, port, atd.)
- **Zařízení** – veškerá další nastavení jako je například typ ovládací klávesnice, rozlišení VGA a HDMI výstupu a parametry alarmového výstupu.
- **Systém** – nastavení data a času, vytváření uživatelských účtů, upgrade firmware a informace o systému.


Obrázek 8.30: Vzhled menu záznamového zařízení Pinetron PDR-X7016

Kompletní popis všech položek menu a způsobu nastavení a ovládání záznamového zařízení je proveden v manuálu [24]. Soubor se zálohou konfigurace digitálního videorekordéru z realizovaného CCTV systému se nachází na DVD přiloženém k této práci.

### 8.3.5 Správa záznamového zařízení přes software a webové rozhraní

Na obrázku 8.31 je zachyceno menu „Síť“, kde se na záložce „Ethernet“ nastavují parametry síťového rozhraní záznamového zařízení. Pro realizovaný systém je nastavena IP adresa 192.168.1.220 a výchozí brána (IP adresa routeru) 192.168.1.1. Na záložce „Hlavní“ je možné určit číslo portu, přes který se k záznamovému zařízení bude možné připojit jak ze software, tak pomocí webového prohlížeče. Přednastavené číslo portu je 7000 a není důvod jej měnit.




Obrázek 8.31: Nastavení síťového rozhraní DVR zařízení Pinetron PDR-X7016

K záznamovému zařízení se lze připojit několika různými způsoby a sledovat tak živý obraz z kamer, přehrávat pořízené videozáznamy a provádět vzdálenou správu a konfiguraci. Konkrétně je pro tyto účely možno použít následující alternativy připojení:

**Software pro OS Windows** – Pro vzdálenou správu, sledování živého videa a prohlížení či stahování záznamů je k videorekordéru dodáván software `EMS Lite` (*Enterprise Management Suite*). Jeho vzhled je prakticky totožný jako vzhled webového rozhraní (viz příloha C) a navíc je zde možnost připojení k více záznamovým zařízením současně. Instalační soubor tohoto programu je uložen na DVD přiloženém k této práci.

**Software pro MAC OS** – Jmenuje se `iSMS` a platí pro něj prakticky totéž, co pro software pro Windows. Opět je dostupný na přiloženém DVD.

**Webové rozhraní** – Na záznamové zařízení je možno přistupovat i z internetového prohlížeče Internet Explorer (jiné prohlížeče nejsou podporovány, protože webové rozhraní je realizováno jako komponenta *ActiveX*). Webové rozhraní realizovaného systému je ve vnitřní síti dostupné na adrese *http://192.168.1.220:7000*.

**Software pro mobilní telefony** – Přístup ke službám záznamového zařízení je možný i z mobilních telefonů. Podporovány jsou funkce prohlížení živého videa, pohybování s PTZ kamerami a přehrávání záznamů. Software je dostupný pro mobilní platformy *Windows Mobile*, *iOS* (*Apple iPhone*) a *Android*. Ke stažení je na *Android Marketu* (pro telefony s operačním systémem *Android*) a na *App Store* (pro telefony s operačním systémem *iOS*). Název tohoto software je `Mobile CMS` a jeho vzhled na telefonu iPhone 4 je zachycen na obrázku v příloze C.

## 8.4 Počítačová síť

Při realizaci systému zabezpečení a střežení objektů a prostor (SZSOP) bylo použito několik různorodých síťových zařízení. Všechna dílčí síťová nastavení těchto komponent jsou popsána v kapitole 8 zabývající se realizací.

Pro přehlednost je uvedena tabulka 8.2 se souhrnem všech použitých zařízení se síťovým rozhraním, včetně nastavených síťových parametrů.

| **Název zařízení** | **IP adresa** | **Port (lokální)** | **Typ služby** |
|---|---|---|---|
| PC - server EZS/ACS | 192.168.1.201 | 17185 | Server Insight |
| DVR Pinetron PDR-X7016 | 192.168.1.220 | 7000 | Síťové a web.rozhraní |
| Ústředna Concept 4000 | 192.168.1.230 | - | Je v režimu klient |
| PC - server Docházka | 192.168.1.240 | 80<br>1433 | HTTP server<br>SQL server |
| Převodník e-NET E-P132-X | 192.168.1.250 | 80<br>101 | Webové rozhraní<br>Sběrnice RS-485 |

Tabulka 8.2: Přehled síťových nastavení jednotlivých zařízení

### Zpřístupnění vybraných síťových služeb do Internetu

Počítačová síť byla realizována jako lokální za použití switche a nastavením statických IP adres v jednotlivých dílčích zařízeních. Pro praktické použití je vhodné mít některé ze služeb zpřístupněny do Internetu. Jedná se zejména o webové rozhraní docházkového podsystému a rozhraní záznamového zařízení umožňující přístup z počítače (přes software či webové rozhraní) a z mobilního telefonu.

Pro výše uvedené účely lze použít libovolný síťový router (návrh a popis konkrétního zařízení není součástí této práce) a správně jej nakonfigurovat zejména z hlediska *přesměrování portů* (*port forwarding*).

Přehled IP adres a příslušných portů, které je třeba přesměrovat, je uveden v tabulce 8.3. Záměrně zde není IP adresa počítače, na kterém běží server Insight, což je software pro správu systému `Concept`. Tento systém využívá z důvodu většího zabezpečení opačný způsob komunikace. Server se softwarem Insight by tak bylo třeba umístit v oddělené počítačové síti a zpřístupnit na veřejné IP adrese. Ta by se poté zadala přímo do ústředny zabezpečovacího systému `Concept`, jak bylo popsáno v kapitole 8.1.4.

| **Zařízení** | **IP adresa** | **Port (lokální)** | **Port (venkovní)** |
|---|---|---|---|
| DVR Pinetron PDR-X7016 | 192.168.1.220 | 7000 | 7000 |
| PC - server Docházka | 192.168.1.240 | 80 | 80 |

Tabulka 8.3: Přehled portů, které je třeba zpřístupnit do Internetu

# Kapitola 9

# Analýza navrženého řešení SZSOP

Tato kapitola se zabývá analýzou systému pro zabezpečení a střežení objektů a prostor (SZSOP) navrženého a popsaného v kapitolách 7 a 8. Návrh je zde diskutován zejména z pohledu bezpečnosti, dostupnosti služeb, spolehlivosti a cenové náročnosti. Pro větší přehlednost je navržený systém rozdělen na dvě logické části a analýza pak provedena pro každou z nich zvlášť.

## 9.1 EZS, ACS a docházkový systém – analýzy

Analýzy elektronického zabezpečovacího (EZS), přístupového (ACS) a docházkového podsystému jsou provedeny současně. Je to z toho důvodu, že v návrhu byly komponenty těchto podsystémů voleny schválně tak, aby spolu dané podsystémy byly co nejvíce provázány a systém působil jako jeden celek.

### Bezpečnost

Hlavní prvky navrženého zabezpečovacího a přístupového podsystému představují komponenty systému `Concept`. Tento systém byl *ministerstvem obrany ČR* otestován a zařazen do *nejvyššího stupně zabezpečení*, tedy *4 – vysoké riziko*. Příslušný certifikát o posouzení systému `Concept` Ministerstvem obrany ČR je uveden v příloze B.

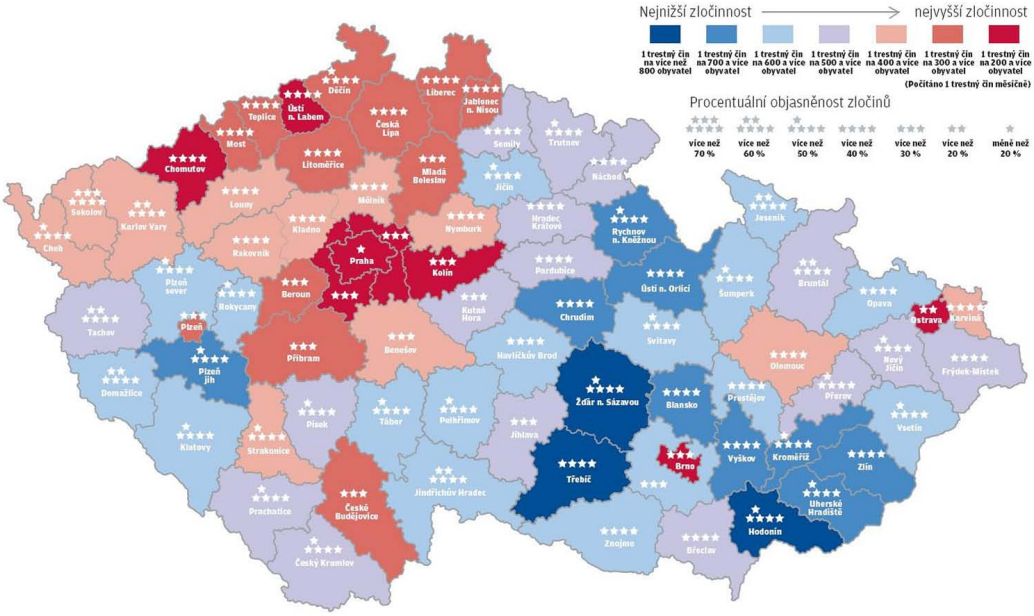
Diskutovaný podsystém je navržen z komponent, které tedy mají certifikaci pro nejvyšší (4.), nebo druhý nejvyšší (3.) stupeň zabezpečení. To samo o sobě ale ještě nevypovídá nic o celkové bezpečnosti systému. Ze všeho nejvíce záleží na způsobu a kvalitě provedení samotné realizace. Teprve, pokud je instalace provedena v souladu s veškerými předpisy a normami, lze hovořit o tom, že zabezpečovací systém je bezpečný a splňuje kritéria určitého stupně zabezpečení.

Největší bezpečnostní riziko pro navržený (respektive obecně jakýkoli) EZS a ACS systém představují samotní uživatelé. Konkrétně jde o problém vyzrazení PINu, či ztráty přístupové karty nebo čipu. Jednou z možností jak se proti tomuto bránit, je zdvojení způsobu autentizace, kdy uživatel musí jednak znát PIN a jednak vlastnit přístupovou kartu. Navíc by mezi uživateli EZS/ACS systému by měl být někdo, kdo bude provádět pravidelné kontroly platnosti karet a občasné změny PIN kódů ostatních uživatel.

U docházkového podsystému, který je z drtivé většiny realizován pomocí docházkového terminálu `ACS Line RT-300W`, nemá cenu bezpečnostní otázku příliš zvažovat. Docházkový podsystém je zcela samostatný a z EZS/ACS systému `Concept` využívá pouze jednu čtečku.

Neexistuje tak žádná možnost, jak by mohl být pomocí docházkového terminálu napadnut EZS/ACS systém `Concept`. Pokud by byl proveden bezpečnostní útok na SQL databázový server, na software, nebo webové rozhraní docházkového systému, dojde v nejhorším případě k získání dat o docházce zaměstnanců. Způsoby jak se proti útokům bránit a jak zabezpečit SQL a HTTP server se tato práce nezabývá.

Zajímavý pohled do problematiky bezpečnosti EZS systémů vnáší takzvaná *mapa zločinu*, která je vyobrazena na obrázku 9.1. Jedná se o vizualizaci statistik krádeží a zločinů páchaných v jednotlivých okresech. Je myslím si bez diskuse, že pravděpodobnost napadení dvou naprosto stejných EZS systémů realizovaných například v Hodoníně a v Praze, se bude značně lišit. I na toto je dobré se při realizaci zaměřit a v regionech s vyšší kriminalitou pak raději volit vždy vyšší stupeň zabezpečení.




