VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

SYSTÉM PRO ZABEZPEČENÍ A STŘEŽENÍ OBJEKTŮ A PROSTOR

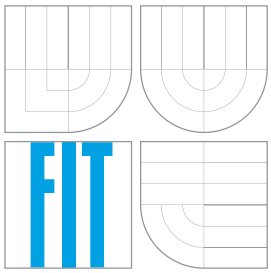
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PETR KOMÍNEK

BRNO 2008

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

SYSTÉM PRO ZABEZPEČENÍ A STŘEŽENÍ OBJEKTŮ A PROSTOR

SYSTEM FOR GUARDING AND SECURING OBJECTS AND AREAS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — PETR KOMÍNEK
AUTHOR

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

BRNO 2008

Zadání bakalářské práce/6892/2007/xkomin04

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav počítačových systémů Akademický rok 2007/2008

Zadání bakalářské práce

Řešitel: **Komínek Petr**
Obor: Informační technologie
Téma: **Systém pro zabezpečení a střežení objektů a prostor**
Kategorie: Vestavěné systémy

Pokyny:

1. Seznamte se s technologiemi používanými při zabezpečení a střežení vnějších a vnitřních prostor (kamery, čidla, světelné závory atd.).
2. Vytvořte specifikaci a s využitím vhodně vybraných technologií z bodu 1 navrhněte blokové schéma systému pro zabezpečení a střežení bytové jednotky včetně jejích okolních prostor.
3. Systém specifikovaný v bodu 2 navrhněte s ohledem na následující požadavky: nízký příkon, snadnost instalace a případných změn struktury systému a jeho komponent, archivace a zasílání uživatelem upřesněných dat.
4. Funkčnost celého systému či jeho vybraných podčástí stanovených po dohodě s vedoucím prakticky ověřte.

Literatura:

- *EZK - elektronika Zdeněk Krčmář* [online]. c2007. http://www.ezk.cz/.
- *FLAJZAR... výroba a prodej elektroniky* [online]. c2005. http://www.flajzar.cz/.
- *GME Česko* [online]. c2007. http://www.gme.cz/.
- *Zabezpečení domů, obbchodů, kanceláří - JABLOTRON - elektronické zabezpečovací systémy*. http://www.jablotron.cz/ezs.php.

Při obhajobě semestrální části projektu je požadováno:

- Bez požadavků (semestrální část obhájena v ak. r. 2006/2007)

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

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% 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: 1. listopadu 2007
Datum odevzdání: 14. května 2008

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

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami

1. Pan

Jméno a příjmení:	**Petr Komínek**
Id studenta:	84308
Bytem:	Přemyslovice 446, 798 51 Přemyslovice
Narozen:	25. 05. 1985, Prostějov

(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta informačních technologií
se sídlem Božetěchova 2/1, 612 66 Brno, IČO 00216305
jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....
(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   bakalářská práce

Název VŠKP:	Systém pro zabezpečení a střežení objektů a prostor
Vedoucí/školitel VŠKP:	Strnadel Josef, Ing., Ph.D.
Ústav:	Ústav počítačových systémů
Datum obhajoby VŠKP:	.....

VŠKP odevzdal autor nabyvateli v:

tištěné formě	počet exemplářů: 1
elektronické formě:	počet exemplářů: 2 (1 ve skladu dokumentů, 1 na CD)

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracování díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizování výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti:
   - □ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

....

Nabyvatel Autor

Abstrakt

Tato práce se zabývá návrhem a realizací elektronického systému pro zabezpečení a střežení objektů a prostor. Návrh je proveden pro malý rodinný domek s ohledem na nízký příkon a snadnost instalace či případných změn struktury systému. Ovládání je možné nejen lokálně, ale i na dálku pomocí sítě GSM a přes Internet. Všechny události jsou zaznamenávány do historie, přičemž o některých vybraných může být uživatel informován zasláním SMS nebo e-mailu. Součástí systému je i modul pro automatizaci a dálkovou správu objektu a nechybí ani kamerový systém s možností přístupu přes Internet. Celá realizace je podrobně popsána, a to včetně ukázek konfigurace jednotlivých komponent.

Klíčová slova

zabezpečení a střežení prostor, elektronický zabezpečovací systém, EZS, zabezpečovací ústředna, detektor, GSM brána, automatizační modul SpringNET, CCTV, DVR, LAN, router

Abstract

This bachelor´s thesis is about design and realization of electronic System for Guarding and Securing Objects and Areas. System is designed for small house. It has low supply, easy mounting and it is possible to change configuration. System can be controlled by keyboard as local or by GSM and Internet as remote. Events are written into history. Also is possible inform the user about events by SMS or E-mail. System includes automation module, object remote controlling and camera's system with Internet connection. Project is described with details about configuration of all components.

Keywords

securing and guarding areas, electronic security system, security control panel, detector, GSM gate, automation module SpringNET, CCTV, DVR, LAN, router

Citace

Petr Komínek: Systém pro zabezpečení a střežení objektů a prostor, bakalářská práce, Brno, FIT VUT v Brně, 2008

Systém pro zabezpečení a střežení objektů a prostor

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Josefa Strnadela, Ph.D. Další informace a odborné rady mi poskytl pan Svatoslav Komínek. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Petr Komínek
13. května 2008

Poděkování

Rád bych poděkoval svému vedoucímu Ing. Josefu Strnadelovi, Ph.D. za jeho vstřícný přístup, ochotu a věcné připomínky. Velký dík patří i panu Svatoslavovi Komínkovi za odborné rady, poskytnutí velkého množství materiálů a zapůjčení jinak poměrně drahých a hůře dostupných komponent.

Obsah

1 Úvod **3**

2 Cíle **4**

3 Způsoby zabezpečení a střežení objektů a okolních prostor **5**
3.1 Mechanické zábranné systémy (MZS) . . . 5
3.2 Elektronický zabezpečovací systém (EZS) . . . 6
3.2.1 Zabezpečovací ústředna . . . 6
3.2.2 Typy zón . . . 8
3.2.3 Základní pravidla pro návrh a užívání EZS . . . 9
3.2.4 Legislativa, stupeň zabezpečení . . . 11
3.3 Elektrická požární signalizace (EPS) . . . 12
3.4 Kamerový systém (CCTV) . . . 13
3.4.1 Kamery a záznamová zařízení . . . 13
3.4.2 Dálkové ovládání kamer . . . 14
3.5 Doplňkové systémy . . . 15

4 Detektory **16**
4.1 Co jsou detektory, základní dělení . . . 16
4.2 Prvky plášťové ochrany . . . 17
4.3 Prvky prostorové ochrany . . . 19
4.4 Prvky perimetrické ochrany . . . 21
4.5 Detektory požární a plynů . . . 21
4.6 Tísňové hlásiče . . . 22

5 Specifikace požadavků na systém **23**
5.1 Specifikace systému pro zabezpečení a střežení . . . 23
5.2 Blokové schéma systému . . . 24

6 Návrh systému **25**
6.1 Analýza požadavků na EZS, výběr vhodných komponent . . . 25
6.1.1 Ústředna EZS . . . 25
6.1.2 Detektory . . . 27
6.1.3 Ostatní prvky . . . 28
6.2 Ovládání a přenos událostí pomocí GSM . . . 28
6.3 Ovládání pomocí LAN/Internetu . . . 29
6.4 Návrh kamerového systému . . . 31
6.5 Požadavky na počítačovou síť . . . 34

7 Realizace systému **35**
7.1 Systém EZS . . . 35
7.1.1 Zapojení drátových detektorů . . . 36
7.1.2 Zapojení bezdrátových detektorů . . . 38
7.1.3 Zapojení sirény . . . 39
7.1.4 Zapojení bezdrátové klávesnice . . . 39
7.1.5 Ovládání pomocí Keyswitch . . . 40
7.1.6 Programovatelné výstupy PGM . . . 40
7.1.7 Programování ústředny . . . 41
7.2 GSM brána . . . 43
7.2.1 Konfigurace pomocí počítače . . . 44
7.2.2 Způsoby využití GSM brány při ovládání EZS . . . 46
7.3 Automatizační modul . . . 48
7.3.1 Síťové nastavení pomocí programu SpringSet . . . 49
7.3.2 Konfigurace a ovládání přes webové rozhraní . . . 50
7.3.3 Způsob použití při ovládání EZS . . . 52
7.4 Kamerový systém . . . 54
7.4.1 Síťová nastavení a odesílání e-mailů . . . 55
7.4.2 Přístup a ovládání přes LAN/Internet . . . 56
7.5 Počítačová síť . . . 58
7.5.1 Nastavení routeru (DHCP, Virtual Server) . . . 58

8 Závěr **60**

Literatura **63**

Seznam příloh **64**

A Příloha 1 - Fotodokumentace **65**

B Příloha 2 - Finanční kalkulace navrženého systému **70**

C Příloha 3 - Adresářová struktura a obsah přiloženého CD **71**

Kapitola 1

Úvod

V dávné minulosti žili lidé dosti primitivně a množství jejich dovedností potřebných k životu nebylo veliké. Každý jednotlivec obstarával potravu, nebo vyráběl nejrůznější nástroje. Většinou z toho dělal buďto pro svoji potřebu, nebo pro blaho všech. Postupem času, jak se lidé zdokonalovali, zvyšovaly se nároky kladené na každého jednotlivce. To přešlo až v potřebu jednotlivé dílčí činnosti mezi sebe rozdělit. Výsledkem byla určitá individuální specializace. Někdo vyráběl oštěpy, zatímco jiný třeba kamenné mísy. To vedlo do jisté míry ke změně způsobu myšlení a lidé tehdy začali využívat služeb *výměnného obchodu*. Pokud ovšem někdo nedokázal vytvořit konkurenceschopný produkt, nemohl očekávat jeho výměnu za jiný, kvalitnější předmět. Prostě a jednoduše, za děravou nádobu vám nikdo kvalitní a ostré kopí nedá.

Z tohoto důvodu se tehdy pravděpodobně vyskytly *první krádeže* a lidé tak začali mít *potřebu si svůj majetek chránit*. Způsoby ochrany se od té doby neustále zdokonalovaly, a to až do jejich současné podoby. Základní principy zůstávají ovšem ve většině případů i nadále stejné. Jen namísto dřevěných kůlů se používají např. mříže a štěkot psů částečně nahradil řev sirén elektronických zabezpečovacích systémů.

Současné způsoby ochrany jsou díky mnohaletému vývoji a zdokonalování na velice kvalitní úrovni. Nejrychlejší rozmach nyní probíhá u *elektronických zabezpečovacích systémů* (dále EZS), jakožto nejmladšího zástupce z této oblasti. Trendem je snaha zařazovat nejrůznější moderní technologie a zvyšovat tak jejich užitnou hodnotu a komfort při ovládání. V souvislosti s tím se v současnosti nejvíce hovoří o využití sítí GSM a Internetu.

Tato práce se zabývá návrhem poměrně kvalitního *systému pro zabezpečení a střežení* menšího objektu a jeho blízkého okolí. Jádro bude tvořit *systém EZS*, jenž bude rozšířen o moduly zajišťující ovládání a komunikaci pomocí sítě GSM a Internetu. Do návrhu bude zařazen i *kamerový systém* s možností nahrávání záznamu. Aktuální dění a pořízený záznam bude možné sledovat na libovolném televizoru připojeném na lokální anténní rozvod. Navíc k němu bude možné přistupovat přes Internet, a to z libovolného počítače a kteréhokoli místa na světě.

Konkrétní cíle, jež si tato práce klade, jsou popsány v kapitole 2. Dále bude následovat krátký přehled nejrůznějších způsobů zabezpečení a střežení (kap. 3) a u vybraných dílčích komponent i jejich stručný popis (kapitola 4). V kapitole 5 bude na základě fiktivního rozhovoru se zákazníkem provedena specifikace požadavků a na základě nich naznačeno blokové schéma systému. Jeho návrhem a realizací se poté budou zabývat kapitoly 6 a 7. Dosažené výsledky a případné náměty na rozšíření budou nakonec shrnuty v kapitole 8.

Kapitola 2

Cíle

Cílem této práce je návrh a realizace *systému pro zabezpečení a střežení* malého rodinného domku včetně jeho okolních prostor. Návrh bude proveden s ohledem na nízký příkon a snadnost instalace. Celý systém by mělo být možné *ovládat pomocí mobilního telefonu a přes Internet*. Rovněž by neměla chybět *historie událostí* a možnost *zasílání SMS zpráv či e-mailů* při definovaných situacích. Součástí návrhu bude i *kamerový systém* s možností pořizování poměrně dlouhého záznamu z barevných kamer. Jelikož bude použito několik síťových zařízení, bude zmíněna i realizace *malé domácí počítačové sítě*.

Práce si klade za cíl čtenáře nejprve seznámit s dostupnými možnostmi pro zabezpečení a střežení objektů (kap. 3). Poté bude proveden přehled nejrůznějších typů detektorů systému elektronické zabezpečovací signalizace. U některých z nich bude vysvětlen princip činnosti (kap. 4). Následovat bude kapitola zabývající se návrhem zmíněného systému. Jednotlivé komponenty budou podrobně popsány a čtenář si udělá kompletní představu o celkové budoucí struktuře (kap. 6). V části týkající se realizace (kap. 7) bude krok za krokem vysvětlen způsob zapojení a nakonfigurování dílčích prvků systému.

Na základě získaných poznatků a případně po dostudování této problematiky z uvedené literatury by měl být čtenář schopný navrhovaný systém sestavit a nakonfigurovat. Posledním dílčím cílem je vytvořit krátkou *video prezentaci* demonstrující možnosti využití realizovaného systému. Ta bude umístěna na přiloženém datovém médiu.

Kapitola 3

Způsoby zabezpečení a střežení objektů a okolních prostor

Zabezpečit majetek proti vniknutí neoprávněné osoby lze různými způsoby. Při výběru toho nejvhodnějšího je třeba brát v úvahu několik faktorů, jako je například typ objektu a způsoby jeho užívání. Napínat kolem rodinného domku plot z ostnatého drátu s vysokým napětím by jistě bylo přehnané, ale například u strategických armádních objektů by mohlo být i toto řešení uplatněno.