Obrázek 9.1: Mapa zločinu v České Republice (zdroj: Lidovky.cz)

### Dostupnost služeb

Na dostupnost služeb u EZS/ACS a docházkového systému lze pohlížet z několika různých úhlů pohledu. Tedy z hlediska dostupnosti hlavních a podpůrných služeb. Dostupnost všech systémově důležitých funkcí EZS/ACS systému je zaručena i v případě výpadku napájení, pomocí záložního akumulátoru. Podpůrnými službami se myslí zejména zasílání SMS zpráv a přístup z Internetu. GSM mobilní síť a přenosové cesty pro přístup k Internetu jsou většinou ve vlastnictví třetích stran (telefonní operátor, poskytovatel Internetu) a jejich stoprocentní spolehlivost a dostupnost tak nejde nikdy zaručit. Toto je možné buďto tolerovat, nebo vyřešit zavedením záložních spojů.

Docházkový terminál a čtečka mohou být při výpadku napájení rovněž provozovány ze záložního akumulátoru. Data o načtených kartách nebo čipech se ukládají přímo ve vnitřní paměti terminálu a do počítače s nainstalovaným docházkovým programem pak mohou být přenesena kdykoli později.

### Spolehlivost

Spolehlivost EZS/ACS a docházkového systému není možné na základě relativně krátkodobého experimentování v rámci diplomové práce určit. Zajímavým vodítkem jsou však statistiky počtů prodaných a následně reklamovaných komponent. Přesná čísla bohužel nemám k dispozici, ale z rozhovorů s obchodníky jisté společnosti (jedna z největších společností v ČR zabývajících se prodejem zabezpečovacích technologií) vyplynulo, že systém `Concept` patří k nejkvalitnějším a nejspolehlivějším zabezpečovacím a přístupovým systémům dostupným na českém trhu.

### Cenová náročnost

Přehled jednotlivých komponent a finanční kalkulace navrženého EZS, ACS a docházkového systému se nachází v příloze E.1. Ceny jsou uvedeny včetně 20 % DPH a byly čerpány z aktuálně platných (květen 2011) ceníků zabezpečovací techniky. Celková cena 337 700 Kč za zabezpečovací, přístupový a docházkový systém se může zdát poměrně vysoká. Je to však dáno tím, že pro návrh byly voleny špičkové komponenty, které nabízí větší bezpečnost a spolehlivost.

## 9.2 CCTV systém – analýzy

Analýzy kamerového (CCTV) systému jsou pro větší přehlednost provedeny odděleně od analýz EZS/ACS a docházkového systému. Důvodem je poměrně velký rozdíl mezi těmito systémy a odlišný pohled na kritéria bezpečnosti.

### Bezpečnost

Otázka bezpečnosti má u kamerových systémů menší váhu než u EZS/ACS systémů. Zatímco napadnutí CCTV systému může vést maximálně k jeho vyřazení z provozu, u EZS a ACS by případně vedlo až k neoprávněnému přístupu do objektu. Kamerový systém je tak v mnohých ohledech možno považovat jen za jakýsi doplňkový systém k EZS.

Pro zajištění správné funkce kamerového systému postačí, aby bylo přítomno napájecí napětí a signál z kamer. Proti výpadku napájení je kamerový systém možno (a doporučeno) zálohovat ze záložního akumulátoru. Odpojení libovolné z kamer dokáže záznamové zařízení detekovat a na tento stav příslušně reagovat. Může být zaslán e-mail, případně sepnut jeden ze 4 alarmových výstupů. Této funkce se doporučuje maximálně využít a alarmový výstup z DVR zařízení mít propojený s EZS ústřednou. V případě výpadku obrazu na libovolné kameře je pak vyhlášen poplach.

Pokud není výše uvedené řešení realizováno, může dojít i k tak absurdní situaci, jako je krádež kamer ze zabezpečeného objektu. V praxi jsem se setkal s instalací CCTV systému na fotovoltaické elektrárně, kde bylo přes noc odcizeno 26 kamer. Systém CCTV po celou dobu nahrával a na záběrech je vidět, jak pachatelé kamery postupně demontují. Pokud by bylo použito výše uvedeného propojení s EZS ústřednou, byl by po odpojení první kamery vyhlášen poplach a díky tomu proti pachatelům včas zakročeno.

DVR zařízení `Pinetron PDR-X7016` je možné připojit do počítačové sítě. Běží na něm *real-time operační systém* (RTOS) unixového typu a úroveň odolnosti proti případnému

napadení by tak měla být vysoká. Co je ale obrovské bezpečnostní riziko je opět samotný uživatel, respektive jeho vyzrazené heslo. Veliké procento (odhadem na základě dlouhodobých zkušeností tak 60 %) uživatelů kamerového systému navíc nezmění tovární heslo pro účet *admin*. To je od výroby nastaveno na *000000* a pokud nebylo změněno, není problém se na zařízení připojit a provést například zastavení záznamu.

#### Dostupnost služeb

Dostupností služeb u kamerového systému lze chápat dva samostatné celky. Jednak se jedná o samotnou funkčnost CCTV systému, jednak o jeho dostupnost v síti či Internetu. První část je možno opět úspěšně řešit použitím záložního napájecího zdroje pro případ výpadku napájení. Co se týče přístupu ze sítě a z Internetu, platí zde totéž, co u EZS/ACS systému. Tedy to, že datové spoje jsou ve vlastnictví třetích stran (telefonní operátor, poskytovatel Internetu) a jejich stoprocentní spolehlivost a dostupnost tak nejde nikdy zaručit.

#### Spolehlivost

Základ kamerového systému tvoří záznamové zařízení `Pinetron PDR-X7016`. Tento výrobce patří na trhu s DVR zařízeními mezi špičku co se kvality a spolehlivosti týče. Totéž platí o výrobcích navržených kamer (tedy LG a KT&C).

Nejméně spolehlivým prvkem CCTV systému jsou tak jednoznačně pevné disky. Používají se klasické 3,5”HDD s rozhraním SATA II. Disky jsou v činnosti nepřetržitě 24 hodin denně, 365 dnů v roce, a to se na nich negativně projevuje opotřebením a poměrně často pak dochází k jejich poruše. Proto je vhodné mít jeden ze čtyř dostupných alarmových výstupů videorekordéru propojen například s EZS systémem a v DVR mít nastaveno, aby spínal při odpojení/poškození pevného disku. EZS systém je pak možné nakonfigurovat tak, aby o sepnutí příslušného vstupu (při poškození HDD) zaslal SMS zprávu. Dalším možností je nechat si informaci o poškození/odpojení HDD zasílat prostřednictvím e-mailů přímo ze záznamového zařízení.

#### Cenová náročnost

Přehled komponent navrženého kamerového systému a jejich finanční kalkulace se nachází v příloze E.2. Ceny byly čerpány z aktuálně platných (květen 2011) ceníků kamerových systémů. Celková cena navrženého CCTV systému je 441 740 Kč včetně 20 % DPH. Může se to sice zdát na první pohled hodně, ale je to dáno tím, že pro návrh byly použity nejkvalitnější dostupné komponenty a moderní prvky (modul pro automatické sledování pohybujícího se objektu). Na druhou stranu je tím zaručena vysoká míra spolehlivosti a z toho plynoucí bezpečnosti.

### 9.3 Nalezené bezpečnostní chyby

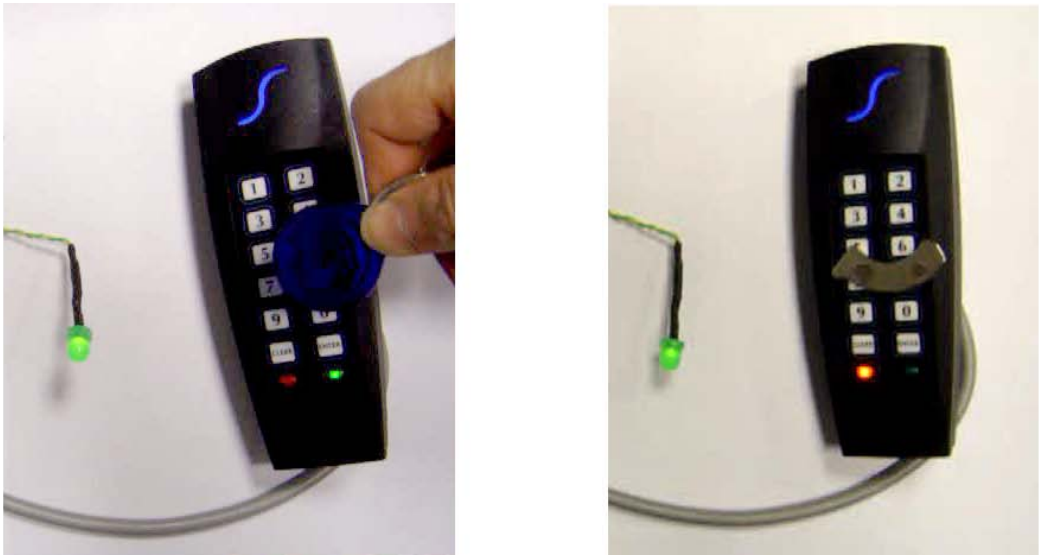
O tom, že žádný systém není nikdy stoprocentně bezpečný, svědčí i tato podkapitola. Během zhruba dvouměsíčního experimentování s realizovanými systémy byly nalezeny 2 bezpečnostní chyby. Jedna byla dokonce natolik závažná, že daná komponenta zabezpečovacího a přístupového systému musela být výrobcem stažena z trhu!

### Nalezená bezpečnostní chyba ve čtečce karet a čipů

V rámci experimentování s realizovaným systémem byl proveden pokus „ošálit“ některou z mnoha testovaných modelů čteček silným permanentním magnetem. Úvaha, proč by to takto mohlo jít, byla založena na jednoduché myšlence. Drtivá většina čteček totiž používá pro spínání výstupu (otevírání dveří) jazýčkové relé, jehož „jazýček“ je magnetický a poměrně slabý.

U jedné z testovaných čteček se pomocí magnetu podařilo dveře otevřít! Byl tedy nalezen obrovský bezpečnostní problém, který by umožnil komukoli, kdo použije permanentní magnet namísto přístupového média (karty nebo čip), přístup do libovolných dveří ovládaných touto čtečkou. Demonstrace tohoto problému je znázorněna na obrázku 9.2. V levé části obrázku je ukázka oprávněného přístupu pomocí načtení přístupového čipu (otevření dveří signalizuje zelená LED dioda vlevo). V pravé části je pak ukázka otevření dveří pomocí přiložení permanentního magnetu na čtečku (otevření dveří opět signalizuje zelená LED dioda vlevo).

Konkrétní typ čtečky, která tuto bezpečnostní chybu obsahuje zde bohužel z důvodu zavázání se výrobci nemůžu uveřejnit. Ten čtečku ihned po oznámení tohoto problému stáhl z prodeje a následně pozastavil její výrobu. To vše až do doby, dokud problém neodstraní. V celém světě je však již provedena spousta instalací, které tuto kombinovanou čtečku s klávesnicí využívají.



Obrázek 9.2: Bezpečnostní chyba čtečky - umožnění přístupu pomocí magnetu

### Nalezená bezpečnostní chyba v DVR Pinetron PDR-X7016

Při hledání bezpečnostního problému u navrženého kamerového systému jsem se zaměřil na nejvíce zranitelné místo, což je prolomení, nebo zjištění přístupového hesla uživatele. Možností jak heslo zjistit je spousta (například sociální inženýrství, slovníkový útok, útok hrubou silou), tato práce se jimi však nezabývá.

Nakonec byla nalezena jistá potenciálně bezpečnostní slabina v XML souboru s exportovaným nastavením záznamového zařízení. Bylo zjištěno, že hesla všech uživatelů (včetně administrátora) jsou v něm uložena formou plaintextu. Pro názornost zde uvádím část obsahu tohoto souboru, kde je heslo administrátora („000000“) přímo vidět:

```
...
<account>
     <admin>
        <user_name value="ADMIN" />
        <activate value="true" />
        <privilege_pb value="true" />
        <privilege_ptz value="true" />
        ...
        <net_password value="000000" />
        <password value="000000" />
     </admin>
</account>
...
```

Rozumnější by rozhodně bylo, kdyby se zde hesla nacházela pouze v šifrované nebo hashované podobě. Výrobce (`Pinetron`) byl na tuto chybu již upozorněn a slíbil rychlé sjednání nápravy. Zatím se tak ale nestalo (květen 2011).

# Kapitola 10

# Závěr

Cílem této diplomové práce byl návrh, realizace a analýza systémů pro zabezpečení a střežení objektů a prostor (SZSOP) obsahujících pokročilé prvky. Na začátku byly nejdříve popsány předpisy, prostředky a postupy používané při návrzích SZSOP. Následně byla provedena neformální specifikace požadavků kladených na navrhovaný sytém. S ohledem na tyto požadavky byl poté proveden návrh systému sestávajícího z několika částí.

Jednu z nich tvoří *elektronický zabezpečovací a docházkový systém (EZS/ACS)*. Návrh byl proveden pro budovu střední firmy o zhruba třiceti zaměstnancích. Použitím vhodně zvolené zabezpečovací ústředny a příslušných komponent byly uspokojeny požadavky na *větší počet podsystémů* a *snadnou správu uživatelů*. Díky velké modularitě lze tento systém v budoucnu *snadno měnit či rozšiřovat*. Pro přístup zaměstnanců či návštěvníků do určených prostor byly použity *čtečky karet a čipů umístěné u dveří*. Systém byl nakonfigurován tak, se co nejvíce *využilo instalovaných PIR detektorů pro spínání světel na chodbě* na základě pohybu. *Ovládání* zabezpečovacího a přístupového systému je možné jednak z klávesnice a jednak *formou SMS zpráv*. Ty mohou být odesílány i *při poplachu a jiných významných stavech systému*. K zabezpečovacímu a přístupovému systému byl navíc přidán modul s ethernetovým rozhraním, díky čemuž je umožněno celý *systém spravovat v rámci počítačové sítě LAN a z Internetu*.

Další část navrženého systému představuje *docházkový podsystém* sloužící k *evidenci docházky zaměstnanců. Docházkový terminál je umístěn u hlavního vchodu* do objektu a k němu připojená čtečka je z praktických důvodů stejná jako u EZS/ACS systému. Data načtená z terminálu jsou ukládána do SQL databáze na serveru a lze je dále zpracovávat pomocí *docházkového programu*. Přístup k veškerým datům a vykonávání operací nad nimi (*souhrnný měsíční výpis odpracované doby, počet hodin přesčasů, generování přehledných tiskových sestav*) je možný i přes *webové rozhraní*, které je zpřístupněno v na stejném serveru, jako SQL databáze. Webové rozhraní je *dostupné v místní síti i z Internetu*.

Poslední část navrženého systému tvoří *kamerový systém se záznamovým zařízením* a šestnácti kamerami. Díky použití externího diskového pole o celkové kapacitě 16 TB lze *uchovávat videozáznamy zpětně po dobu až půl roku*, což je mnohonásobně více, než bylo požadováno. Do návrhu byly zahrnuty i venkovní *otočné PTZ kamery a moduly zajišťující automatické sledování pohybujícího se objektu*. Záznamové zařízení je možné *ovládat z počítače pomocí programu* pro vzdálenou zprávu, nebo přes *webové rozhraní*, případně *z mobilního telefonu*.

Seznam všech komponent navrženého systému pro zabezpečení a střežení objektů a prostor, včetně podrobné finanční kalkulace je umístěn v příloze E.

Navržený systém byl v celé míře realizován formou dvou demonstračních tabel. Jedno představuje realizovaný EZS, ACS a docházkový systém, druhé pak kamerový (CCTV) systém. Při realizaci byly použity a nakonfigurovány naprosto všechny popisované komponenty, jen v menších počtech, než je uvažováno v návrhu. Například pro kamerový systém byly namísto navrhovaných šestnácti kamer použity jen čtyři, tedy od každého typu jedna. Toto je dáno zejména tím, že veškeré prvky realizovaných systémů byly zapůjčeny od jisté obchodní společnosti a z důvodu velmi vysoké souhrnné ceny (řádově statisíce) bylo třeba volit kompromis. Jedinou, zato prakticky zanedbatelnou změnou oproti návrhu, bylo použití přístupového modulu pro jedny dveře (`IRR3000/1`) namísto dvoudveřového (`IRR3000`), avšak způsob použití a konfigurace těchto dvou prvků je prakticky totožný. Důvodem byly opět limitní možnosti zapůjčení komponent.

Činnost a požadované funkce realizovaných podsystémů byly názorně demonstrovány a vše bylo zaznamenáno na videokameru. Sestříhané *videoprezentace* jsou umístěny na přiloženém datovém nosiči, kde se dále mimo jiné nachází i rozsáhlá fotodokumentace. Některé vybrané snímky jsou pak umístěny v příloze D.

Dále byla provedena analýza a diskuze všech navržených podsystémů zejména z hledisek dostupnosti služeb, bezpečnosti, spolehlivosti a cenové náročnosti. Výsledky analýzy jsou uvedeny v kapitole 9 a finanční kalkulace jednotlivých podsystémů pak v příloze E.

Za vlastní přínos lze považovat návrh a následné sestavení komplexního zabezpečovacího systému, složeného z poměrně různorodých komponent a moderních prvků, z nichž některé jsou na trhu teprve velice krátce. Tím je myšleno zejména použití modulu pro automatické sledování pohybujícího se objektu, což je velice zajímavé a užitečné zařízení. Všechny kroky návrhu a realizace byly podrobně popsány a doplněny množstvím illustrací. Díky tomu může tato práce dobře posloužit i jako zajímavý zdroj informací mnoha instalačním firmám zabývajících se problematikou zabezpečovacích, přístupových, docházkových a kamerových systémů. Za obvzvláště přínosné lze považovat objevení obrovské bezpečnostní chyby ve čtečce přístupových karet a čipů kombinované s klávesnicí. Čtečka musela být výrobcem dokonce stažena z prodeje a její výroba byla pozastavena do doby, než se problém podaří vyřešit (viz kapitola 9).

Díky této diplomové práci jsem získal mnoho zkušeností z oblasti návrhu a realizace zabezpečovacích systémů a ověřil jsem si teoretické znalosti získané při tvorbě semestrálního projektu, na nějž tato práce volně navazuje. Zajímavým námětem na rozšíření tohoto řešení by bylo vytvoření jednotného a graficky příjemného webového rozhraní k jednotlivým podsystémům. V současnosti jsou dílčí webová rozhraní dosti nehomogenní, což může případnému uživateli ztěžovat práci se systémem jako celkem. Dalším zajímavým námětem na pokračování v tomto projektu je pokusit se jej co nejvíce převést z analogových technologií do IP. Tím je myšlen zejména kamerový systém, který by mimo automatické sledování pohybu mohl umožňovat i nejrůznější další analýzy, jako je například počítání průchodů, překročení čáry, rozpoznání obličeje, rozpoznání poznávací značky a podobně.

# Literatura


[1] ČSN 33 4590*: Elektrotechnické předpisy. Zařízení elektrické zabezpečovací signalizace.* Praha: Úřad pro normalizaci a měření, 1987.

[2] Pulty centralizované ochrany - efektivní mástroj prevence majetkové kriminality. *Security magazín*, 2000, ročník 7, č. 1-2, str. 6-8.

[3] ČSN EN 50133-1 (33 4593)*: Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky.* Praha: Český normalizační institut, Březen 2001, 28 s.

[4] ČSN EN 50131-1 ed.2 (33 4591)*: Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky.* Praha: Český normalizační institut, 2007, 40 s.

[5] DH servis: *Popis protokolu Wiegand a řešení jeho čtení procesorem – DHSERVIS.cz: Vývoj a výroba elektroniky na zakázku.* [online], 2009, [rev. 2009-12-09], [cit. 2011-04-12].
URL <http://www.dhservis.cz/dalsi_1/wiegand.htm>

[6] ESTELAR s.r.o.: *Docházkový terminál RT300, RT300-B, RT300-F – Návod k obsluze.* [online], [cit. 2011-05-20].
URL <http://helpdesk.estelar.cz/download.php?filename=Manu%E11%20RT300%20v2,25.pdf>

[7] ESTELAR s.r.o.: *Instalace MS SQL Server Express a MS SQL Server Management Express.* [online], [cit. 2011-05-20].
URL <http://helpdesk.estelar.cz/download.php?filename=Instalace%20SQL%202005%20Express%20-%20komplet.pdf>

[8] EUROSAT: *PSD-CJ1000 – Ovládací panel k PTZ kamerám a DVR Pinetron, Instalační a uživatelský manuál.* [online], Verze 1.0, [cit. 2011-03-28].
URL <http://www.eurosat.cz/UserFiles/Manual/CCTV/Pinetron/psd-cj1000_manual_cz_v1.0.pdf>

[9] EUROSAT: *Směrový stropní digitální detektor pohybu DG466 – Instalační manuál.* [online], [cit. 2011-05-08].
URL
<http://www.eurosat.cz/UserFiles/Manual/Paradox/Detektory/dg466.pdf>

[10] HID Global Corporation: *125 kHz Physical Access „How to Order“ Guide.* [online], Květen 2010, [cit. 2011-04-12].
URL <www.hidglobal.com/documents/125khz_htog_en.pdf>

[11] Inner Range: *Unrivalled Integrated Security and Access Control – Product Catalogue 2010 / 2011*. [online], 2011, [cit. 2011-04-11].
URL <http://mirror.innerrange.com/mirror/downloads/Open/Product_Brochures/IR_Catalogue_web.pdf>

[12] JABLOTRON: *Současný stav norem na Poplachové systémy v ČR*. [online], Březen 2000, [cit. 2010-12-27].
URL <www.jablotron.cz/upload/File/legislativa.pdf>

[13] KŘEČEK, S.: *Základy techniky EZS*. Cricetus, 1997, 74 s.

[14] KŘEČEK, S.: *Technická normalizační informace: Komentář k ČSN CLC/TS 50131-7 - Část 1: Návrh EZS*. Praha: Český normalizační institut, 2005, 24 s.

[15] KŘEČEK, S.; MERHAUT, J.: *Elektronické zabezpečovací systémy EZS*. In *Příručka zabezpečovací techniky*, kapitola 3, Cricetus, 2002, iSBN 80-902938-2-4.

[16] Komínek, P.: *MF-AT100 – Instalační a uživatelský manuál*. EUROSAT cs, [online], Verze 1.1, [cit. 2011-03-27].
URL <http://www.eurosat.cz/UserFiles/Manual/CCTV/MF-AT100/mf-at100_tracking_box_manual_cz_%28ver.1.1%29.pdf>

[17] MALÝ, L.: *Návrh metodiky řešení elektronického zabezpečení objektu*. Diplomová práce, FEKT VUT v Brně, 2008.