Tato kapitola stručně popisuje některé možné způsoby zabezpečení objektů. Vybrané dílčí prvky jsou podrobněji popsány v kapitole 4.

3.1 Mechanické zábranné systémy (MZS)

Pod pojmem mechanické zábranné systémy (MZS) si lze představit všemožné, od nepaměti používané prostředky proti násilnému vniknutí neoprávněných osob. Již naši dávní předkové využívali příkopy a pevné kamenné nebo dřevěné opevnění na obranu svého života a majetku.[1]

Průlomová odolnost MZS

Úkolem mechanických zábranných systémů je narušitele při jejich překonávání co nejvíce zdržet. Nejlépe do doby, kdy je možno provést například fyzický zásah. Jako modelový příklad lze uvést objekt střežený elektronickým zabezpečovacím systémem (EZS) s výstupem na PCO[2] a s mřížemi na oknech. Jejich překonávání pachatelem poskytne dostatečný prostor pro příjezd zasahující bezpečnostní agentury.

Všechny mechanické zábranné systémy jsou v konečném čase překonatelné. Tato doba závisí především na jejich kvalitě a umístění. Určitý vliv na ni má rovněž znalost konstrukce ze strany pachatele, druh použitých nástrojů při překonávání, nebo například možnost použít elektrickou zásuvku.

[1] Dnes o mechanických zábranách uvažujeme už jen z hlediska ochrany majetku.

[2] PCO – Pult Centrální Ochrany je zažitý název pro bezpečnostní agenturu provádějící případný zásah v hlídaném objektu. Více o tomto a o principu elektronického zabezpečovacího systému v kapitole 3.2.

Rozdělení MZS:

Prostředky obvodové ochrany: Jejich úkolem je zajistit bezpečnost prostor kolem objektu. Většinou bývají umístěny na samotné hranici parcely a vytvářejí tak právní hranici pozemku. Nejčastěji jsou to zdi nebo ploty se vstupní brankou či vraty.

Prostředky objektové ochrany: Slouží k zabezpečení všech otvorů, které by mohly být využity pro vstup do objektu. Nejčastěji tedy oken a dveří. Důležitá je kvalita jejich provedení, použití bezpečnostních zámků a mříží, popř. bezpečnostních fólií na sklo.

Prostředky individuální ochrany: Jsou ochranné prostředky, u nichž je kladen důraz především na vysokou průlomovou odolnost. Mohou sloužit k úschově finanční hotovosti, šperků, cenných listin a dokumentů. Patří sem trezory, bankovní schránky, pokladny, ale také bezpečnostní kufry a zavazadla.

O problematice mechanických zábranných systémů podrobněji pojednává publikace [11].

3.2 Elektronický zabezpečovací systém (EZS)

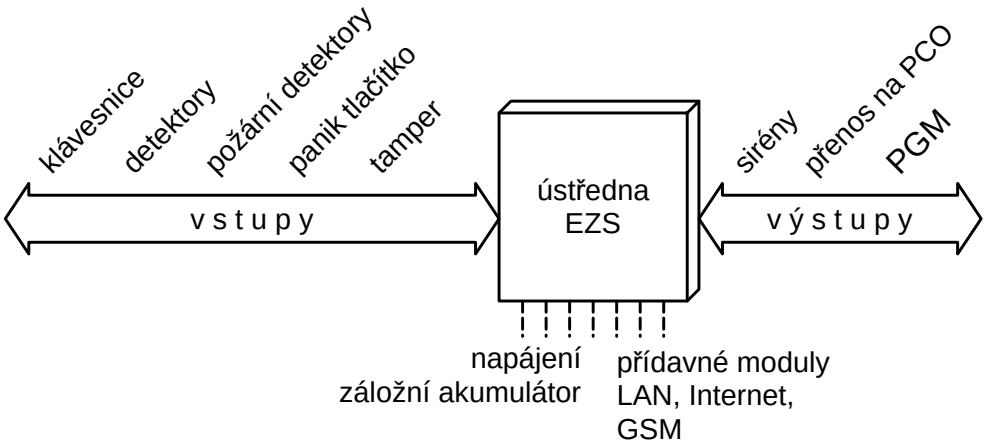
Elektronický zabezpečovací systém EZS slouží k upozornění na narušení hlídaného objektu. Děje se tak pomocí akustické a optické signalizace, tj. poplachové sirény. Siréna umístěná uvnitř objektu působí na narušitele psychicky, zatímco venkovní siréna dá o poplachu vědět širokému okolí. Zprávu o narušení je dále možné přenášet po telefonních linkách, bezdrátově, či pomocí sítě GSM na specializované bezpečnostní pracoviště (PCO), případně dalším určeným osobám. Na poplachový stav je třeba ihned reagovat a zajistit fyzickou ostrahu objektu. O to se může postarat samotný majitel, nebo někdo ze sousedů. Ovšem vhodnější je zásah přenechat bezpečnostní agentuře, případně policii. K tomu je třeba, aby majitel objektu uzavřel smlouvu s vybraným bezpečnostním pracovištěm PCO (Pult Centrální Ochrany). Montážní firma zajistí technickou realizaci propojení střeženého objektu na konkrétní PCO. Od této chvíle jsou pracovníky operačního dozoru nepřetržitě monitorovány veškeré podstatné události systému EZS a v případě narušení je vyslána ozbrojená výjezdová jednotka. V souladu se smlouvou a právními předpisy ČR je provedena kontrola objektu. Pokud se zjistí že došlo ke vniknutí do objektu, jsou podniknuty kroky vedoucí k zajištění pachatele. Majitel objektu je o zásahu informován a v případě poškození bezpečnostních prvků (dveře, okna, EZS apod.) je s ním řešen postup vedoucí k obnovení alespoň nejdůležitějších částí zabezpečení.

Samotný zabezpečovací systém EZS tedy nezabrání narušení objektu a měl by proto být použit jako doplňková ochrana k prvkům mechanických zábran MZS (viz. kapitola 3.1). Právě tyto zábrany hrají rozhodující roli v zabezpečení majetku. Je důležité aby pachateli co nejvíce zkomplikovaly průnik a prodloužily tak dobu narušení.

3.2.1 Zabezpečovací ústředna

Tato kapitola popisuje základní princip funkce zabezpečovací ústředny a jejich periferií. Informace v ní obsažené jsou převážně čerpány z příručky [22].

Jádro EZS tvoří zabezpečovací ústředna, což je deska plošného spoje osazená mikroprocesorem, napájecími obvody a svorkovnicí pro připojení vstupních a výstupních periferií.



Obrázek 3.1: Zjednodušené blokové schéma ústředny EZS

K ovládání a programování ústředny slouží klávesnice. Uživatel může pomocí svého uživatelského kódu zapínat a vypínat střežení objektu. Při zapnutí jsou pomocí detektorů hlídány určené prostory. Detektory nepřetržitě vyhodnocují jevy související s narušením (otevření dveří, pohyb, rozbití skla, atd.) a v případě, že k některému z nich dojde, informují sepnutím relé zabezpečovací ústřednu. Detektory se vyrábí v mnoha provedeních a škála veličin které vyhodnocují je široká. Podrobněji se jim věnuje kapitola 4.

Při narušení je vyvolán poplachový stav, jenž je signalizován sirénou. Pro komunikaci s vnějším světem bývají ústředny vybaveny telefonním komunikátorem, s jehož pomocí lze systém napojit např. na pult centrální ochrany a zajistit tak nad ním nepřetržitý dohled.

Další výhodnou vlastností většiny zabezpečovacích ústředen je programovatelný výstup `PGM`. Typicky bývá k dispozici 1 až 2, ale může jich být i více. V ústředně EZS je možno každému z nich nastavit událost, při které má dojít k jeho sepnutí. Takto je možné docílit třeba automatického uzavření garážových roletových vrat při zapnutí EZS do režimu střežení objektu.

Dle [8] lze ústředny EZS rozdělit na:

- **Ústředny smyčkové** – Každý detektor je připojený do proudové smyčky. K vyhlášení poplachu dojde při změně odporu smyčky aktivací některého z čidel.
- **Ústředny s přímou adresací detektorů** – Komunikace mezi ústřednou a detektory probíhá po datové sběrnici. Minimalizuje se tak množství kabelů v systému.
- **Ústředny smíšeného typu** – Po datové sběrnici probíhá komunikace mezi ústřednou a koncentrátory. Ke koncentrátorům jsou detektory připojeny pomocí smyček jako u smyčkových ústředen.
- **Ústředny s bezdrátovým přenosem od čidel** – Komunikace mezi ústřednou a detektory probíhá bezdrátově na frekvenci 433 MHz. Dosah je 100-200 m. Výhodou je snadná a rychlá instalace.

3.2.2 Typy zón

Pojem „zóna“ a popis jednotlivých typů zón bude pro názornost vysvětlen na nejjednodušší, tedy smyčkové ústředně. Ve smyčkové ústředně je každý detektor zařazen do zóny. Dříve se do každé smyčky připojoval právě jeden detektor a ten tvořil zónu. U současných ústředen lze pomocí zdvojení zón `ATZ` (více v kapitole 7.1.1) připojit do jedné smyčky dva detektory, přičemž každý tvoří samostatnou zónu. Díky tomu se zredukuje počet vstupů ústředny a sníží množství kabeláže.

Jelikož je klávesnice pro ovládání EZS většinou instalována uvnitř střeženého objektu, je třeba určité časové prodlevy mezi zapínacím/vypínacím úkonem a skutečným zapnutím/vypnutím systém. Proto byl zaveden:

- **Odchodový čas** – je prodleva mezi zadáním kódu na klávesnici a skutečným zapnutím systému při níž musí uživatel opustit objekt. Po uplynutí této doby přejde systém do režimu střežení.
- **Příchodový čas** – je doba, za kterou musí uživatel po vstupu do střežených prostor systém vypnout. Příchodový čas se aktivuje jen při vstupu řádnou vstupní cestou, v opačném případě dojde ihned k poplachovému stavu.

Rozeznáváme několik typů zón. Každému detektoru je v ústředně programově přiřazeno jaký typ zóny bude tvořit a podle toho potom zabezpečovací ústředna volí reakci na jeho narušení. O tom, jak se v praxi programují zóny v ústředně se lze dočíst v manuálu [13]. Nejpoužívanější jsou:

Okamžitá zóna: Narušení detektoru při zapnutém stavu systému způsobí okamžitý poplach. Nejčastěji se používá při střežení vnitřních prostor a oken.

Zpožděná zóna: Při narušení detektoru tvořícího zpožděnou zónu je aktivován příchodový čas. Během této doby musí dojít k vypnutí systému platným uživatelským kódem, jinak nastane po uplynutí příchodového času poplach.

Podmínečně zpožděná zóna: Pokud je narušena během příchodového času, chová se jako zpožděná. V opačném případě dojde k okamžitému poplachu. Požívá se např. pro detektor hlídající prostor klávesnice.

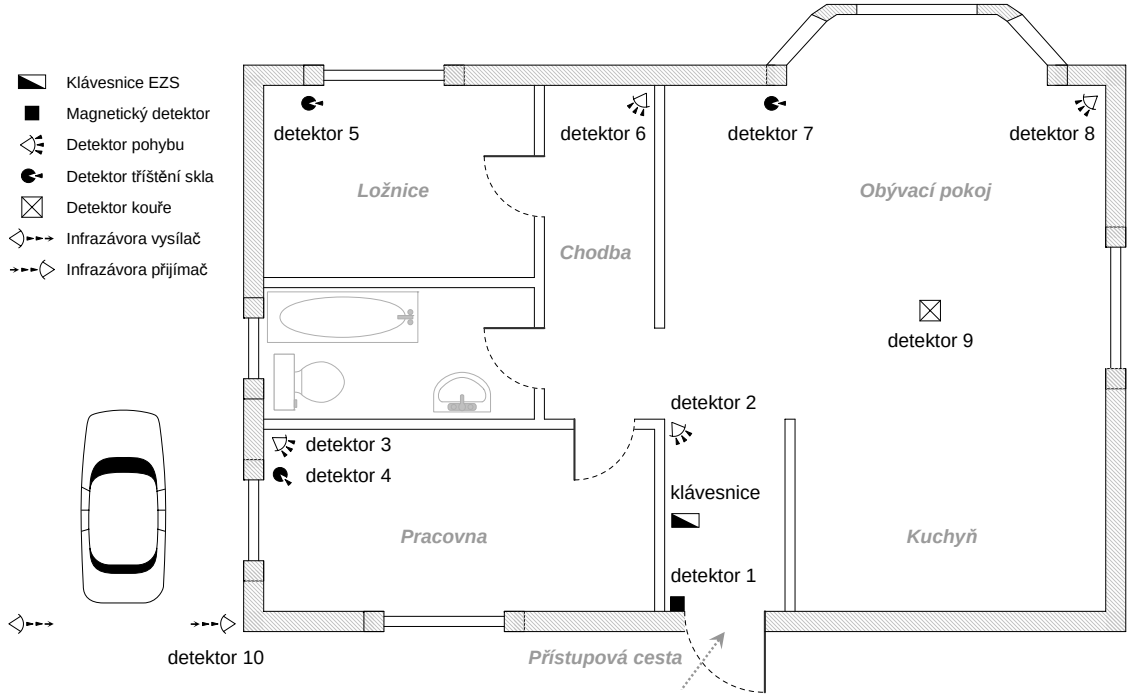
24 hodinová zóna: Její narušení vyvolá okamžitý poplach, a to bez ohledu na to, zda byl systém EZS zapnut do režimu střežení či nikoli. Používá se většinou pro sabotážní kontakt na víku zabezpečovací ústředny. Při otevření je aktivován poplach a zabrání se tak jakémukoli neoprávněnému zásahu do systému EZS. Dalším příkladem použití může být tzv. `PANIK` tlačítko, kterým vyvolá obsluha poplach při přepadení nebo v tísni.

Požární zóna: Chová se totožně jako 24 hodinová, pouze s rozdílem, že poplach je signalizován přerušovaně. Jak již název napovídá, do této zóny se zařazují výlučně požární detektory.