[18] METEL: *METEL – Katalog 2011-2012*. [online], 2011, [cit. 2011-05-21].
URL <http://www.metel.eu/data/ftp/files/METEL%20Katalog%202011-2012_%20CZ.pdf>

[19] Michálek, M.: *Insight verze 4.2 – Uživatelská příručka*. EUROSAT cs, [online], [cit. 2011-05-14].
URL <http://eurosat.cz/UserFiles/Manual/Concept/Software/insight_4.2_uziv.pdf>

[20] Michálek, M.: *Programovací příručka pro EZS Concept 4000, díl druhý – komunikační úlohy, systém, zabezpečení, modul Ethernet UART*. EUROSAT cs, [online], [cit. 2011-05-07].
URL <http://www.eurosat.cz/UserFiles/Manual/Concept/Hardware/programovaci_prirucka-7.8_2a.pdf>

[21] Michálek, M.: *Programovací příručka pro EZS Concept 4000, díl první – uživatelé, prostory, zóny, moduly, dveře, výtahy*. EUROSAT cs, [online], [cit. 2011-05-07].
URL <http://www.eurosat.cz/UserFiles/Manual/Concept/Hardware/programovaci_prirucka-7.8_1a.pdf>

[22] Michálek, M.: *Systém Concept 3000 / Access 4000 – Instalační příručka, díl druhý – Rozšiřující desky a ostatní moduly*. EUROSAT cs, [online], [cit. 2011-05-07].
URL <http://www.eurosat.cz/UserFiles/Manual/Concept/Hardware/concept_instalacni_dil_2.pdf>

[23] Michálek, M.: *Systém Concept 3000 / Access 4000 – Instalační příručka, díl první – Ústředna a sběrnicové moduly*. EUROSAT cs, [online], [cit. 2011-05-07].

URL <http://www.eurosat.cz/UserFiles/Manual/Concept/Hardware/concept_instalacni_dil_1.pdf>

[24] Pinetron: *PDR-X7016 User's Guide – 16 Channel H.264 Digital Video Recorder.* [online], Verze 1.0, [cit. 2011-03-27].
URL <http://info.pinetron.co.kr/sites/partner/Manual/DVR/X7K/X7K_V1.0_101207.pdf>

[25] RON Software: *Funkce a vlastnosti – RON Software - komplexní řešení v oblasti lidských zdrojů.* [online], 2009, [rev. 2009-03-15], [cit. 2011-04-18].
URL <http://cms.ron.cz/www/cl-600/23-funkce-a-vlastnosti>

[26] SLOUP, P.; LEVÍČEK, V.; KREJČÍ, F.: *Elektrická požární signalizace – EPS.* In *Příručka zabezpečovací techniky*, kapitola 4, Cricetus, 2002, iSBN 80-902938-2-4.

[27] TOMS, L.: *Mechanické zábranné systémy.* In *Příručka zabezpečovací techniky*, kapitola 2, Cricetus, 2002, iSBN 80-902938-2-4.

[28] UHLÁŘ, J.: *Technická ochrana objektů: Elektrické zabezpečovací systémy II.* Vydavatelství PA ČR, 2005, 229 s., iSBN 80-7251-189-0.

[29] UHLÁŘ, J.: *Technická ochrana objektů: Ostatní zabezpečovací systémy.* Vydavatelství PA ČR, 2006, 243 s., iSBN 80-7251-235-8.

[30] VARIANT: *VARIANT plus – Katalog 2010.* [online], 2010, [cit. 2011-01-08].
URL <http://www.variant.cz/src/get.php?id=/DATA/VARIANT%20plus%20-%20Katalog%202010.pdf>

[31] Wikipedia: *Charge-coupled device* – Wikipedia, The Free Encyclopedia. [online], 2010, [rev. 2010-12-17], [cit. 2011-01-06].
URL <http://en.wikipedia.org/w/index.php?title=Charge-coupled_device&oldid=402782100>

[32] Wikipedia: *Infračervené záření* – Wikipedie: Otevřená encyklopedie. [online], 2010, [rev. 2010-11-11], [cit. 2011-01-07].
URL <http://cs.wikipedia.org/w/index.php?title=Infra%C4%8Derven%C3%A9_z%C3%A1%C5%99en%C3%AD&oldid=6070368>

[33] Wikipedia: *JFS (file system)* – Wikipedia, The Free Encyclopedia. [online], 2011, [rev. 2011-03-06], [cit. 2011-03-28].
URL <http://en.wikipedia.org/w/index.php?title=JFS_(file_system)&oldid=417392710>

[34] WWW stránky: Zabezpečovací a kamerové systémy.
URL <http://www.eurosat.cz>

[35] ZAHRÁDKA, J.: *Začínáme s EZS.* [online], 2005, [cit. 2010-12-24].
URL <www.variant.cz/src/get.php?id=/DATA/Zaciname%20s%20EZS.pdf>

# Seznam příloh

**Příloha 1** - Schematické značky EZS dle normy ČSN EN 50131-1 ed. 2

**Příloha 2** - Certifikát Concept

**Příloha 3** - Ukázky webových rozhraní, tiskové sestavy a software

**Příloha 4** - Fotodokumentace realizovaných systémů

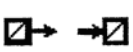
**Příloha 5** - Finanční kalkulace navrženého systému

**Příloha 6** - Adresářová struktura a obsah přiloženého DVD

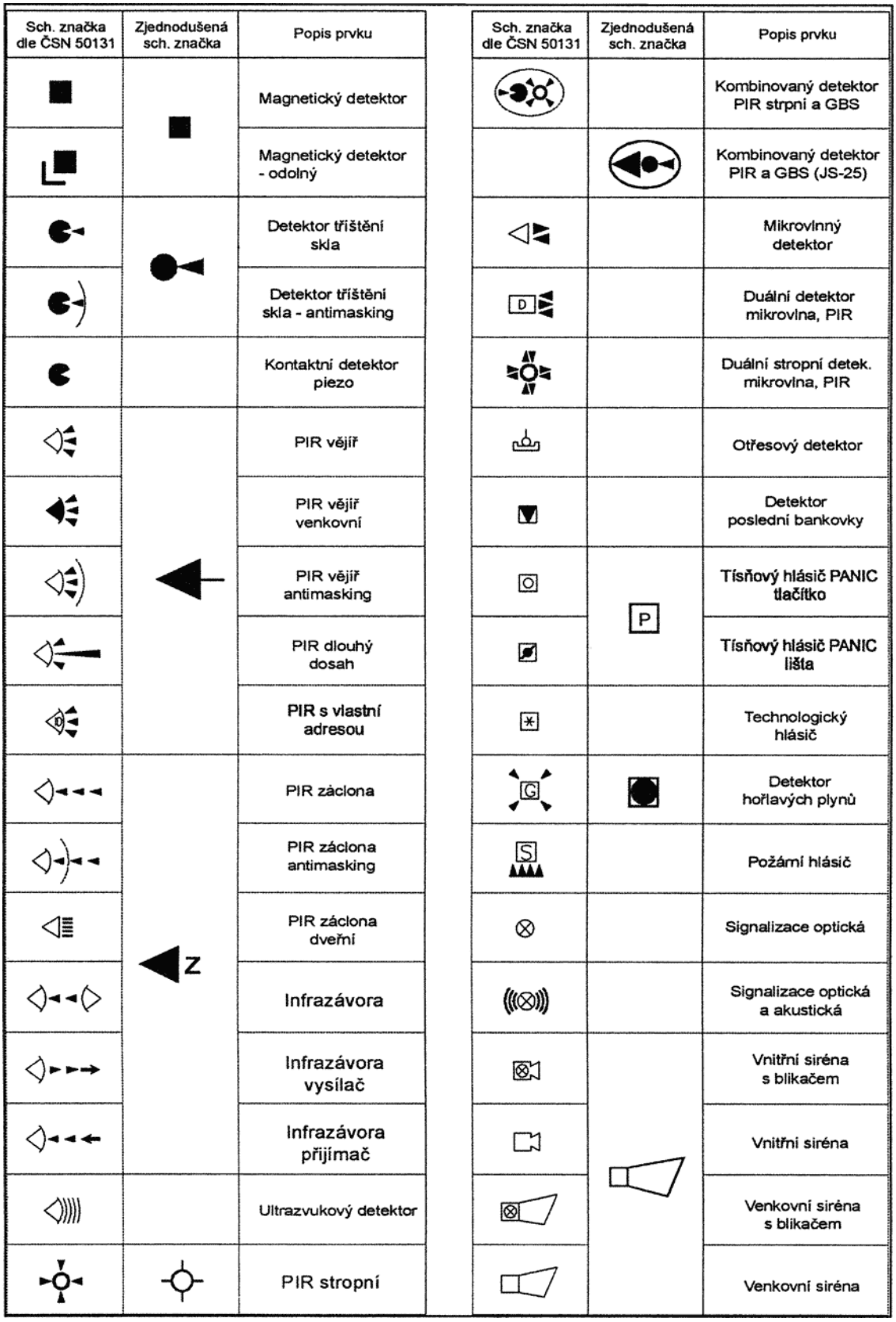
# Příloha A

# Příloha 1 - Schematické značky EZS dle ČSN EN 50131-1 ed. 2

| Sch. značka dle ČSN 50131 | Zjednodušená sch. značka | Popis prvku |
|---|---|---|
|  | | Výstražné zařízení maják |
|  |  | Ústředna EZS |
|  | | Napájecí zdroj |
|  | | Expandér, link. modul koncentrátor |
|  | | Tablo EZS |
|  | | Přenosové zařízení komunikátor |
|  | | Transformátor 220/16 V |
|  | | Záložní akumulátor |
| |  | Přijímač řady UC (216, 220, ...) |
| |  | Expandér řady UC 280 |
| |  | Detektor kouře |

| Sch. značka dle ČSN 50131 | Zjednodušená sch. značka | Popis prvku |
|---|---|---|
|  | | Bezdrátový vysílač, přijímač |
|  | | Klíčový spínač |
|  | | Propouštěcí zámek |
|  | | Ovladač, klávesnice |
|  | | Vstupně-výstupní modul |
|  | | Reléový modul |
| |  | Detektor kouře |
| |  | Vysílač GSM |
| |  | Vysílač PCO |
| |  | Záplavový detektor |
| |  | Vývod kabelu |