Plášťová (STAY): Při zapnutí systému EZS v režimu `STAY` (plášťová ochrana) jsou zóny označené jako `STAY` vyřazeny z hlídání. Při běžném režimu střežení se chovají jako okamžité. Plášťová ochrana je velice užitečná třeba při hlídání bytových prostor přes noc. Detektory v místnostech kde se předpokládá pohyb uživatelů objektu jsou ignorovány, zatímco ostatní reagují dle nastavení.

3.2.3 Základní pravidla pro návrh a užívání EZS

Tato kapitola popisuje využití různých typů zón při realizaci systému EZS a na konkrétních situacích vysvětluje chování zabezpečovacího zařízení při užívání objektu.



Obrázek 3.2: Využití zón v systému EZS

zóna 1	zpožděná		detektor 1
zóna 2	podmínečně zpožděná	`STAY`	detektor 2
zóna 3	okamžitá		detektor 3
zóna 4	okamžitá		detektor 4
zóna 5	okamžitá		detektor 5
zóna 6	okamžitá	`STAY`	detektor 6
zóna 7	okamžitá		detektor 7
zóna 8	okamžitá	`STAY`	detektor 8
zóna 9	požární		detektor 9
zóna 10	okamžitá		detektor 10

Zapnutí systému – režim střežení (ARM): Zabezpečovací ústředna testuje před zapnutím všechny zóny zda jsou v klidu. Dokud tomu tak není, nelze systém zapnout. Tímto se ověří, že jsou uzavřeny všechny hlídané dveře a zabrání se možnosti zapomenout v objektu zvíře či další osobu. Po uklidnění všech zón a zadání platného kódu na klávesnici začne běžet odchodový čas, do jehož vypršení je třeba opustit objekt. Poté je systém EZS zapnut v režimu střežení (`ARM`).

Vypnutí systému – režim střežení (DISARM): Celý systém musí být navržen tak, aby se v režimu střežení nebylo možné ke klávesnici dostat jinak, něž tzv. *přístupovou cestou*. Otevřením vstupních dveří dojde k narušení *zpožděné zóny 1* (rozpojením magnetického kontaktu) a tím k aktivaci příchodového času. Do vypršení časového limitu musí být zadán platný kód pro vypnutí systému. Je třeba si všimnout faktu, že při pohybu ke klávesnici dojde k narušení *detektoru zóny 2*, a to ještě před možností vypnutí. Proto musí být i tato zóna nastavena jako zpožděná, nebo ještě lépe podmínečně zpožděná. V praxi to znamená, že aktivace *detektoru 2* způsobí poplach jen v případě, že k ní nedošlo ve chvíli, kdy běží čas pro příchod. Tato situace nastane při použití jiné než přístupové cesty, např. při vloupání.

Poplach a vypnutí poplachu: Je-li systém zapnut, způsobí narušení *detektorů zón 2 – 8 a 10* okamžitý poplach. Za povšimnutí stojí *podmínečně zpožděná zóna 2*, která se v tomto případě chová jako *okamžitá*. K poplachu může dojít i v případě příchodu obsluhy přístupovou cestou, pokud uživatel nestihne zadat kód do uplynutí příchodového času. Poplachový stav bývá zpravidla signalizován vnitřní a venkovní sirénou a současně může být tato informace přenášena na PCO. Dobu trvání poplachu lze nastavit, zpravidla bývá 1 minutu. I po jeho skončení zůstává systém samozřejmě zapnut. Vypnout ho lze jedině zadáním platného kódu. O skončení poplachu či jeho vypnutí je opět možno přenášet informaci na PCO. Po vypnutí si může uživatel prostřednictvím klávesnice prohlédnout informaci ve které zóně (popř. více zónách) došlo k aktivaci detektoru.
Praktická poznámka na závěr: Jeden osamocený poplach způsobený jedinou zónou mohl vzniknout v důsledku čehokoli (pohyb záclony, přeběhnutí velkého pavouka přes detektor apod.), více poplachů a ve více zónách už by nemělo zůstat bez povšimnutí. Tady už se může jednat o neoprávněné vniknutí do objektu.

Požární poplach: Bez ohledu na stav systému EZS způsobí narušení *zóny 9 (detektor kouře)* okamžitě poplach. Tato zóna je totiž nastavena jako *požární*, tzn. že stav detektoru je vyhodnocován 24 hodin denně. *Požární poplach* je narozdíl od klasického *signalizován přerušovaným tónem sirény*. V případě napojení objektu na PCO je i zde přenášená rozdílná informace oproti klasickému poplachu. K vypnutí dojde automaticky po uhašení požáru, do té doby je poplachový výstup stále aktivní. Pokud by tato skutečnost vadila, je možné *detektor 9* dočasně vyřadit pomocí funkce vyřazení zón – `BYPASS` (viz. dále).

Zapnutí systému – režim plášťová ochrana (STAY): Při zapínání je možné na klávesnici zadat, že se má systém zapnout v režimu tzv. *plášťové ochrany*. Narušení zón definovaných jako `STAY` (2, 6, 8) *bude ignorováno*, zbylé reagují dle nastavení. Tohoto lze využít například při střežení přes noc, přičemž osoby uvnitř objektu se mohou v zónách `STAY` volně pohybovat. Hlídaná je pracovna, přístup k automobilu *(zóna 10-infrazávora)* a pomocí detektorů reagujících na tříštění skla i obvodová okna.

Vypnutí systému – režim plášťová ochrana (STAY): Jelikož je systém z režimu plášťové ochrany většinou potřeba vypínat zevnitř objektu, musí být i *zóna 2* definovaná jako STAY. Díky tomu je možno ke klávesnici přijít nejen tzv. *přístupovou cestou*, ale třeba i chodbou z ložnice. K vypnutí systém dojde klasicky zadáním uživatelského kódu.

Zapnutí s vyřazením zón (BYPASS): Funkce `BYPASS` je užitečná v případě, že chce uživatel některou *zónu dočasně vyřadit z hlídání*. Tato potřeba může nastat při poruše detektoru nebo např. při probíhajících stavebních úpravách v části objektu. Pro požadovanou zónu musí být v ústředně EZS vyřazení povoleno a uživatel musí mít patřičná oprávnění. Funkce `BYPASS` je *platná vždy jen pro pro jedno zapnutí*. To probíhá klasicky jen s tím rozdílem, že před zapnutím jsou zadány čísla zón, jejichž stav má být při střežení ignorován.

Podsystémy a oprávnění uživatelů: Ústředna EZS umožňuje *rozdělit zóny v objektu do více podsystémů*. Ty lze ovládat zcela samostatně a jednotlivým uživatelům lze přidělit oprávnění pouze pro určitou část systému. Příkladem může být domek, kde je v přízemí prodejna a v patře bydlí majitel. První patro tvoří *podsystém 1* a prodejna *podsystém 2*. Majitel může ovládat oba podsystémy, zatímco prodavačka má oprávnění pouze pro ovládání podsystému prodejny.

3.2.4 Legislativa, stupeň zabezpečení

Návrh elektronického zabezpečovacího systému musí být proveden s ohledem na splnění mnoha podmínek. Jednou z nich je, že EZS musí mít svůj vlastní zdroj energie pro případ výpadku nebo úmyslného vypnutí elektřiny. Dále je třeba, aby sytém hlídal sám sebe. To znamená, že ve stavu střežení se nikdo nesmí dostat k žádné části EZS bez narušení detektoru.

Veškeré požadavky kladené na systém EZS a jeho prvky jsou obsaženy v České technické normě [1] (ČSN EN 50131-1/Z1). Jedním z nejdůležitějších kritérií je tzv. *stupeň zabezpečení*, který určuje: *oprávnění, přístupové úrovně, provozování, vyhodnocení, detekce, hlášení, napájení, zabezpečení proti sabotáži, monitorování propojení, záznam událostí.*

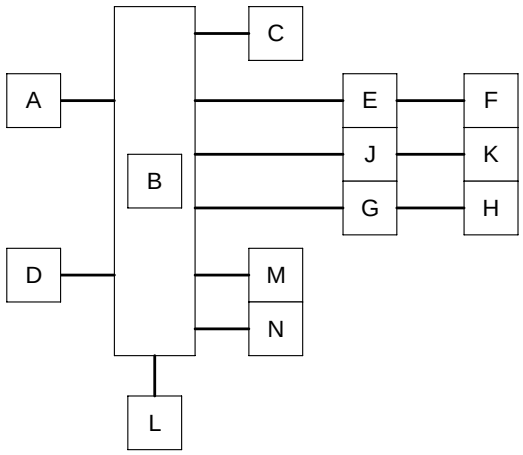
Stupeň	**Míra rizika**	**Typ narušitele**
1	Nízké	Předpokládá se, že narušitelé mají malou znalost EZS a že mají k dispozici omezený sortiment snadno dostupných nástrojů.
2	Nízké až střední	Předpokládá se, že narušitelé mají určité znalosti o EZS a že použijí základní sortiment nástrojů a přenosných přístrojů.
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.

Tabulka 3.1: Stupně zabezpečení dle normy [1] (ČSN EN 50131-1/Z1)

Podle míry rizika napadení se systém rozděluje na 4 stupně. Všechny prvky systému EZS musí být schváleny pro použití minimálně v kategorii, které má celý navrhovaný systém vyhovovat. Jejich posuzování a schvalování provádí nezávislá akreditovaná zkušebna. V praxi se při návrhu a realizaci EZS nejčastěji používají komponenty schválené pro kategorii 2 nebo 3.

3.3 Elektrická požární signalizace (EPS)

Úkolem elektrické požární signalizace (zkratka EPS) je upozornit na vznikající požár v objektu.



A Hlásiče požáru
B Ústředna EPS
C Požární poplachové zařízení
D Hlásiče tlačítkové
E Zařízení přenosu poplachu
F Ohlašovna požáru
G Řídící jednotka samočinného zařízení
H Samočinné zařízení požární ochrany
J Zařízení přenosu poruchových stavů
K Přijímací místo hlášení poruchových stavů
L Napájecí zařízení
M Obslužné pole požární ochrany
N Klíčový trezor požární ochrany

Obrázek 3.3: Blokové schéma systému EPS (převzato z [10])

Na obrázku 3.3 je znázorněna základní struktura systému EPS. Jeho základ tvoří ústředna, která neustále vyhodnocuje stav připojených požárních hlásičů. Ty lze rozdělit na 2 základní kategorie:

Automatické hlásiče: Reagují na jevy charakteristické pro požár, tj. kouř, nárůst teploty a plameny. Existuje velké množství typů lišících se principem detekce (ionizační, optické, tepelné, kombinované) a provedením.

Manuální tlačítkové hlásiče: Slouží k ručnímu vyhlášení požárního poplachu. Nejčastěji bývají instalovány na chodbách nebo jiných frekventovaných místech. Poznáme je podle toho, že mají vždy červenou barvu. Aby se zabránilo nechtěné aktivaci, bývá tlačítko umístěno za sklíčkem, které je potřeba nejdříve rozbít.

Popisu požárních hlásičů bude věnována kapitola 4.5, další informace lze získat v knize [3].

Při aktivaci některého z hlásičů (při požáru) zajistí ústředna EPS vyhlášení poplachu pomocí lokální akustické signalizace. Zároveň s tím jsou řídícímu centru automaticky přeneseny podrobné informace o místě vzniku požáru. Řídícím centrem může být stejně jako u systémů EZS pult centrální ochrany (PCO), nebo veřejný hasičský sbor. Ústředna EPS může v součinnosti s ostatními systémy provádět řadu dalších činností. Například zajistit otevření únikových východů, zapnout nouzová osvětlení, uzavřít požární dveře, aktivovat instalovaná hasící zařízení nebo zařízení sloužící k odsávání kouře, zastavit výrobní proces (v továrnách), apod.

Klíčový trezor požární ochrany (KTPO)

Zajímavým řešením je tzv. *klíčový trezor požární ochrany (KTPO)*. Jedná se o malý trezor zabudovaný do vnější zdi a obsahující veškeré klíče od objektu. Při požáru zajistí ústředna

EPS jeho otevření. Přesněji řečeno otevření jeho hlavních dvířek. Za nimi jsou ještě další, odemknutelná speciálním klíčem, tzv. hasičským univerzálem. Toto řešení je užitečné zejména v objektech, kde není zajištěná nepřetržitá přítomnost osob. V takovém případě pomáhá trezor s klíči hasičům usnadnit a hlavně urychlit vstup do objektu.

Problematika kolem systémů elektrické požární signalizace je velice rozsáhlá. Tato kapitola si kladla za cíl popsat jen základní možnosti těchto zařízení. Systémy EPS se v praxi používají spíše u rozsáhlejších objektů, nebo v místech se zvýšeným výskytem osob. Využití najdou především v hotelech, obchodních domech, restauracích, výrobních provozech apod. Pro většinu běžných prostor postačí možnost zařadit požární detektory do systému EZS.

3.4 Kamerový systém (CCTV)

Dříve se o kamerových systémech CCTV hovořilo spíše v souvislosti s průmyslovými aplikacemi, proto jsou někdy nazývány jako *průmyslové kamery* nebo *systémy průmyslové televize*. V současnosti nachází uplatnění snad ve všech oborech. Používají se ve zdravotnictví, v dopravě, ve výrobních procesech a v neposlední řadě pro bezpečnostní účely.

Zkratka CCTV je odvozena z anglického „Closed Circuit Television“ [17], což volně přeloženo do češtiny znamená „uzavřený televizní okruh“. Uzavřený proto, že narozdíl od veřejného televizního vysílání je video/audio distribuováno jen v určitém omezeném prostoru, například areálu firmy.

3.4.1 Kamery a záznamová zařízení

Základními prvky, jež zároveň významně ovlivňují kvalitu celého CCTV systému jsou kamery. Jejich úkolem je převést obrazovou informaci na videosignál[3], se kterým lze dále pracovat. Současné kamery k tomu používají součástku zvanou CCD.[4] Existuje spousta druhů a nejrůznějších provedení, takže pro konkrétní použití je třeba pečlivě vybírat vhodný typ.