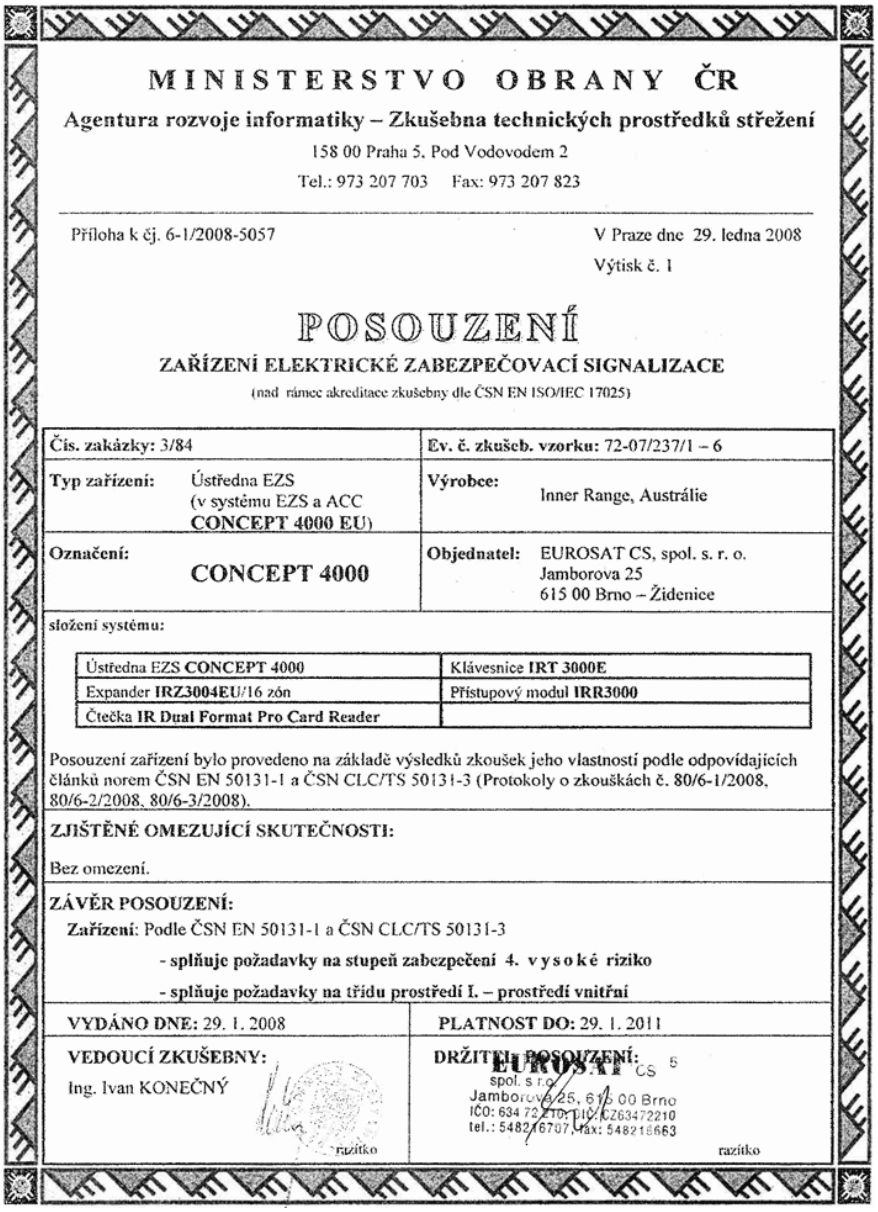
Obrázek A.1: Schematické značky EZS dle normy ČSN EN 50131-1 ed. 2 (převzato z [4])




Obrázek A.2: Schematické značky EZS dle normy ČSN EN 50131-1 ed. 2 (převzato z [4])

# Příloha B

# Příloha 2 - Certifikát Concept



**MINISTERSTVO OBRANY ČR**

**Agentura rozvoje informatiky – Zkušebna technických prostředků střežení**

158 00 Praha 5, Pod Vodovodem 2

Tel.: 973 207 703 Fax: 973 207 823

Příloha k čj. 6-1/2008-5057

V Praze dne 29. ledna 2008

Výtisk č. 1

## POSOUZENÍ

**ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE**

(nad rámec akreditace zkušebny dle ČSN EN ISO/IEC 17025)

| | |
|---|---|
| **Čís. zakázky:** 3/84 | **Ev. č. zkušeb. vzorku:** 72-07/237/1 – 6 |
| **Typ zařízení:** Ústředna EZS (v systému EZS a ACC **CONCEPT 4000 EU**) | **Výrobce:** Inner Range, Austrálie |
| **Označení:** **CONCEPT 4000** | **Objednatel:** EUROSAT CS, spol. s. r. o. Jamborova 25 615 00 Brno – Židenice |

**složení systému:**

| | |
|---|---|
| Ústředna EZS **CONCEPT 4000** | Klávesnice **IRT 3000E** |
| Expander **IRZ3004EU**/16 zón | Přístupový modul **IRR3000** |
| Čtečka **IR Dual Format Pro Card Reader** | |

Posouzení zařízení bylo provedeno na základě výsledků zkoušek jeho vlastností podle odpovídajících článků norem ČSN EN 50131-1 a ČSN CLC/TS 50131-3 (Protokoly o zkouškách č. 80/6-1/2008, 80/6-2/2008, 80/6-3/2008).

**ZJIŠTĚNÉ OMEZUJÍCÍ SKUTEČNOSTI:**

Bez omezení.

**ZÁVĚR POSOUZENÍ:**

**Zařízení:** Podle ČSN EN 50131-1 a ČSN CLC/TS 50131-3

**- splňuje požadavky na stupeň zabezpečení 4. v y s o k é riziko**

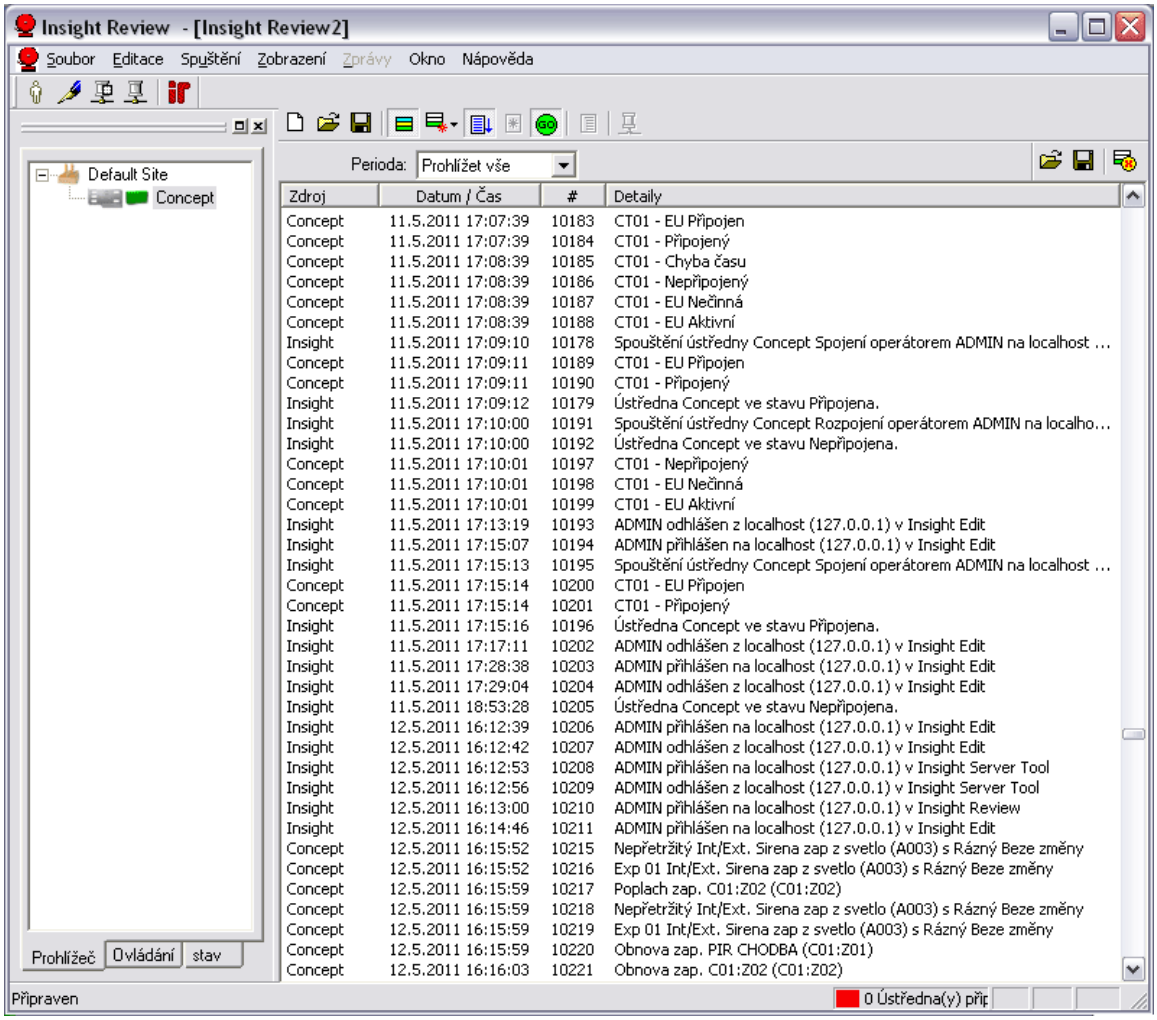
**- splňuje požadavky na třídu prostředí I. – prostředí vnitřní**

| | |
|---|---|
| **VYDÁNO DNE:** 29. 1. 2008 | **PLATNOST DO:** 29. 1. 2011 |
| **VEDOUCÍ ZKUŠEBNY:** Ing. Ivan KONEČNÝ razítko | **DRŽITEL POSOUZENÍ:** EUROSAT CS spol. s r.o. Jamborova 25, 615 00 Brno IČO: 634 72 210, DIČ: CZ63472210 tel.: 5482/6707, fax: 548216663 razítko |