Kamery lze dělit podle:

1. *Barevnosti*
   - **Černobílé** – někdy označované jako `b/w` (z anglického bleack/white).
   - **Barevné** – někdy označované jako `color`.
2. *Druhu přenosu video/audio signálu*
   - **Klasické** – přenos probíhá analogově přes koaxiální kabel.
   - **Bezdrátové** – přenosové médium tvoří vzduch, pracují v bezlicenčním pásmu (např. WiFi).
   - **IP kamery** – video/audio je přenášeno po ethernetu (počítačové síti). V kameře je zabudován webserver, který umožňuje konfiguraci a sledování odkudkoli z počítačové sítě nebo internetu pomocí běžného internetového prohlížeče. Přenášený obraz a zvuk je komprimován.

[3] Pro úplnost je třeba dodat že většina kamer snímá i zvukovou informaci a převádí ji na audiosignál.

[4] Z anglického „Charge-Coupled Device“, což v překladu znamená zařízení s vázanými náboji [21]. V dnešní době tvoří základ většiny kamer a digitálních fotoaparátů.

3. *Konstrukčního provedení*

   - **Vnitřní** – pro použití v místnostech a vnitřních prostorech.
     - **Deskové** – bez krytu, jen základní elektronika a mikrobjektiv, jsou určené pro zabudování do různých krytů či jiných zařízení.
     - **Kompaktní** – s odnímatelným objektivem, zabudované v krytu a s držadlem pro připevnění na zeď. Většinou jsou dodávány bez objektivu, ten se volí až podle požadovaných parametrů.
     - **Maskované** – používají se pro skryté monitorování. Vzhledově vypadají jako jiná zařízení, nejčastěji se používají zabudovaná do funkčních detektorů pro systémy EZS.
   - **Venkovní** – zabudované do masivního krytu pro použití i při zhoršených klimatických podmínkách (déšť, mlha, sníh). Někdy bývají vytápěné.

4. *Doby a místa používání*

   - **Denní** – určeny ke snímání za dobrých světelných podmínek.
   - **Kombinované, s IR LED přisvětlením** – ve dne pracují v klasickém barevném režimu. Při zhoršení světelných podmínek přisvětlují monitorovaný prostor pomocí infračervených LED umístěných okolo objektivu. V tomto režimu produkují černobílý obraz. Nejlepší kamery dokáží snímat v úplné tmě na vzdálenost až 100 m!
   - **Speciální** – pro nejnáročnější podmínky. Patří sem např. termální kamery, které jsou schopny snímat v úplné tmě, mlze nebo dešti na vzdálenost až několika kilometrů.

Kromě sledování reálného dění v monitorvaných prostorech umožňují kamerové systémy CCTV i záznam pořizovaného video/audio signálu. Dříve se pro tento účel používaly analogové „time-lapse“ (český ekvivalent je *pomaloběžné*) videorekordéry, které umožňovaly nahrát na běžnou VHS kazetu až 24 hodin záznamu. Dnes jsou nahrazovány *digitálními videorekordéry (DVR)* [18] ukládajícími záznam na pevný disk (HDD). Díky použití ztrátové komprese MPEG [19] a neustále se zvyšující kapacitě pevných disků (HDD) umožňují až několikaměsíční zpětnou archivaci. Další výhodou rekordérů DVR je, že mnohdy obsahují tzv. *videoserver*, což umožňuje vzdálený přístup přes počítačovou síť LAN nebo Internet.

Jako digitální záznamové zařízení může sloužit i běžný počítač osazený přídavnými kartami pro zpracování video/audio signálu a s nainstalovaným speciálním softwarem. Toto řešení je levnější a univerzálnější než použití DVR rekordéru, avšak za cenu nižší spolehlivosti.

3.4.2 Dálkové ovládání kamer

V praxi se výstupy ze všech instalovaných kamer většinou soustřeďují do jednoho místa, tzv. *dohledového centra*. Často je umístěno na vrátnicích, nebo jiných místnostech, kde je v požadované míře zaručena přítomnost případné obsluhy. Ta má možnost na televizoru (nebo počítačovém monitoru) sledovat reálné dění v monitorovaných prostorech a v případě potřeby procházet již pořízené záznamy.

Výbavou dohledového centra bývá často i ovládací klávesnice s joystickem pro ovládání tzv. *PTZ kamer*. To jsou speciální pohyblivé kamery, nebo kamery umístěné na pohyblivých

hlavicích. Komunikace mezi monitorovacím pracovištěm a kamerami PTZ probíhá přes *sériové rozhraní RS-485*, jenž je vylepšenou variantou *sériového portu RS-232*. Na jedno vedení tak lze připojit více samostatných PTZ zařízení a jeho celková délka může dosahovat až 1600 m [5]. Zkratka PTZ pochází z anglického „Pan Tilt Zoom“, což zároveň vyjadřuje možnosti jenž PTZ nabízí. Tedy:

- Pohyb kamery v horizontální rovině (Pan)
- Pohyb kamery ve vertikální rovině (Tilt)
- Změna ohniskové vzdálenosti (Zoom)

Obrázek 3.4: Monitorovací pracoviště MKS Svitavy

Pomocí klávesnice s joystickem je možné přepínat mezi ovládanými kamerami, řídit jejich pohyb a přibližovat na požadovaný detail. Systém CCTV v kombinaci s PTZ kamerami je tak neocenitelným pomocníkem nejen ve službách policie při zajišťování bezpečnosti a pořádku ve městech. Na obr. 3.4 je fotografie monitorovacího pracoviště městského kamerového systému (MKS) ve Svitavách. Z obrázku je dobře patrný způsob ovládání kamer PTZ pomocí joysticku.

3.5 Doplňkové systémy

V součinnosti s již popisovanými způsoby zabezpečení objektů a okolních prostor lze použít ještě některé další systémy.

Ozvučovací systémy a systémy místního rozhlasu: Bývají instalovány do objektů a okolních prostor za účelem okamžitě sdělit potřebné informace všem přítomným osobám. Používají se převážně v součinnosti se systémy EZS, EPS a CCTV pro sdělování důležitých informací. Za příklad lze použít třeba *evakuační pokyny při požáru*, které mohou být buďto předem nahrané (Aktivaci zařízení pro přehrávání zajistí ústředna EPS.), nebo sdělované určenou osobou pomocí mikrofonu.

Přístupové systémy: Na základě přístupových práv řídí přístup osob do chráněných prostor [7]. Ty mohou být zabezpečeny pomocí turniketů, závor nebo elektrických zámků. Pro každý prostor jsou definována potřebná oprávnění. Ověřování probíhá nejčastěji zadáním kódu (nebo pomocí tzv. *čipové karty*) u vstupních dveří (závor, turniketů) do chráněné části objektu. Vstup je poté umožněn jen osobám s příslušným oprávněním.

Kapitola 4

Detektory

Systémy pro zabezpečení a střežení (EZS, EPS) potřebují pro svoji činnost nějakým způsobem vyhodnocovat určité fyzikální jevy jako je např. pohyb osoby, zvuk způsobený rozbitím skla, nebo kouř vznikající při požáru. K tomuto účelu se používají tzv. *detektory*.

Existuje nepřeberné množství druhů a typů lišících se jak principem detekce, tak provedením. Tato kapitola má za cíl celou problematiku trochu objasnit. Obsahuje dělení detektorů dle různých hledisek a popis principů detekce používaných u jednotlivých typů.

4.1 Co jsou detektory, základní dělení

Bezpečnostní *detektory*, nebo-li *čidla* jsou zařízení, určená pro převod fyzikálních jevů (souvisejících s narušením bezpečnosti) na elektrický signál. Existuje velké množství detektorů pracujících na různých fyzikálních principech a detekujících různé typy narušení. O vyhodnocování se stará ústředna, k níž jsou čidla připojena [2].

Detektory lze z hlediska způsobů přenosu signálu o poplachu do ústředen EZS rozdělit na:

- **Detektory pro smyčkové ústředny** - Uvnitř každého čidla je zařazen rezistor. Při aktivaci detektoru dojde k rozpojení poplachového relé a tím ke změně hodnoty odporu. Ústředna tuto situaci vyhodnotí jako poplachový stav.
- **Sběrnicové detektory** - Jsou určeny pro *ústředny s přímou adresací detektorů*. Mezi detektorem a ústřednou probíhá po čtyřvodičové sběrnici obousměrná datová komunikace. Aby mohla ústředna rozpoznat, které čidlo aktivovalo poplachový stav, musí být detektory adresovatelné. Tzn. každý komunikuje pod jedinečným identifikátorem. Tyto adresy přiřazuje detektorům sběrnicová ústředna EZS [8].
- **Bezdrátové detektory** - Používají se ve spojení s *ústřednami s bezdrátovým přenosem od čidel*. Komunikace mezi detektorem a ústřednou probíhá bezdrátově na frekvenci 433 MHz. Pokud není vysílací/přijímací jednotka součástí ústředny, probíhá komunikace mezi ní a ústřednou po sběrnici.

Podle aktivity se detektory dělí na:

- **Aktivní** - Vysílají určitou energii (např. světelný paprsek) a sledují odezvu okolí.
- **Pasivní** - Vyhodnocují změny energie přijímané z okolí (např. teplo lidského těla).

Podle plánovaného umístění v objektu rozeznáváme:

- **Prvky plášťové ochrany** - Používají se pro ochranu *pláště budovy*, většinou tedy oken a dveří. Patří sem magnetické detektory, čidla rozeznávající tříštění skla a detektory otřesu.
- **Prvky prostorové ochrany** - Jsou určeny pro instalaci do vnitřních prostor. Nejpoužívanější jsou pasivní infračervená (PIR), ultrazvuková, mikrovlná nebo kombinovaná čidla.
- **Prvky perimetrické (obvodové) ochrany** - Slouží pro ochranu pozemku před vstupem cizích osob. Hlavními zástupci jsou venkovní infrazávory, infrabariéry, mikrovlnné bariéry a tlakové hadice.
- **Prvky předmětové ochrany** - Mají za cíl střežit konkrétní předmět. Používají se např. pro hlídání trezorů nebo uměleckých předmětů v muzeích a galeriích. Své uplatnění zde najdou otřesová a kapacitní čidla, nebo detektory na ochranu zavěšených předmětů.

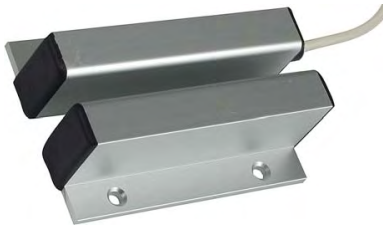
4.2 Prvky plášťové ochrany

Do této kategorie patří veškeré detektory zajišťující hlídání plášťových (obvodových) prvků objektu. To jsou okna, dveře nebo vrata.

Magnetický kontakt

Nejjednodušším prvkem plášťové ochrany objektu je *magnetický kontakt*. Používá se k hlídání otevření dveří nebo oken. Skládá se ze 2 oddělených částí, kde jedna obsahuje permanentní magnet a druhá jazýčkové relé napojené na výstupní svorky. Magnet se většinou připevní na pohyblivou část dveří (nebo okna) a zbytek je umístěn na rámu. V klidovém stavu (uzavřené dveře, okno) je jazýčkové relé sepnuto. V případě oddálení magnetu dojde k jeho rozepnutí a vyhlášení poplachu.

Magnetické kontakty se vyrábí v mnoha provedeních vzájemně se lišících barvou a tvarem. Základní princip funkce zůstává stále stejný. Krom provedení pro povrchovou montáž se lze setkat i s kontakty zapuštěnými přímo do futra nebo okenního rámu.



Obrázek 4.1: Magnetický kontakt

Detektory tříštění skla

Za pomocí mikrofonu je snímána slyšitelná část zvuku v okolí detektoru. K jeho narušení dojde při současném výskytu tlakové vlny a akustického projevu s charakteristikou odpovídající tříštění skla. Mezi skleněnou plochou a detektorem by měl být volný prostor, jinak nebude zaručena jeho správná funkce.
Při výběru konkrétního typu by měl být brán ohled na parametr vyjadřující minimální plochu skla, při které je ještě zaručena detekce. Dalším kritériem by mělo být to, zda je schopný detekovat i rozbití skla potaženého bezpečnostní fólií.

Obrázek 4.2: Detektor tříštění skla PARADOX GLASSTREK 456

Otřesové detektory

Otřesové detektory slouží ke střežení všech ploch, k jejichž překonání je třeba hrubá síla. Jsou založeny na principu tzv. *piezo-elektrického jevu*. Obsahují tedy krystal, jenž při chvění generuje elektrické napětí. To je dále vyhodnocováno elektronikou čidla a v případě dosažení určité hodnoty je detekováno narušení.

Otřesové detektory reagují např. na rány kladivem nebo zbíječkou do zdi a na vibrace vznikající při řezání pilou nebo plamenem. Pro dosažení optimální citlivosti je třeba čidla co nejlépe připevnit k povrchu, jehož chvění bude snímáno. Otřesové detektory jsou schopny detekovat poměrně široké rozmezí otřesů, proto je nezbytné je po instalaci zkalibrovat pro použití v konkrétním prostředí [22].

Obrázek 4.3: Otřesový detektor OPTEX VIBRO

4.3 Prvky prostorové ochrany

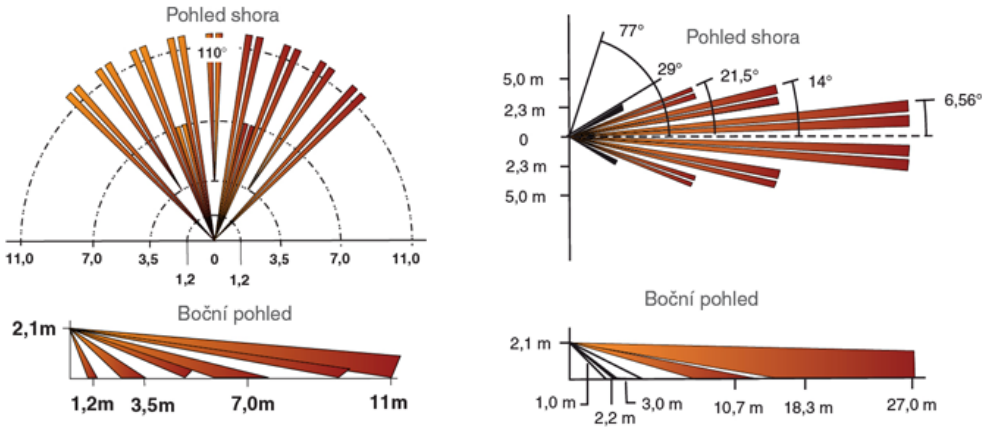
Prostorová ochrana slouží ke střežení vnitřních (někdy i venkovních) prostor objektů. Tvoří ji čidla určená k detekci pohybu, vzájemně se lišící principem funkce a provedením. Existují varianty pro montáž na zeď nebo na strop. Setkat se lze i s detektory odolnými proti narušení malými zvířaty jako je pes a kočka.