Obrázek B.1: Certifikát o posouzení systému Concept Ministerstvem obrany ČR

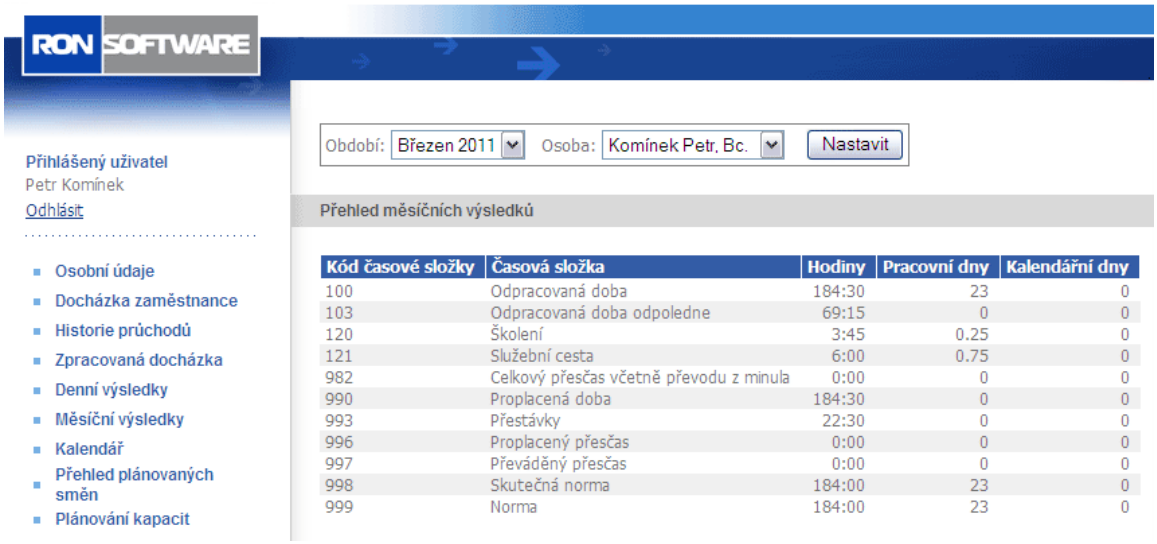
# Příloha C

# Příloha 3 - Ukázky webových rozhraní, tiskové sestavy a software



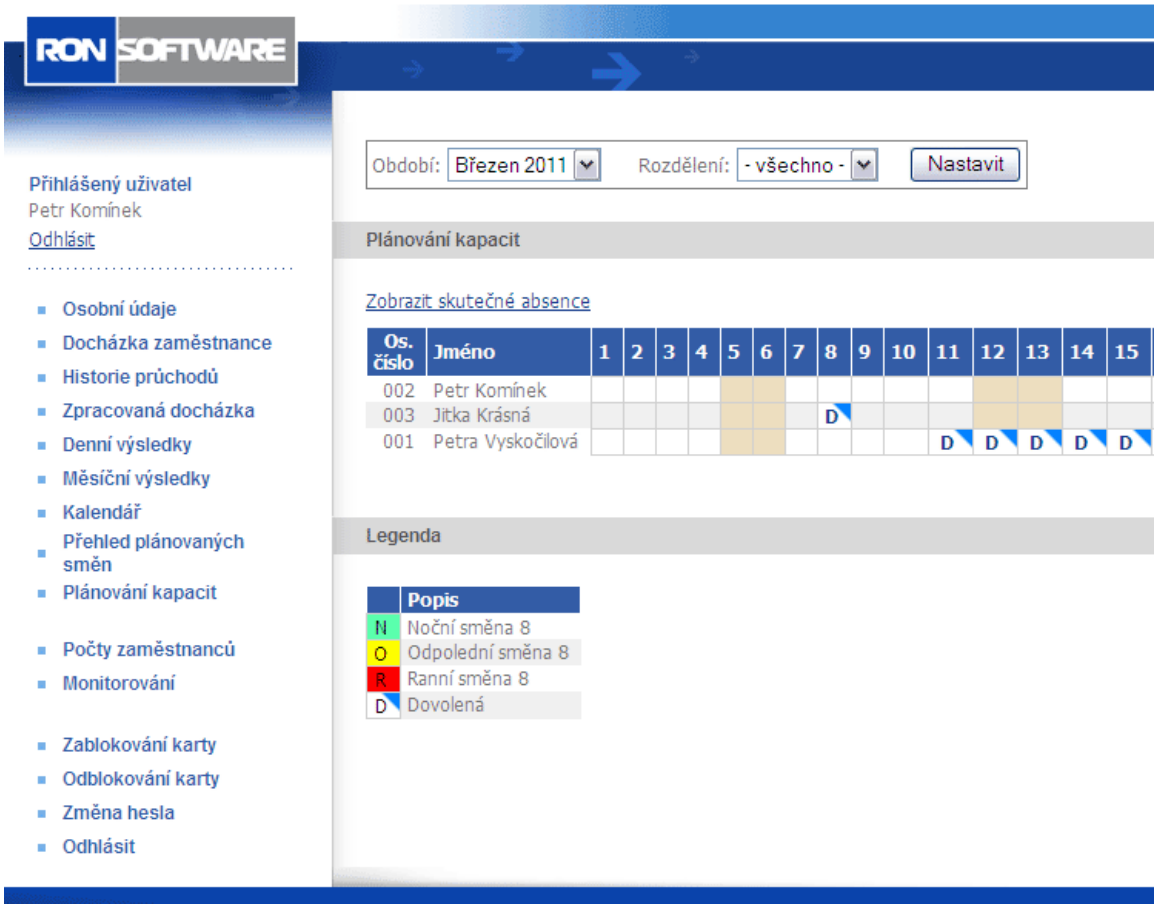

| Zdroj | Datum / Čas | # | Detaily |
|---|---|---|---|
| Concept | 11.5.2011 17:07:39 | 10183 | CT01 - EU Připojen |
| Concept | 11.5.2011 17:07:39 | 10184 | CT01 - Připojený |
| Concept | 11.5.2011 17:08:39 | 10185 | CT01 - Chyba času |
| Concept | 11.5.2011 17:08:39 | 10186 | CT01 - Nepřipojený |
| Concept | 11.5.2011 17:08:39 | 10187 | CT01 - EU Nečinná |
| Concept | 11.5.2011 17:08:39 | 10188 | CT01 - EU Aktivní |
| Insight | 11.5.2011 17:09:10 | 10178 | Spouštění ústředny Concept Spojení operátorem ADMIN na localhost ... |
| Concept | 11.5.2011 17:09:11 | 10189 | CT01 - EU Připojen |
| Concept | 11.5.2011 17:09:11 | 10190 | CT01 - Připojený |
| Insight | 11.5.2011 17:09:12 | 10179 | Ústředna Concept ve stavu Připojena. |
| Insight | 11.5.2011 17:10:00 | 10191 | Spouštění ústředny Concept Rozpojení operátorem ADMIN na localho... |
| Insight | 11.5.2011 17:10:00 | 10192 | Ústředna Concept ve stavu Nepřipojena. |
| Concept | 11.5.2011 17:10:01 | 10197 | CT01 - Nepřipojený |
| Concept | 11.5.2011 17:10:01 | 10198 | CT01 - EU Nečinná |
| Concept | 11.5.2011 17:10:01 | 10199 | CT01 - EU Aktivní |
| Insight | 11.5.2011 17:13:19 | 10193 | ADMIN odhlášen z localhost (127.0.0.1) v Insight Edit |
| Insight | 11.5.2011 17:15:07 | 10194 | ADMIN přihlášen na localhost (127.0.0.1) v Insight Edit |
| Insight | 11.5.2011 17:15:13 | 10195 | Spouštění ústředny Concept Spojení operátorem ADMIN na localhost ... |
| Concept | 11.5.2011 17:15:14 | 10200 | CT01 - EU Připojen |
| Concept | 11.5.2011 17:15:14 | 10201 | CT01 - Připojený |
| Insight | 11.5.2011 17:15:16 | 10196 | Ústředna Concept ve stavu Připojena. |
| Insight | 11.5.2011 17:17:11 | 10202 | ADMIN odhlášen z localhost (127.0.0.1) v Insight Edit |
| Insight | 11.5.2011 17:28:38 | 10203 | ADMIN přihlášen na localhost (127.0.0.1) v Insight Edit |
| Insight | 11.5.2011 17:29:04 | 10204 | ADMIN odhlášen z localhost (127.0.0.1) v Insight Edit |
| Insight | 11.5.2011 18:53:28 | 10205 | Ústředna Concept ve stavu Nepřipojena. |
| Insight | 12.5.2011 16:12:39 | 10206 | ADMIN přihlášen na localhost (127.0.0.1) v Insight Edit |
| Insight | 12.5.2011 16:12:42 | 10207 | ADMIN odhlášen z localhost (127.0.0.1) v Insight Edit |
| Insight | 12.5.2011 16:12:53 | 10208 | ADMIN přihlášen na localhost (127.0.0.1) v Insight Server Tool |
| Insight | 12.5.2011 16:12:56 | 10209 | ADMIN odhlášen z localhost (127.0.0.1) v Insight Server Tool |
| Insight | 12.5.2011 16:13:00 | 10210 | ADMIN přihlášen na localhost (127.0.0.1) v Insight Review |
| Insight | 12.5.2011 16:14:46 | 10211 | ADMIN přihlášen na localhost (127.0.0.1) v Insight Edit |
| Concept | 12.5.2011 16:15:52 | 10215 | Nepřetržitý Int/Ext. Sirena zap z svetlo (A003) s Rázný Beze změny |
| Concept | 12.5.2011 16:15:52 | 10216 | Exp 01 Int/Ext. Sirena zap z svetlo (A003) s Rázný Beze změny |
| Concept | 12.5.2011 16:15:59 | 10217 | Poplach zap. C01:Z02 (C01:Z02) |
| Concept | 12.5.2011 16:15:59 | 10218 | Nepřetržitý Int/Ext. Sirena zap z svetlo (A003) s Rázný Beze změny |
| Concept | 12.5.2011 16:15:59 | 10219 | Exp 01 Int/Ext. Sirena zap z svetlo (A003) s Rázný Beze změny |
| Concept | 12.5.2011 16:15:59 | 10220 | Obnova zap. PIR CHODBA (C01:Z01) |
| Concept | 12.5.2011 16:16:03 | 10221 | Obnova zap. C01:Z02 (C01:Z02) |

Obrázek C.1: Výpis historie událostí ze systému Concept v programu Insight Review




| Kód časové složky | Časová složka | Hodiny | Pracovní dny | Kalendářní dny |
|---|---|---|---|---|
| 100 | Odpracovaná doba | 184:30 | 23 | 0 |
| 103 | Odpracovaná doba odpoledne | 69:15 | 0 | 0 |
| 120 | Školení | 3:45 | 0.25 | 0 |
| 121 | Služební cesta | 6:00 | 0.75 | 0 |
| 982 | Celkový přesčas včetně převodu z minula | 0:00 | 0 | 0 |
| 990 | Proplacená doba | 184:30 | 0 | 0 |
| 993 | Přestávky | 22:30 | 0 | 0 |
| 996 | Proplacený přesčas | 0:00 | 0 | 0 |
| 997 | Převáděný přesčas | 0:00 | 0 | 0 |
| 998 | Skutečná norma | 184:00 | 23 | 0 |
| 999 | Norma | 184:00 | 23 | 0 |

Obrázek C.2: Webové rozhraní docházkového systému – přehled měsíčních výsledků




Obrázek C.3: Webové rozhraní docházkového systému – plánování kapacit

## Výkaz odpracovaných směn (grafický) A

**TESTOVACÍ LICENCE**
**Testovací licence pro Eurosat** **IČO:** 47678526 **Období:** Březen 2011
Náměstí Budovatelů 1405 **DIČ:**
735 06 Karviná - Nové Město **Tel:** 596 312 827 **Vytištěno:** 20.5.2011 23:57:48
**e-mail:** **Uživatel:** ¤

### Bc. Petr Komínek

**Osobní číslo:** 002 **Karta číslo:** 004_privesek **Schváleno do:**
**Skupina:** Skupina všech osob **Kalendář:** K_R8 **Měsíc / rok:** březen 2011

Legenda: Příchod | Přestávka | Služ.cesta | Školení

| Datum | 0 2 4 6 8 10 12 14 16 18 20 22 24 | Odpracoval | Strav | Přesčas | Odpol. | Noční | Svátek | So+Ne |
|---|---|---|---|---|---|---|---|---|
| út 01 | | 8:00 | | | 3:00 | | | |
| st 02 | | 8:00 | | | 3:00 | | | |
| čt 03 | | 8:00 | | | 3:00 | | | |
| pá 04 | | 8:00 | | | 3:00 | | | |
| so 05 | | | | | | | | |
| ne 06 | | | | | | | | |
| po 07 | | 8:00 | | | 3:00 | | | |
| út 08 | | 8:00 | | | 3:00 | | | |
| st 09 | | 8:00 | | | 3:00 | | | |
| čt 10 | | 8:00 | | | 3:00 | | | |
| pá 11 | | 8:00 | | | 3:00 | | | |
| so 12 | | | | | | | | |
| ne 13 | | | | | | | | |
| po 14 | | 8:00 | | | 3:00 | | | |
| út 15 | | 8:00 | | | 3:00 | | | |
| st 16 | | 8:00 | | | 3:00 | | | |
| čt 17 | | 8:00 | | | 3:00 | | | |
| pá 18 | | 8:00 | | | 3:00 | | | |
| so 19 | | | | | | | | |
| ne 20 | | | | | | | | |
| po 21 | | 8:00 | | | 3:00 | | | |
| út 22 | | 8:00 | | | 3:00 | | | |
| st 23 | | 8:00 | | | 3:00 | | | |
| čt 24 | | 8:15 | | | 3:00 | | | |
| pá 25 | | 8:00 | | | 3:00 | | | |
| so 26 | | | | | | | | |
| ne 27 | | | | | | | | |
| po 28 | | 8:00 | | | 3:00 | | | |
| út 29 | | 8:15 | | | 3:15 | | | |
| st 30 | | 8:00 | | | 3:00 | | | |
| čt 31 | | 8:00 | | | 3:00 | | | |
| **Součet** | | 184:30 | 0 | 0:00 | 69:15 | 0:00 | 0:00 | 0:00 |

| | | | |
|---|---|---|---|
| **Neodprac. doba z důvodu nepřítomnosti** | 0:00 | | |
| **Plnění průměru hod. za měsíc** | 184:30 | | |
| **Povinnost odpracovat** | 184:00 | **V měsíci hod - FPD** | **184:00** |
| **Převod do dalšího měsíce** | 0:00 | **Převod z minulého měsíce** | **0:00** |