Doplňkovou funkcí je tzv. *antimasking* nebo-li **ochrana proti zastínění**. Ta je aktivní i v klidovém stavu systému a má za úkol upozornit v případě zastínění čidla nějakým předmětem, nebo např. při jeho přestříkání barvou. Potenciálním pachatelům se tak zabrání možnosti připravit si objekt pro vloupání během doby, kdy je systém vypnut. V případě, že dojde z zastínění některého z čidel vybavených funkcí *antimasking*, zamezí ústředna EZS obsluze zapnout systém do stavu střežení.

Pasivní infračervené detektory (PIR)

Pasivní infračervené detektory (PIR – z anglického „passive infrared sensor“) pracují na principu vyhodnocování změn infračerveného spektra elektromagnetického vlnění [8]. Každé těleso má určitou teplotu a je tedy zdrojem vlnění s odpovídající vlnovou délkou. Ta je pro teplotu lidského těla 9,4 mm.

Jádro detektoru tvoří senzor snímající infračervené (IR) záření a *Fresnelova čočka*[1] dělící snímaný prostor na aktivní a neaktivní zóny. Pohybující se těleso s odlišnou teplotou od okolí (člověk) vyvolá v senzoru při přechodu z aktivní do neaktivní zóny (a naopak) změny signálu. Ty jsou elektronikou čidla vyhodnoceny a v případě dosažení určitých hodnot je aktivován poplach. Velikost zorného úhlu a dosah detektoru jsou závislé na provedení *Fresnelovy čočky*. Tu je třeba volit podle požadovaných parametrů. Jak moc ovlivňuje rozložení zón je patrné z detekčních charakteristik na obrázku 4.4. Levá polovina odpovídá čočce detektoru pro kratší dosah a větší zorný úhel, pravá potom pro detektor s větším dosahem.



Obrázek 4.4: Detekční charakteristiky PIR detektoru

[1] Pojmenovaná podle jejího vynálezce *Augustina-Jeana Fresnela*. Oproti běžné čočce má odstraněny části nepodílející se přímo na lomu paprsků. Díky tomu má menší tloušťku a hmotnost [20].

Obrázek 4.5: PIR detektory (na zeď, na strop, odolný proti zvířatům)

Aktivní ultrazvukové detektory (US)

Ultrazvukové detektory US (z anglického „Ultrasonic sensor“) využívají ke své činnosti *Dopplerova jevu*. Je-li f_0 frekvence vysílaná vysílačem, potom pro frekvenci f přijatou přijímačem platí:

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

kde v je rychlost pohybu tělesa odrážejícího vlnění (např. pohybující se pachatel) a c je rychlost pohybu vlnění vysílaného detektorem.

Ultrazvukový detektor obsahuje vysílač a přijímač ultrazvukových vln (zpravidla kolem 40 kHz). Vysílané vlnění o konstantní frekvenci se odráží od překážek a po přijetí přijímačem se sleduje změna jeho fáze. K té dojde při pohybu libovolného tělesa v monitorovaném prostoru. V takovém případě se elektronika čidla postará o vyhlášení poplachu. Narozdíl od PIR čidel detekují nejlépe pohyb směrem k detektoru a od něj.

Aktivní mikrovlnné detektory (MW)

Mikrovlnné detektory MW (z anglického „Microwave senzor“) pracují na obdobném principu jako ultrazvuková čidla. Opět je využito *Dopplerova jevu*. Rozdíl je pouze ve vysílaných kmitočtech (2,5 GHz, 10 GHz, nebo 24 GHz) a tomu je uzpůsobena i elektronika čidel. Stejně jako ultrazvuková čidla detekují nejlépe pohyb směrem k detektoru a od něj. Negativně na ně působí hladké kovové plochy a problémy mohou způsobovat i vlny ze sousedního detektoru pronikající přes sklo nebo tenké stěny. Proto se v praxi používají jen na místech kde nelze použít PIR čidla.

Duální (kombinované) detektory

V obvzvláště problematických prostorách se používají kombinovaná čidla obsahující nejčastěji PIR a MW detektor. Poplach je vyhlášen jen při současném narušení obou částí čidla, z nichž každá je založena na jiném principu detekce. Díky tomu se značně minimalizuje riziko falešných poplachů.

4.4 Prvky perimetrické ochrany

Pro ochranu vnějších částí objektů před neoprávněným vstupem osob se používají *prvky perimetrické (obvodové) ochrany*. Existuje mnoho typů detektorů založených na různých fyzikálních principech. Nejznámější jsou infračervené, případně mikrovlnné závory a bariéry. Pro rozsáhlejší plochy najdou uplatnění tlakové hadice zakopané v zemi.

Infračervené závory a bariéry

Infrazávory jsou nejpoužívanějším druhem čidel používaným pro obvodovou ochranu objektu nebo určitého území (pozemku). Sestávají ze 2 samostatných částí. Vysílací strana vysílá infračervený paprsek (IR), který je nepřetržitě přijímán přijímací stranou. Ta při detekování přerušení paprsku (např. procházející osobou) zajistí vyhlášení poplachového stavu. Běžně používané infrazávory pracují se dvěma až čtyřmi paprsky a mají dosah okolo 100 metrů. Pro menší náchylnost k chybám jsou paprsky mnohdy vysílány pulsně a pro omezení působení vnějších vlivů mají některé infrazávory vlastní vyhřívání.

4.5 Detektory požární a plynů

Požární detektory jsou určeny pro použití v systémech elektrické požární signalizace (EPS) a doplňkově též v elektronických zabezpečovacích systémech (EZS).

Požární detektory

Úkolem požárních detektorů je detekovat požár pokud možno v jeho začínající fázi. Poplachový stav je předán ústředně a některé detektory jej navíc signalizují zabudovanou sirénou. Existuje více typů pracujících na různých principech:

Obrázek 4.6: Požární detektor

Tepelné (termodiferenciální): Reagují na prudký nárůst teploty nebo dosažení její určité hodnoty. Jsou náchylné na prach a nečistoty, na požár reagují s poměrně velkým zpožděním.

Opticko-kouřové: Někdy nazývané *bodové optické hlásiče kouře*. V detektoru je komůrka se zabudovanou pulsně svítící IR diodou a vyhodnocovací fotodiodou. Při začínajícím požáru vnikne do komůrky kouř a způsobí na fotodiodě světelnou ztrátu. Ta je elektronikou čidla vyhodnocena jako poplachový stav. Nevýhodou těchto detektorů je náchylnost na zanesení prachem, proto je potřeba je v pravidelných intervalech čistit. Výhodou je, že reagují na kouř a díky tomu detekují požár v jeho samotném počátku.

Kombinované (multisenzorové): K detekci požáru využívají kombinovaný detektor obsahující tepelný, opticko-kouřový a chemický senzor. Pro vyhlášení poplachu dostačuje aktivace jednoho z nich. Jako chemický se nejčastěji používá detektor oxidu uhelnatého (CO), který vzniká při nedokonalém hoření na začátku požáru.

Detektory plynů

Používají se jako doplňkové detektory k systémům EPS a EZS. Pracují většinou na principu převodu koncentrace konkrétního plynu na proudový signál, který je elektronikou čidla dále vyhodnocován. Běžně uplatňované jsou detektory oxidu uhelnatého (CO), zemního plynu a propan butanu.

4.6 Tísňové hlásiče

Tísňové hlásiče umožňují ručně vyvolat poplach a slouží k ochraně osob při přímém ohrožení. Mohou být instalovány skrytě, nebo na viditelném místě.

Panik tlačítko

Tlačítko *PANIK* (někdy nazývané *EMERGENCY*) slouží k nepozorovanému vyvolání poplachu v případě přímého ohrožení osoby. Používá se například na pokladnách obchodů. Bývá instalováno tak, aby jej bylo možné ohroženou osobou nenápadně aktivovat. O tísňové situaci lze prostřednictvím EZS ústředny komunikující s PCO informovat bezpečnostní agenturu nebo Policii.

Požární tísňový hlásič

Požární tlačítkové hlásiče slouží k ručnímu vyhlášení požárního poplachu. Používají se v systémech EPS i EZS pro případ, že si někdo všimne začínajícího požáru dříve než je detekován detektory, nebo v objektech bez instalovaných požárních čidel.

Obrázek 4.7: Požární tísňové tlačítko

Nejčastěji bývají instalovány na chodbách a jiných veřejně dostupných místech. Z důvodu ochrany před nechtěným vyhlášením požárního poplachu je tlačítko umístěno za sklíčkem, které je třeba nejdříve rozbít.

Kapitola 5

Specifikace požadavků na systém

Cílem této práce je návrh *systému pro zabezpečení a střežení bytové jednotky včetně jejích okolních prostor*. Návrh by měl být proveden s ohledem na nízký příkon, snadnost instalace a případných změn struktury systému a jeho komponent. Požadována je i možnost archivace a zasílání uživatelem upřesněných dat.

5.1 Specifikace systému pro zabezpečení a střežení

Aby bylo možné přistoupit k samotnému návrhu, je třeba nejdříve provést specifikaci. Jinak řečeno, je třeba sepsat požadavky zákazníka na tento systém. Pro další postup bude uvažován fiktivní rozhovor se zákazníkem (říkejme mu pan Novák) a prohlídka jeho malého rodinného domku.

Již při prvním pohledu na velikost objektu bylo jasné, že počet střežených zón nepřesáhne číslo 10 a rozdělení na více podsystémů nebude mít smysl. Z rozhovoru potom vyplynulo, že objekt užívá 4-členná rodina, majitel se ženou a dvěma dětmi středního věku. Jelikož chce mít pan Novák neustálou kontrolu nad stavem objektu, požaduje možnost být pomocí sms na jeho mobilní telefon informován o událostech jako je zanutí/vypnutí, porucha systému a případný poplach. Připojení objektu na PCO není plánováno. Jelikož v domku žijí i děti, které mohou při odchodu zapomenout provést aktivaci systému, potřeboval by pan Novák toto učinit kdykoli na dálku prostřednictvím mobilního telefonu. Velice se mu zamlouvá i případné ovládání přes Internet. To by mu mělo zároveň umožnit sledovat aktuální stav systému a procházet historii událostí.

Paní Nováková pěstuje ve skleníku na zahradě květiny náročné na světlo. Už ji ale nebaví chodit každý večer zapínat umělé osvětlení, proto by chtěla tuto činnost nějak zautomatizovat. Použité zařízení musí umožňovat nadefinovat si pro každý den čas aktivace a deaktivace osvětlení. Jeho ovládací rozhraní musí být přístupné přes internetový prohlížeč z počítače v domácí síti LAN nebo odkudkoli z Internetu.

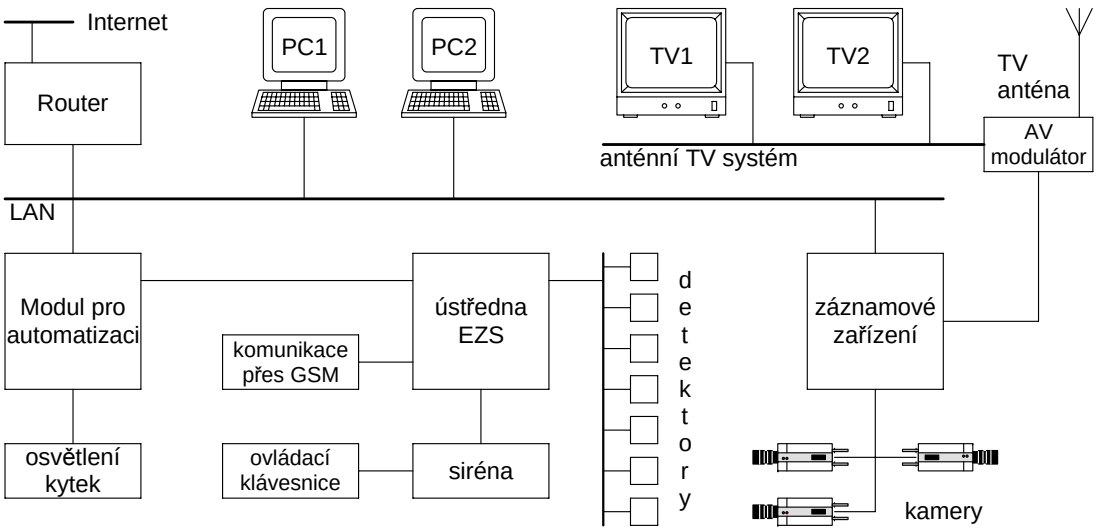
Posledním požadavkem Novákových byla instalace venkovních bezpečnostních kamer. Plánované jsou pro začátek 2, časem uvažují přidat další, ale větší počet než 3 by prý neměl smysl. Kamery by měly být barevné a poskytovat relativně čistý a ostrý obraz i při úplné tmě. Ze všech kamer bude kvůli pojišťovně automaticky prováděn záznam. Měl by být zpětně dostupný alespoň po dobu 30 dnů. Sledovat aktuální dění chtějí na kterémkoli televizním přijímači ve svém domku přepnutím na příslušný kanál. Panu Novákovi by se navíc velice hodila možnost přístupu k aktuálním i zaznamenaným obrazovým datům z počítačů v domácí síti LAN, nebo odkudkoli pomocí Internetu.