**Měsíční součty dle časových složek**

| Kód | Popis časové složky | Kal.dny | Prac.dny | Hodiny |
|---|---|---|---|---|
| 120 | Školení | 0 | 0,25 | 3:45 |
| 121 | Služební cesta | 0 | 0,75 | 6:00 |
| 990 | Proplacená doba | 0 | 0 | 184:30 |

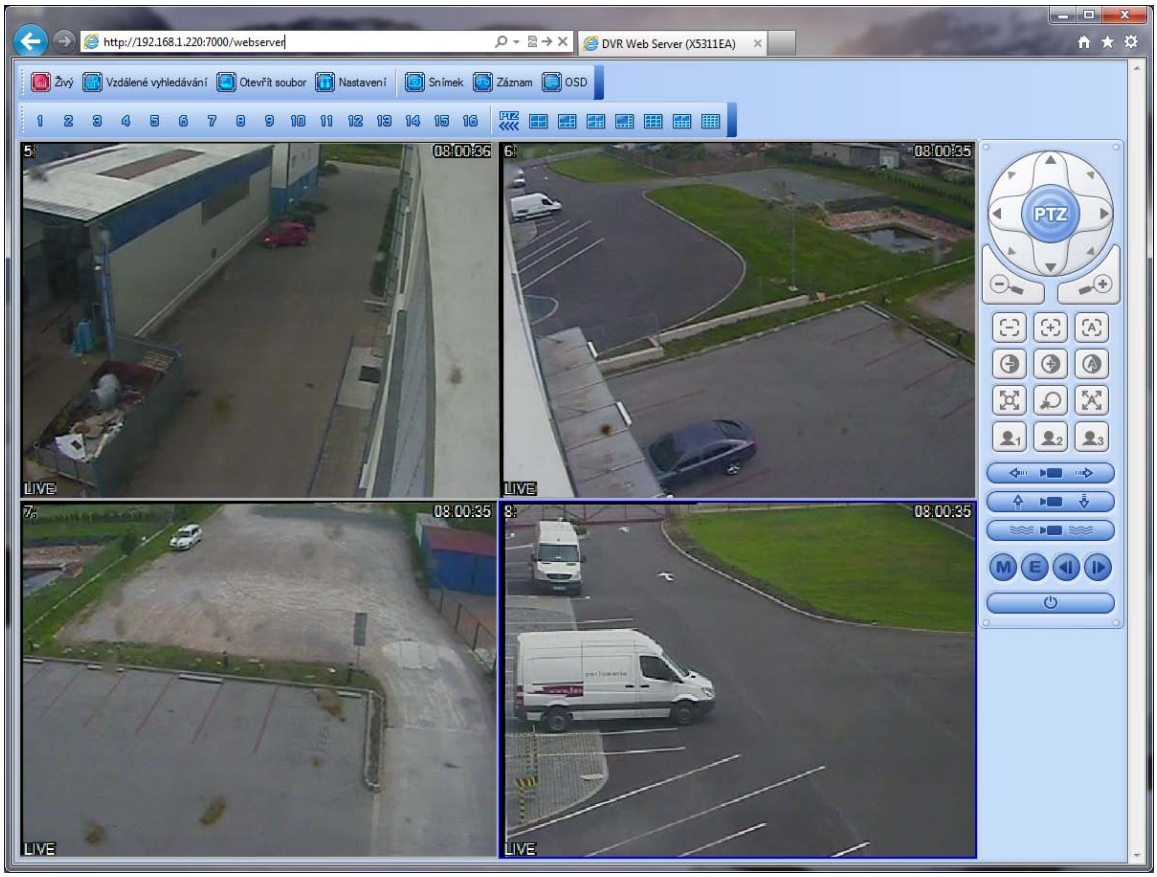
**Mzdové položky vložené v docházce**

| Popis mzdové položky | | Celkem |
|---|---|---|

pracovník . . . . . vedoucí . . . . . .



Obrázek C.4: Ukázka tiskového výstupu programu ADS 4 – výkaz odpracovaných směn

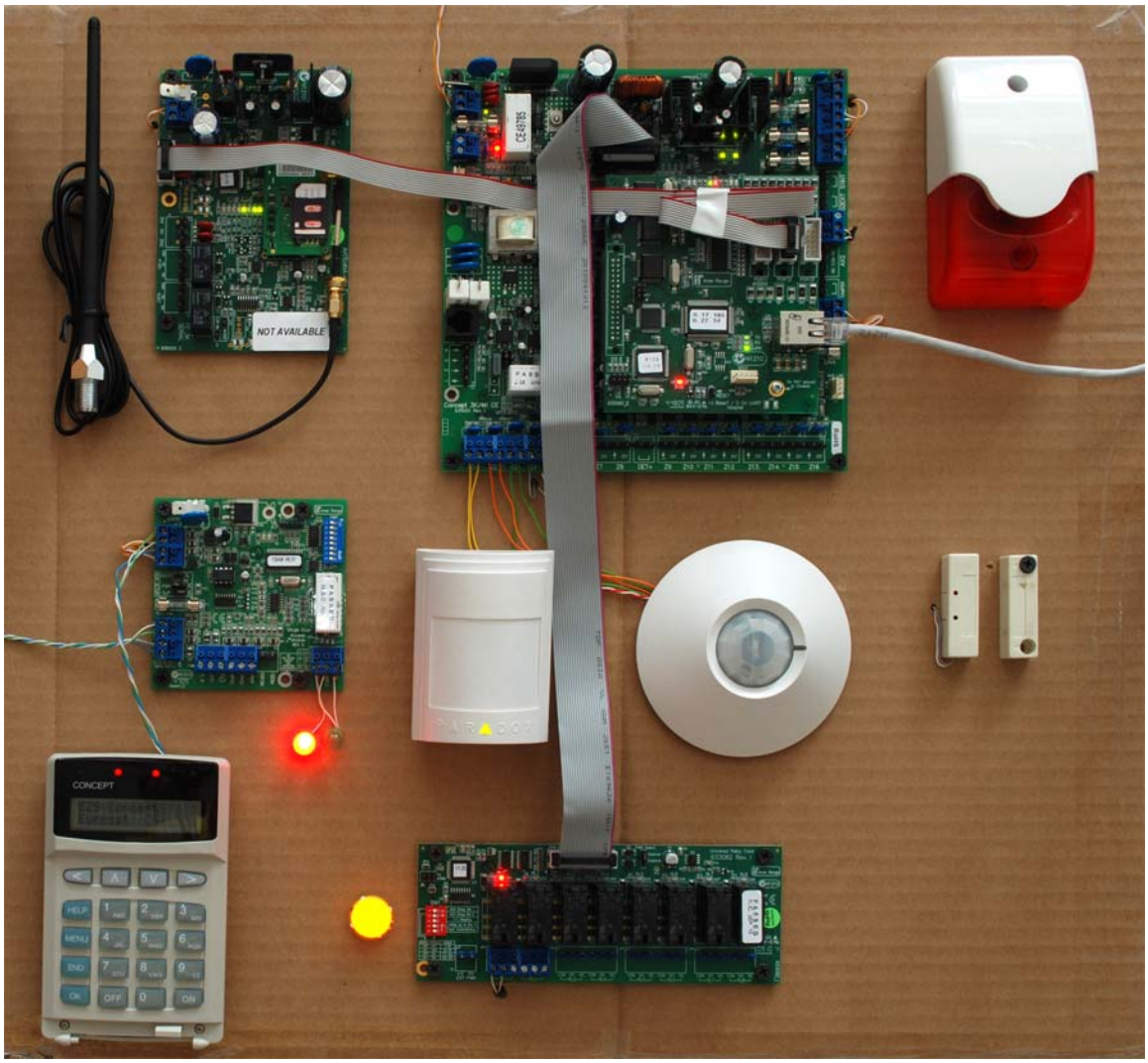



Obrázek C.5: Webové rozhraní záznamového zařízení Pinetron PDR-X7016

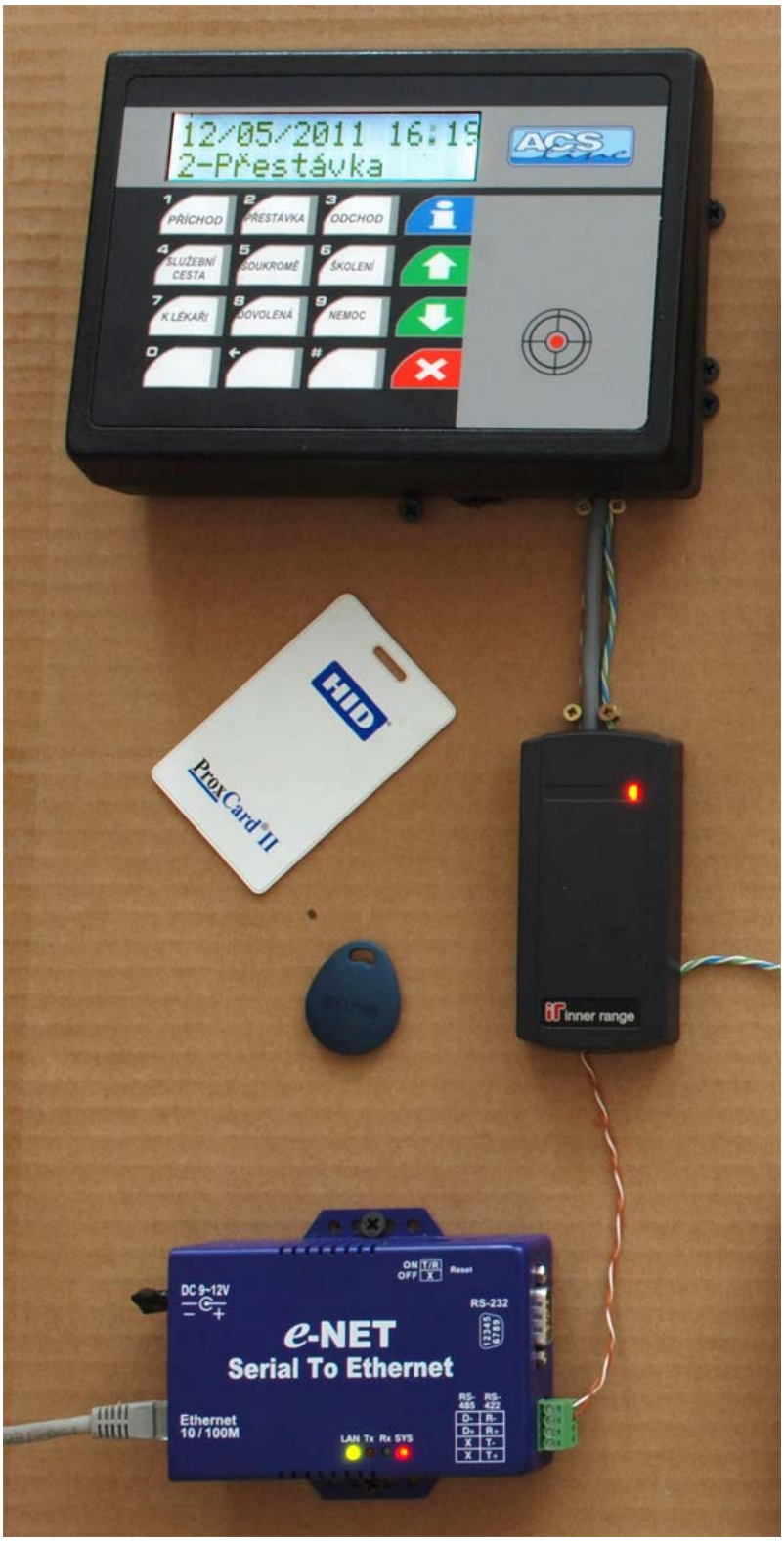

Obrázek C.6: Aplikace Mobile CMS spuštěná na telefonu Apple iPhone 4.