Zákazník ve fiktivním rozhovoru jasně definoval, jaké nároky na systém klade. Pro přehlednost a snažší orientaci je vhodné výsledné požadavky na systém shrnout do několika bodů.

- **Požadavky na systém EZS**
  - 4 stálí uživatelé, netřeba dělit na podsystémy, méně než 10 střežených zón.
  - Ovládání systému a přenos informací o událostech (zapnuto/vypnuto, poplach, porucha) pomocí sítě GSM.
  - Ovládání a sledování stavu systému pomocí domácí sítě LAN a přes Internet.
  - Historie základních událostí s možností nahlížet přes LAN a Internet.
- **Požadavky na automatizaci v objektu**
  - Automatické ovládání umělého osvětlení květin podle plánovacího kalendáře. Možnost změny časů a ručního ovládání přes domácí síť LAN a přes Internet.
- **Požadavky na kamerový systém**
  - Kvalitní venkovní barevné kamery s možností snímat i po tmě.
  - Záznam videa ze 3 kamer. Musí být zpětně dostupný alespoň 30 dnů.
  - Sledování aktuálního dění přes anténní systém na běžném televizoru.
  - Přístup k aktuálním i zaznamenaným obrazovým datům přes LAN a Internet.

5.2 Blokové schéma systému

Na základě výše stanovených požadavků lze vytvořit blokové schéma systému pro zabezpečení a střežení objektu a okolních prostor. Výsledkem je obr. 5.1. Spojnice mezi jednotlivými bloky naznačují pouze tok informací, nikoli fyzické propojení dílčích komponent.



Obrázek 5.1: Blokové schéma navrhovaného systému pro zabezpečení a střežení

Kapitola 6

Návrh systému

Tato kapitola se zabývá návrhem systému a volbou jeho dílčích komponent. Vše je vybíráno s ohledem na požadavky plynoucí ze zadání a ze specifikace provedené v kapitole 5.

6.1 Analýza požadavků na EZS, výběr vhodných komponent

Podstatnou část požadavků na zabezpečení objektu by měl uspokojit vhodně zvolený elektronický zabezpečovací systém (EZS). Základní principy a funkce EZS jsou popsány v kapitole 3.2.

6.1.1 Ústředna EZS

Hlavním prvkem EZS, jež zároveň zásadně ovlivní parametry celého systému, je ústředna EZS. Proto velice záleží na výběru vhodného typu.

Ze specifikovaných požadavků jsou pro výběr ústředny rozhodující tyto:

Nízký příkon: Díky vysoké úrovni technologií výroby elektroniky a elektronických součástek se daří neustále snižovat příkon zařízení. Klidový proudový odběr současných ústředen se pohybuje okolo 100 mA. Při požadavku na co nejnižší příkon je třeba volit takovou ústřednu EZS, aby pro daný objekt nebyla zbytečně předimenzovaná. Rovněž je třeba vhodně zvolit všechny ostatní použité komponenty.

Snadnost instalace a změn struktury systému: V praxi provádí montáž EZS ve většině případů specializovaná firma, proto kritérium snadné instalace nebývá při návrhu nikterak rozhodující. V případě, že se počítá s budoucími změnami struktury systému EZS (např. přidávání, přemisťování, nebo změna typu detektorů), jeví se jako vhodné použití tzv. *bezdrátové nadstavby*. Komunikace mezi ústřednou EZS a jednotlivými prvky (detektory, klávesnice) potom probíhá bezdrátově na frekvenci 433 MHz. Změna struktury systému je potom možná jednoduchým přemístěním požadovaných komponent. Bezdrátové řešení se používá rovněž v případě, že není možné nebo vhodné natahovat kabely, tedy např. v objektech vyhlášených za chráněnou památku.

4 stálí uživatelé: Ústředna EZS umožňuje definovat běžně kolem osmi a více tzv. *uživatelských kódů*. Pro objekt užívaný čtyřmi osobami bude tedy v tomto ohledu dostačující většina typů ústředen.

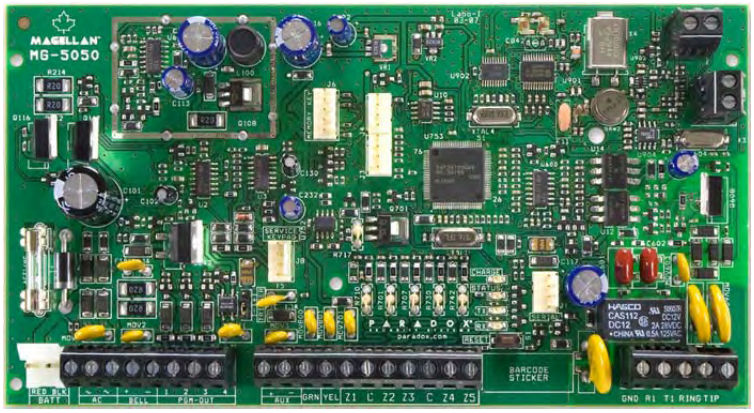
Netřeba dělit na podsystémy: Možností rozdělit systém EZS na několik podsystémů (minimálně 2) disponuje drtivá většina ústředen. V malých objektech je použití podsystémů mnohdy zbytečné, avšak je ho možné kdykoli dodatečně realizovat. Stačí k tomu obyčejný zásah do nastavení ústředny EZS.

Méně než 10 střežených zón: Dalším kritériem pro výběr ústředny je *počet zón* definující množství připojitelných detektorů. Většina ústředen umožňuje připojení 8, 16 nebo 32 a v případě potřeby lze toto číslo zvětšit pomocí rozšiřujícího prvku zvaného *expandér zón*.

Další požadavky jsou již spíše na periferie než samotnou ústřednu EZS. Výběr a popis těchto komponent bude proveden v dalších kapitolách (konkrétně v kap. 6.2 a 6.3). Při volbě vhodné ústředny je v našem případě třeba počítat s připojením modulů zajišťujících následující činnosti:

- archivaci a zasílání uživatelem upřesněných dat
- ovládání systému a přenos informací o událostech pomocí sítě GSM
- ovládání a sledování stavu systému pomocí LAN a přes Internet
- historii událostí s možností nahlížet přes LAN a Internet

Na základě výše uvedených kritérií byla za nejvhodnější zvolena ústředna `Magellan MG-5050` kanadského výrobce `PARADOX`®.



Obrázek 6.1: Ústředna PARADOX Magellan MG-5050

Jedná se o ústřednu hybridního typu s integrovaným vysílačem/přijímačem komunikujícím na frekvenci 433 MHz s možností připojení bezdrátových detektorů, klávesnic a PGM modulů. Maximální počet zón v systému může být 32. Přímo na desku je možné „drátově“ připojit až 10 zón, další potom buďto bezdrátově nebo pomocí *expandéru zón*. Ústředna umožňuje rozdělení systému na 2 podsystémy a definovat až 32 bezpečnostních kódů. Součástí jsou i 4 programovatelné výstupy PGM a telefonní komunikátor pro komunikaci s PCO.

Detailní popis, specifikaci, instalační manuály a software pro nastavení ústředny lze nalézt na webu [12].

6.1.2 Detektory

Při volbě vhodných detektorů je třeba brát v úvahu požadavky na nízký příkon, snadnost instalace a snadnost případných změn nebo rozšíření systému. Těmto kritériím nejvíce vyhovují bezdrátové detektory pracující na frekvenci 433 nebo 868 MHz. K napájení se používají klasické tužkové baterie, které vydrží až několik roků. Díky bezdrátovému přenosu informací mezi detektory a ústřednou a díky samostatnému napájení pomocí baterií je lze umístit na kterékoli místo bez nutnosti tahat jakékoli dráty. V případě potřeby potom není problém požadované čidlo velice rychle demontovat a přesunout jinam.

Existuje velké množství druhů použitelných v nejrůznějších podmínkách. Většina z nich byla podrobně popsána v kapitole 4. Při praktické realizaci je třeba vždy vybírat s ohledem na klady a zápory daného typu čidla a poměry v prostorách, v nichž bude instalováno. Pro návrh našeho systému budou použity náhodně zvolené detektory (vyhovující požadavkům zadání a specifikaci), protože poslouží jen pro demonstraci jejich činnosti.

Z důvodu kompatibility se zvolenou ústřednou EZS budou pro navrhovaný systém použity detektory značky PARADOX®:

Bezdrátový PIR detektor MG-PMD1P: Je odolný proti zvířatům do 18 kg. Napájení zajišťují 3 alkalické AA baterie s životností až 4 roky. Pracuje na frekvenci 433 MHz s dosahem okolo 70 m.

Bezdrátový magnetický kontakt MG-DCT2: Je určený pro povrchovou montáž. Pracuje na frekvenci 433 MHz s dosahem okolo 40 m. Napájení zajišťuje knoflíková baterie s životností až 2 roky.

Bezdrátový požární detektor MG-SD738: Jedná se o opticko-kouřový detektor se zabudovanou sirénou. Pro napájení slouží jedna 9 V baterie, která umožní až rok provozu. Dosah bezdrátového vysílače je okolo 70 m.

Detektor rozbití skla Glasstrek 457: Je určen pro střežení skleněných ploch větších než 40 x 60 cm v prostorách větších než 3 x 3 m. Umožňuje připojení ke smyčkovým i sběrnicovým typům ústředen.

Venkovní infrazávora VAR-TEC TRIPLE PB-150: Jedná se o 3 paprskovou infrazávoru pro vnitřní i venkovní montáž připojitelnou ke smyčkovým ústřednám. Maximální vzdálenost mezi přijímačem a vysílačem IR paprsků je 150 m při venkovním použití a 300 m uvnitř objektů.

Obrázek 6.2: Použité detektory (v pořadí dle popisu)

6.1.3 Ostatní prvky

K dokončení návrhu systému EZS je třeba ještě vybrat vhodnou ovládací klávesnici, poplachovou sirénu, napájecí zdroj a záložní baterii. Aby byly dodrženy požadavky na nízký příkon a snadnost instalace či případných změn, byla zvolena bezdrátová klávesnice a moderní nízkoodběrová siréna.

Bezdrátová klávesnice Magellan MG32LRF: Jedná se o LED klávesnici komunikující s ústřednou EZS bezdrátově s dosahem 40 m. Napájení je zajištěno adaptérem 6 V / 200 mA a pro případ výpadku elektřiny je použita integrovaná nabíjecí baterie.

Venkovní zálohovaná siréna TEKNIM-720WR: Pro akustickou signalizaci je použit piezoměnič a pro optickou stroboskop. Díky tomuto řešení bylo dosaženo snížení příkonu sirény a je možno ji napájet z malé dobíjecí baterie. Ta zároveň slouží pro zálohování v případě výpadku elektřiny.

Napájecí zdroj: Použitou ústřednu Magellan MG-5050 je třeba napájet střídavým napětím 16 V. K tomuto účelu poslouží transformátor na 230 V, 50 Hz s výstupním napětím 16 V a maximální zátěží 2 A.

Zálohovací akumulátor: Z důvodu zajištění funkčnosti systému EZS i při výpadku elektřiny je potřeba použít záložní napájecí zdroj. K tomuto účelu slouží dobíjecí akumulátory. V našem případě bude použit bezúdržbový olověný akumulátor o jmenovitém napětí 12 V a kapacitě 7 Ah.

Obrázek 6.3: Použité prvky (klávesnice, siréna, napájecí zdroj, akumulátor)

6.2 Ovládání a přenos událostí pomocí GSM

Ve specifikaci bylo požadováno *ovládání systému a přenos informací o událostech pomocí sítě GSM*. Toto lze vyřešit použitím *GSM pageru* nebo *GSM brány*. Obojí umožní ovládání zasláním sms zpráv v určitém tvaru nebo prozvoněním z konkrétního telefonního čísla. GSM brána navíc přidává možnost přenosu hlasových zpráv. Jelikož pro systém EZS simuluje pevnou telefonní linku, lze pomocí ní realizovat i připojení na PCO.

Navrhovaný systém sice dle specifikace nebude připojen na PCO, ani není třeba přenášet hlasové zprávy, ale pro případné budoucí změny je vhodné použít GSM bránu. Cenový rozdíl oproti GSM pageru není nikterak zásadní a díky tomuto řešení může být případná realizace hlasového přenosu nebo připojení na PCO poměrně snadná a rychle proveditelná.

Pro ovládání systému a přenos informací o událostech pomocí sítě GSM bude tedy použita `GSM brána GSM-VT-10`.

Obsahuje zabudovaný GSM modul, který po vložení SIM karty zajišťuje veškerou komunikaci v síti GSM. Pro ústřednu EZS simuluje pevnou telefonní linku a je tak možno realizovat datový přenos na PCO v hlasovém pásmu GSM. V základním provedení obsahuje 2 vstupy a 2 reléové výstupy, v případě potřeby je možno přidat další pomocí rozšiřujících modulů (tzv. *expandérů*). Při aktivaci některého ze vstupů umožňuje zaslání sms nebo přenos hlasové zprávy (potřeba expandér `VT-04 VOICE`) až na 4 telefonní čísla. Výstupní relé mohou být ovládány buďto zasláním sms ve speciálním tvaru z jakéhokoli telefonu na číslo GSM brány, nebo prozvoněním z jednoho definovaného čísla. Veškeré programování se provádí přes sériového rozhraní pomocí počítače. Kompletní specifikaci, popis způsobu použití a návod na programování GSM brány lze nalézt v uživatelském manuálu [4]. Způsob propojení se systémem EZS a postup programování bude podrobně vysvětlen v kapitole 7.2.

Obrázek 6.4: GSM brána GSM-VT-10

6.3 Ovládání pomocí LAN/Internetu

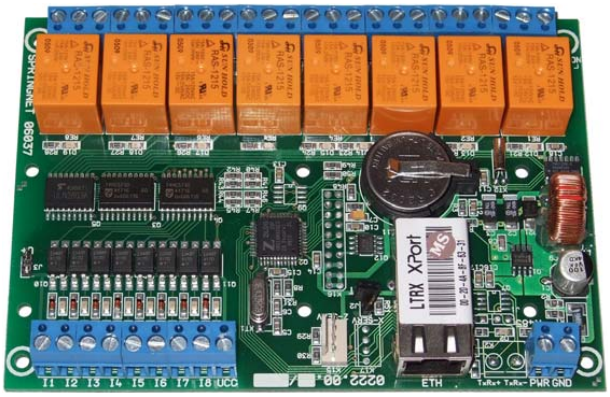
V zadání a specifikaci je obsaženo několik požadavků souvisejících s automatizací v objektu a ovládáním systému EZS přes síť LAN/Internet. Konkrétně je potřeba zajistit:

- Ovládání a sledování stavu systému EZS pomocí LAN a přes Internet.
- Archivaci a zasílání uživatelem upřesněných dat.
- Historii událostí s možností nahlížet přes LAN a Internet.
- Automatické ovládání umělého osvětlení květin podle plánovacího kalendáře. Možnost změny časů a ručního ovládání přes domácí síť LAN a přes Internet.

Pro *ovládání a sledování stavu systému EZS pomocí LAN a přes Internet* slouží modul `Paradox IP100` komunikující mimo jiné i s ústřednami Magellan. Díky zabudovanému web serveru je možné k němu přistupovat pomocí webového prohlížeče z počítače v síti LAN nebo přes Internet. Umožňuje základní ovládání ústředny EZS, monitorování jejího stavu a odesílání e-mailů při zapnutí/vypnutí, poplachu a poruše. Bohužel ale neobsahuje historii událostí v systému EZS a nesplňuje ani další kritéria specifikace.

Jako zajímavější řešení se jeví použití modulu pro automatizaci a dálkovou správu objektů `SpringNET CP-1`.

Jedná se o zařízení se zabudovaným web serverem *komunikující po počítačové síti LAN a Internetu*. Umožňuje definovat až 8 uživatelských účtů s různou úrovní oprávnění. Veškeré ovládání, sledování stavu a konfiguraci lze provádět pomocí libovolného internetového prohlížeče. Modul obsahuje 8 vstupů a 8 reléových výstupů. Jednotlivé výstupy je možno ovládat buďto ručně přes webové rozhraní, nebo automaticky pomocí časového plánu. V případě potřeby je možné nastavit závislost stavu výstupů na vstupech a realizovat tak velké množství automatizačních úkonů. Při změně stavu kteréhokoli vstupu *může být odeslán e-mail* s popisem události která změnu vyvolala a časem kdy k ní došlo. Veškerá činnost zařízení je zaznamenávána a uživatelé s příslušným oprávněním mohou prohlížet *historii obsahující 1 000 posledních událostí*. Ke každé položce je doplněno datum a čas, nechybí krátký popis a v případě změny stavu výstupu pomocí webového rozhraní i jméno uživatele, jenž změnu provedl. Obsluha a programování modulu je velice snadná, webové rozhraní je přehledné a kompletně v českém jazyce.



Obrázek 6.5: SpringNET CP-1

Informace o technickém popisu modulu `SpringNET CP-1` byly čerpány z manuálu [15]. Způsob propojení s navrhovaným systémem EZS a nastavení pro požadovanou činnost bude popsáno v kapitole 7.3. Díky použití tohoto automatizačního prvku bude umožňeno na dálku provádět tyto činnosti:

- Zapnutí/vypnutí systému EZS do/ze stavu střežení.
- Monitorování událostí (zapnutí/vypnutí, poplach, požární poplach, výpadek napájení) a zasílání e-mailů při jejich nastání či ukončení.
- Ovládání osvětlení květin podle týdenního časového plánu s možností ručního zásahu.
- Procházení historie obsahující 1 000 posledních událostí s datem a časem. Dostupné budou informace o zapnutí/vypnutí systému EZS, poplachu, požárním poplachu, výpadku napájení, zapnutí/vypnutí osvětlení květin, odeslání e-mailu a přihlášení/odhlášení uživatele.

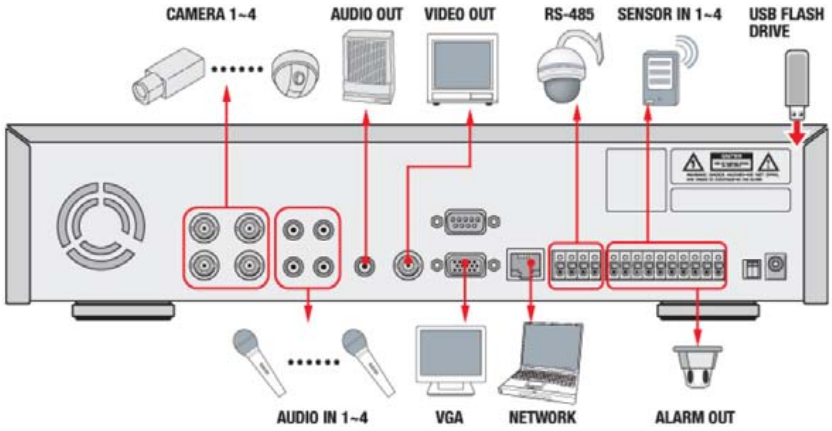
6.4 Návrh kamerového systému

Dalším bezpečnostním prvkem v objektu bude kamerový systém CCTV, který musí splňovat tyto podmínky:

- Záznam videa ze 3 kamer musí být zpětně dostupný alespoň 30 dnů.
- Přístup k aktuálním i zaznamenaným obrazovým datům přes LAN a Internet.
- Použití kvalitních venkovních barevných kamer s možností snímat i po tmě.
- Sledování aktuálního dění přes anténní TV systém na běžném televizoru.

Digitální videorekordér

Základ kamerového systému bude tvořit *triplexní digitální videorekordér* s ethernetovým rozhraním pro připojení do počítačové sítě. Triplexní znamená, že je v jednom časovém okamžiku možné současné nahrávání, přehrávání záznamu a síťový přístup. Konkrétně byl zvolen model `Nadatel SDVR-4500C`.



Obrázek 6.6: Možnosti použití videorekordéru Nadatel SDVR-4500C

Možnosti použití tohoto videorekordéru jsou patrné z obrázku 6.6. Obsahuje video/audio vstupy pro *připojení 4 kamer*, audio výstup pro připojení externího reproduktoru a obrazové výstupy na televizor a počítačový (VGA) monitor. Díky *ethernetovému rozhraní RJ-45* ho lze připojit do počítačové sítě a pomocí dodávaného softwaru k němu na dálku přistupovat. Takto je možné odkudkoli z objektu (nebo ze světa v případě připojení do Internetu) sledovat aktuální dění, přehrávat záznam a provádět jeho zálohu. Zálohovat vybrané úseky videa je navíc možné i přes port USB 2.0[1] nebo CD-RW mechaniku. Na zadní straně videorekordéru se dále nachází vývody rozhraní RS-485 pro ovládání PTZ kamer (popsáno v kapitole 3.4.2), konektory pro připojení 4 detektorů a reléový poplachový výstup (*alarm out*). Účel tohoto výstupu a použití detektorů bude popsán později.

[1]USB 2.0 je vylepšená verze staršího sériového rozhraní USB 1.1 se zachováním zpětné kompatibility. Maximální přenosová rychlost byla zvýšena z 12 Mbit/s na 480 Mbit/s.

O řízení videorekordéru se stará *Real-time operační systém* (RTOS – z anglického „Real-time operating system“). Nahrávané video/audio je hardwarově komprimováno do formátu MPEG-4 a ukládáno na zabudovaný pevný disk (HDD). K tomu je použit filesystem (souborový systém) `NaFS` společnosti `Nadatel`, jež byl navržen pro kamerová záznamová zařízení s ohledem na dosažení vysokého výkonu a co největší spolehlivosti. Díky zvolenému rozhraní E-IDE/ATA133 je možné použít jakýkoli počítačový 3.5″ HDD o maximální kapacitě 750 GB. Do zařízení lze instalovat až 4 HDD (musela by být odpojena CD-RW mechanika obsazující jednu E-IDE pozici) a dosáhnout tak celkové záznamové kapacity 3 TB. Videorekordér podporuje evropskou obrazovou normu PAL a umožňuje záznam obrazu v plném (704x576) nebo poloviční (352x288) obrazovém rozlišení. Rychlost nahrávání (počet obrazových snímků za sekundu) je sdílená mezi všemi čtyřmi kanály a pro každý libovolně nastavitelná. Při poloviční rozlišení je možné nahrávat až 100 (pro každý kanál 25) snímků za sekundu a při plném pak 25 (pro každý kanál 6) snímků za sekundu. Kvalita komprese je volitelná ve třech úrovních (standard, high a super).

Díky nastavitelným parametrům nahrávání pro každý kanál (kameru) lze dosáhnout požadovaného *poměru mezi obrazovou kvalitou a délkou záznamu*. V našem případě bude použit jeden HDD o velikosti 500 GB. Při plném obrazovém rozlišení PAL (704x576) a kvalitě komprese nastavené na „high“ se na něj vejde *40 dnů nepřetržitého záznamu ze 3 kamer* frekvencí 8 snímků/sec. Jen pro zajímavost, po omezení kvality (rozlišení 352x288, komprese „low“, 1 snímek/sec.) by se tato doba zvýšila až na 6 měsíců.

Pro každý video/audio vstup lze nastavit mód nahrávání. Dostupné jsou:

- **Nahrávání zapnuto:** Video/audio ze snímaných prostor je ukládáno.
- **Nahrávání vypnuto:** Video/audio ze snímaných prostor se nezaznamenává.
- **Detekce pohybu v obraze:** Ve snímaném obraze se definují zóny, ve kterých by nemělo docházet k pohybu. V případě že videorekordér rozpozná v těchto místech pohyb, je na určenou dobu spuštěno nahrávání. Současně s tím může být aktivován reléový poplachový výstup a *odeslán e-mail s fotografií snímaného prostoru*. Video/audio je v tomto režimu nahráváno pouze do operační paměti rekordéru a na disk se ukládá jen při rozpoznaném pohybu. Tím dochází k úspoře záznamové kapacity.
- **Detekce pohybu senzorem:** Totéž jako při detekci pohybu v obraze, jen s tím rozdílem, že se používají externí detektory připojené k videorekordéru.
- **Plánovací kalendář:** V menu rekordéru se nachází plánovací kalendář, ve kterém lze pro každou hodinu libovolného dne v týdnu nastavit mód nahrávání. Na výběr jsou všechny výše zmíněné režimy. Díky tomuto řešení lze systém přesně optimalizovat pro konkrétní objekt. Například při použití v obchodě může být záznam v pracovní době prováděn nepřetržitě, zatímco mimo ni pouze při detekovaném pohybu.

Veškeré nastavení, konfigurace a obsluha videorekordéru `Nadatel SDVR-4500C` se provádí pomocí tlačítek na předním panelu nebo dálkového ovladače. Ovládací menu je dostupné v několika jazycích, včetně Češtiny. Většina údajů použitých v této kapitole byla čerpána z oficiálních materiálů výrobce [9].

Kamery

Na celkovou kvalitu kamerového systému CCTV mají největší vliv použité kamery. V případě jejich špatné volby může být výsledkem nepěkný obraz nebo nemožnost nočního monitorování rozsáhlejších prostor. Pro navrhovaný systém bylo ve specifikaci požadováno *použití kvalitních venkovních barevných kamer s možností snímat i po tmě*. Jelikož je výběr prováděn s ohledem na umístění ve venkovních prostorách rodinného domku, neměly by být zbytečně velké, aby nekazily vzhled okolí.

S ohledem na zmíněná kritéria padla volba na venkovní barevné kamery `Avideo ACC-90X` stejnojmenného výrobce.

Obrázek 6.7: Venkovní barevná kamera Avideo ACC-90X s IR přisvětlením

Jedná se o analogovou kameru poskytující obraz po koaxiálním kabelu. Její jádro tvoří obrazový senzor `SONY` velikosti 1/3″ s obrazovým rozlišením 480 TV řádků. Ten je spolu s kvalitním objektivem umístěn do masivního hliníkového krytu kompaktních rozměrů zajišťujícího vysokou odolnost proti povětrnostním podmínkám. Okolo objektivu se nachází 48 infračervených LED a fotoelektrický prvek vyhodnocující intenzitu okolního světla. Při zhoršení světelných podmínek (při mlze, v noci) jsou IR LED automaticky aktivovány a díky tomu je i při úplné tmě možné snímat kvalitní obraz až na vzdálenost 40 metrů.

AV modulátor

Dalším požadavkem kladeným na kamerový systém bylo zajištění možnosti sledování výstupu z kamer přes anténní systém na běžném televizoru. K tomu je potřeba použít tzv. *AV modulátor*.

Obrázek 6.8: AV modulátor MD-5s

AV modulátor je zařízení, sloužící k distribuci video/audio signálu z libovolného zdroje do anténního TV rozvodu. Zjednodušeně řečeno se vloží mezi anténu a TV přijímače a na zvoleném kanále bude „vysílán“ požadovaný videosignál. Ten lze pak klasicky naladit na kterémkoli televizoru připojeném na anténním rozvodu v objektu.

Pro naše účely bude použit AV modulátor `MD-5s`. Jak vypadá je patrné na obr. 6.8. Levý vstup `RF-IN` je určen pro připojení koaxiálního kabelu vedoucího od TV antén a do konektorů vpravo se připojí video a audio výstupy z videorekordéru `Nadatel SDVR-4500C`. Pomocí ovládacích tlačítek a displeje se vybere nejvhodnější volný kanál[2], na který bude dodávaný obraz a zvuk modulován. Z výstupu `RF-OUT` bude pokračovat koaxiální kabel dále do TV anténního rozvodu v objektu. V tuto chvíli bude možné na libovolném televizoru naladit všechny dosavadní TV stanice a na zvoleném kanále i obraz z kamerového systému.

6.5 Požadavky na počítačovou síť

V navrhovaném systému budou použita dvě zařízení schopná komunikovat po počítačové síti LAN. Jedná se o automatizační modul `SpringNET CP-1` a digitální videorekordér `Nadatel SDVR-4500C`. Dále se počítá s několika (prozatím dvěma) osobními počítači. Pro realizaci této malé domácí počítačové sítě bude použit router `ASUS WL-500g Deluxe`.