# Příloha D

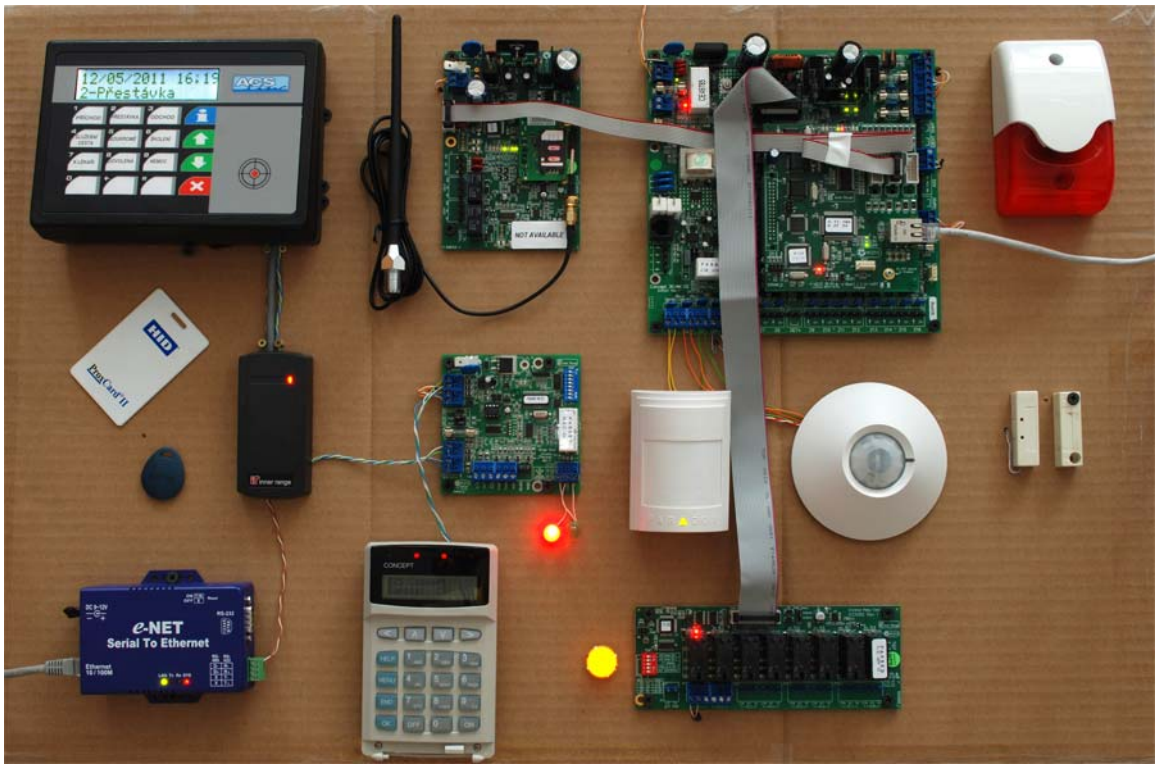
# Příloha 4 - Fotodokumentace realizovaných systémů



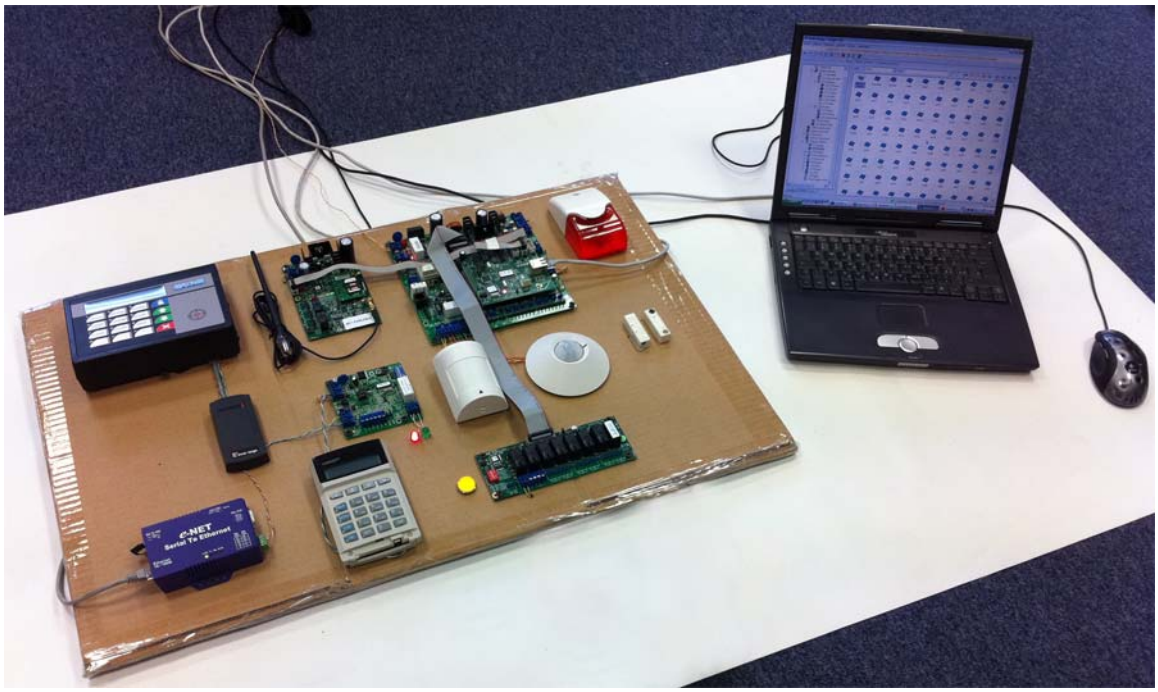

Obrázek D.1: Elektronický zabezpečovací (EZS) a přístupový (ACS) systém




Obrázek D.2: Realizovaný podsystém pro evidenci docházky




Obrázek D.3: Realizovaný zabezpečovací, přístupový a docházkový systém



Obrázek D.4: Kompletní pohled na zabezpečovací, přístupový a docházkový systém

Obrázek D.5: Realizovaný kamerový (CCTV) systém

Obrázek D.6: Realizovaný kamerový (CCTV) systém

# Příloha E

# Příloha 5 - Finanční kalkulace navrženého systému

| Použitá komponenta | Typ/model | Počet | Cena v Kč |
|---|---|---|---|
| Ústředna EZS a ACS systému | IRC4000 EU | 1 | 19 200 |
| Univerzální expandér | IRZ3004 EU EXP/16 | 1 | 11 500 |
| Univerzální expandér | IRZR3082-C | 1 | 3 300 |
| Komunikační deska | IRPX13BaseT | 1 | 14 900 |
| GSM modul | FE3000-S | 1 | 14 900 |
| Přístupový modul pro 2 dveře | IRR3000 | 10 | 9 300 |
| LCD klávesnice | IRT3000-E | 6 | 6 100 |
| Čtečka Inner Range Proximity | Dual-Format reader | 20 | 3 000 |
| Přístupová média (karty) | HID ProxCard II | 80 | 200 |
| Přístupová média (přívěšky) | HID | 50 | 200 |
| PIR detektor | PARADOX 476 Pro | 10 | 270 |
| Stropní PIR detektor | PARADOX DG466 Paradome | 6 | 800 |
| Dveřní PIR záclona | PARADOX 460 Paradoor | 4 | 800 |
| Magnetický dveřní kontakt | SA-200A | 6 | 50 |
| Venkovní zálohovaná siréna | PARADOX PS-128 | 1 | 1 500 |
| Vnitřní siréna | Jablotron SA-913F | 2 | 300 |
| Napájecí transformátor | TRN 16 V / 30 VA | 1 | 350 |
| Zálohovací akumulátor | Alarmguard 12 V / 18 Ah | 1 | 1 150 |
| Instalační boxy | | - | 3 000 |
| Kabeláž, instalační materiály | | - | 2 000 |
| Docházkový terminál | ACS-line RT-300W | 1 | 14 400 |
| Převodník RS-485 - ethernet | e-NET E-P132-X | 1 | 2 500 |
| Docházkový software ADS 4 | SQL verze pro 50 uživatel | 1 | 11 800 |
| Modul do sw ADS 4 | Intraweb | 1 | 6 000 |
| Modul do sw ADS 4 | Služba | 1 | 4 000 |
| *Cena v Kč celkem (včetně DPH):* | | | **337 700** |

Tabulka E.1: Finanční kalkulace navrženého EZS, ACS a docházkového systému

| **Použitá komponenta** | **Typ/model** | **Počet** | **Cena v Kč** |
|---|---|---|---|
| Vnitřní barevná kamera | LG L332-BP | 5 | 9 900 |
| Objektiv Computar | TG4Z-2813-IR | 5 | 1 850 |
| Stropní (dome) kamera | LG L6323-BP | 5 | 9 900 |
| Venkovní kamera s IR | KT&C KPC-N680QPH | 2 | 7 500 |
| Venkovní PTZ kamera | LG LT903PB | 4 | 45 000 |
| Digitální záznamové zařízení | Pinetron PDR-X7016 | 1 | 58 000 |
| Pevný disk SATA HDD | WD WD20EURS | 8 | 2 000 |
| Diskové pole | DAT Optic sBOX-R | 1 | 18 900 |
| Ovládací klávesnice | Pinetron PSD-CJ1000 | 1 | 12 900 |
| LCD monitor 24¨ | Samsung BX2431 | 1 | 5 000 |
| Automatické sledování pohybu | Tracking Box MF-AT100 | 1 | 8 590 |
| Koaxiální kabel a konektory | RG-6U/32CA | 500 m | 600 |
| UTP kabel | Cat.5E | 500 m | 400 |
| Set twist převodníků | Metel TW-500 | 4 | 1 400 |
| Přepěťová ochrana | Metel BREAK-COP-VD24 | 4 | 1 800 |
| Napájecí zdroj | MW DR-120, 12 V DC, 10 A | 2 | 2 250 |
| Napájecí transformátor | TRN 24 V / 30 VA | 1 | 700 |
| Výstražné samolepky | | 5 | 20 |
| *Cena v Kč celkem (včetně DPH):* | | | **441 740** |

Tabulka E.2: Finanční kalkulace navrženého kamerového (CCTV) systému

# Příloha F

# Příloha 6 - Adresářová struktura a obsah přiloženého DVD

| Soubor/adresář | Popis |
|---|---|
| DVD_potisk.pdf | Potisk DVD ve formátu *.pdf |
| README.txt | Soubor s informacemi o adresářové struktuře DVD |
| \01_technicka_zprava | Zdrojový kód v LaTeXu, použité obrázky v plném rozlišení |
| \02_fotogalerie | Fotodokumentace realizovaných systémů a dílčích komponent |
| \03_videogalerie | Video prezentace realizovaných systémů |
| \04_webova_rozhrani | Ukázky webových rozhraní jednotlivých podsystémů |
| \05_konfigurace | Soubory s konfiguracemi jednotlivých podsystémů |
| \06_software | Uživatelský a instalační software k jednotlivým systémům |
| \07_literatura | Literatura a manuály které jsou dostupné v el. podobě |

Tabulka F.1: Adresářová struktura a obsah přiloženého DVD