Obrázek 6.9: Router ASUS WL-500g Deluxe

Jedná se o velmi rozšířený a oblíbený router, jehož firmware je založen na linuxovém jádře a nabízí velké možnosti konfigurace. Obsahuje jeden konektor `WAN` pro připojení do internetu a 4 konektory `LAN` pro přímé připojení síťových prvků (počítačů). Použití dalších síťových zařízení je možné pomocí *switche* a díky integrovanému *WiFi rozhraní* lze komunikaci realizovat i bezdrátově.

Problematika návrhu a konfigurace počítačových sítí je velice rozsáhlá a tato práce se jí podrobně nezabývá. Bude zde pouze naznačen způsob připojení výše zmíněných síťových prvků a nastavení routeru pro domácí počítačovou síť a pro přístup na Internet. Tomu je věnována kapitola 7.5.

[2] Je možné vybrat libovolný kanál v TV pásmu, ale při použití již obsazeného dojde k nahrazení stávajícího video/audio signálu signálem z AV modulátoru.

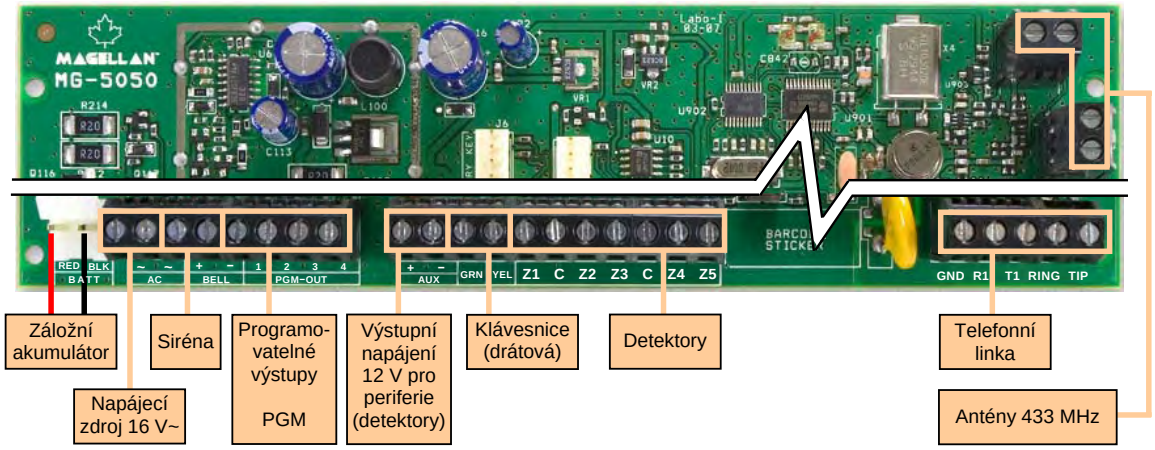
Kapitola 7

Realizace systému

V této části je podrobně popsána realizace systému pro zabezpečení a střežení specifikovaného v kap. 5 a navrženého v kap. 6. U každého dílčího prvku je naznačen způsob zapojení a konfigurace pro požadovanou činnost.

7.1 Systém EZS

Hlavním prvkem systému EZS je zabezpečovací ústředna. Dle kapitoly 6.1.1 věnované její volbě bude pro realizaci použit model `Magellan MG-5050` výrobce `PARADOX`®. Veškeré další zde použité komponenty byly popsány a jejich výběr odůvodněn v kapitole 6.1.

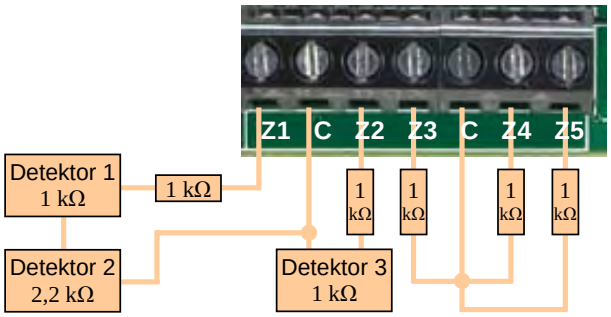


Obrázek 7.1: Zapojení ústředny PARADOX Magellan MG-5050

Způsob zapojení ústředny je patrný z obr. 7.1. Bílý konektor vlevo slouží pro připojení zálohovacího akumulátoru. Ostatní komponenty se připojují pomocí svorkovnice. Do svorek označených `AC~` je zapojen výstup z napájecího zdroje dodávajícího střídavé napětí 16 V. To je po usměrnění a upravení ústřednou na 12 V dostupné na vývodech `AUX + -` pro napájení dalších periferií (detektorů). Z výstupů `BELL + -` je přenášen poplachový stav do poplachové sirény, `GRN` a `YEL` slouží jako vstupní pro připojení klávesnice. Dále se zde nachází vývody čtyř programovatelných výstupů `PGM` a svorky pro připojení detektorů. Do svorkovnic vpravo nahoře se umísťují antény pro bezdrátovou komunikaci na frekvenci 433 MHz. Pod nimi se nachází vývody telefonního komunikátoru umožňujícího po připojení telefonní linky přenos na PCO.

7.1.1 Zapojení drátových detektorů

Na desce zabezpečovací ústředny `Magellan MG-5050` je vyvedena svorkovnice pro vytvoření pěti smyček. Přímo lze tedy zapojit 5 detektorů tvořících 5 zón. Použitím technologie `ATZ` (viz. dále) lze tuto hodnotu zdvojnásobit. Způsob připojení detektorů je naznačen na obrázku 7.2. Zapojují se po jednom (po dvou v případě zdvojení zón `ATZ`) do smyčky vždy mezi svorky `Zx` (Zóna) a `C` (COM). Pro správnou funkci ústředny EZS musí být hodnota odporu každé smyčky (i neobsazené) vždy 1 kΩ.



Obrázek 7.2: Způsob zapojení detektorů v ústředně Magellan MG-5050

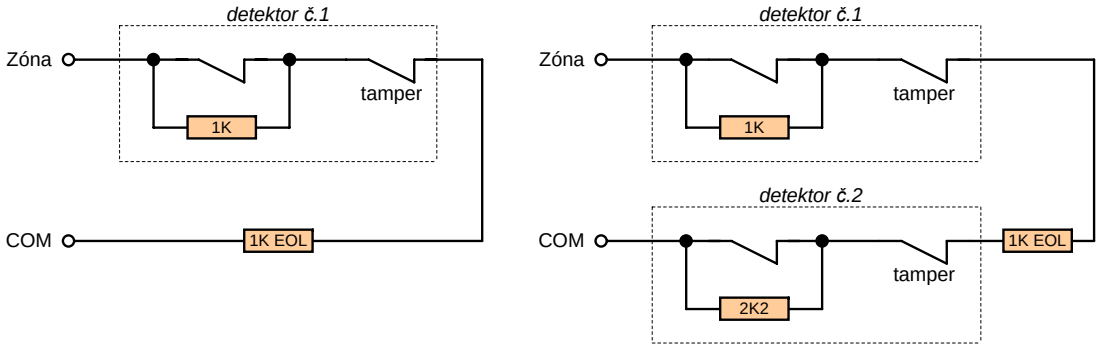
Technologie zdvojení zón (ATZ)

Z důvodu úspory místa a vodičů je možné u všech ústředen `PARADOX`® využít technologii zdvojení zón `ATZ` (z anglického „Advanced Technology Zoning“). Takto lze do jedné smyčky připojit dvě nezávislé zóny, které jsou od sebe odlišeny rozdílnou hodnotou impedance v detektorech. Na výše uvedeném obrázku 7.2 jsou pomocí `ATZ` připojeny detektory 1 a 2. Přesto že jsou oba ve stejné smyčce, tvoří každý samostatnou zónu.

Rozdíl mezi zapojením klasickým způsobem a zapojením s využitím zdvojení zón `ATZ` je patrný z obr. 7.3.

Je-li při běžném zapojení (vlevo) detektor č.1 v klidovém stavu, pak je celková impedance smyčky rovna hodnotě zakončovacího `EOL` rezistoru (tedy 1 kΩ). Ke změně této hodnoty dojde zařazením rezistoru v čidle při jeho aktivaci (impedance bude 2 kΩ), nebo rozpojením sabotážního kontaktu `tamper` při otevření čidla (impedance vzroste k ∞ kΩ). Změna odporu smyčky je ústřednou vyhodnocena jako poplachový stav, přičemž se rozlišuje, zda došlo k narušení nebo otevření detektoru. Dále je postupováno podle toho, jaký typ zóny detektor tvoří. Například je-li nastaven jako zpožděná zóna, začne běžet příchodový čas. Naproti tomu při otevření detektoru (při sabotáži) je okamžitě vyhlášen poplach.

Při zapojení využívajícím zdvojení zón `ATZ` (vpravo) má celková impedance smyčky opět hodnotu 1 kΩ. Jelikož smyčku tvoří 2 detektory, z nichž každý má být samostatnou zónou, je potřeba je nějak rozlišit. K tomu se používají rozdílné hodnoty rezistorů v každém z čidel. Při narušení detektoru č.1 bude celková hodnota impedance smyčky 2 kΩ, v případě aktivace detektoru č.2 bude 3 kΩ a při současném narušení obou čidel pak 4 kΩ. Při otevření kteréhokoliv z čidel dojde k rozpojení sabotážního kontaktu a impedance vzroste k ∞ kΩ. Každý z těchto možných stavů zapříčiní rozdílnou změnu impedance smyčky a díky tomu je ústředna EZS schopna rozpoznat, na kterém detektoru došlo k narušení.



Obrázek 7.3: Zapojení zón (klasické a se zdvojením zón ATZ)

Výhodou použití `ATZ` oproti klasickému zapojení je úspora vodičů a místa na desce ústředny (méně vývodů na svorkovnici). Nevýhodou pak nemožnost rozeznat, na kterém z dvojice detektorů došlo k rozpojení kontaktu `tamper`. v případě sabotáže.

Popis připojení a nastavení použitých drátových detektorů

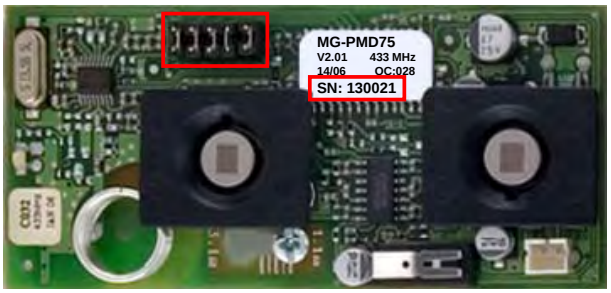
Jako smyčkové zóny jsou dle návrhu z kapitoly 6.1.2 použity níže uvedené detektory. Princip jejich zapojení do ústředny EZS je shodný s tím, jenž byl popsán výše. K napájení se používá napětí 12 V dostupné v ústředně na svorkách `AUX + -`. Všechny ostatní použité prvky jsou připojeny bezdrátově a budou popsány v kap. 7.1.2.

Detektor rozbití skla Glasstrek 457: Správná funkce je zajištěna pouze při instalaci v místnosti se stropem níže než 5 m a se sklem nepotaženým bezpečnostní fólií. Veškerá nastavení se provádí na desce elektroniky čidla pomocí přepnutí *jumperů*. Podle velikosti okolního prostoru a vzdálenosti detektoru od skleněné plochy je třeba nastavit jednu ze dvou citlivostí. Nízkou citlivost lze použít pro vzdálenost do 4,5 m, vysokou do devíti metrů. Jelikož detektor `Glasstrek 457` umožňuje použití s ústřednami smyčkového i sběrnicového typu, je třeba zvolit typ výstupu. V našem případě se pomocí jumperu nastaví typ výstupu na `RELÉ`. Dále už je způsob instalace stejný jak bylo popsáno na začátku této kapitoly.

Infrazávora VAR-TEC TRIPLE PB-150: Při instalaci je třeba dát pozor na případné oslňování jinými světelnými zdroji, obvzvláště pak sluncem. Infrazávora musí být umístěna na pevném nepohyblivém podkladu a to v místě, kde je nejnižší riziko falešných poplachů např. vlivem pohybu keřů při větru. Mezi vysílačem a přijímačem musí být přímá viditelnost a oba musí být na sebe co nejlépe nasměrovány. Toho se docílí pomocí voltmetru připojeného ke svorkám kontrolního napětí v přijímači a směrováním vysílače. Obě části infrazávory jsou správně nasměrovány v momentě, kdy kontrolní napětí dosáhne nejvyšší hodnoty. Dále je potřeba pomocí otočného voliče nastavit rychlost detekce. To je možné v rozmezí od 50 ms (přeskok, rychlý běh) do 700 ms (pomalá chůze, šplhání na zeď). Pro snížení rizika falešných poplachů např. vlivem působení slunce může být IR paprsek vysílače modulován jednou ze čtyř volitelných frekvencí. Tuto frekvenci je potřeba shodně nastavit v přijímači i vysílači pomocí přepnutí příslušných jumperů.

7.1.2 Zapojení bezdrátových detektorů

K zabezpečovací ústředně `Magellan MG-5050` je možné připojit až 32 bezdrátových detektorů. Každý má z výroby své jedinečné sériové číslo, které je většinou nalepeno uvnitř na desce s elektronikou. Zapsáním tohoto čísla do ústředny na příslušnou adresu (viz. programování ústředny v kap. 7.1.7) dojde k přiřazení detektoru do konkrétní zóny. Pro dokončení připojení je poté ještě potřeba bezdrátové čidlo narušit. Další nastavení detektorů se provádí většinou pomocí *jumperů*. Jejich podoba a umístění se může u jednotlivých typů lišit. Pro napájení se používají běžné alkalické baterie. Pokles jejich napětí pod určitou mez je ústřednou prostřednictvím klávesnice signalizován a je potřeba baterie co nejdříve vyměnit. Jejich životnost je závislá na počtu uskutečněných přenosů mezi konkrétním detektorem a ústřednou a u většiny typů se pohybuje v rozmezí 1 – 4 roky.



Obrázek 7.4: Jumpery a sériové číslo na desce bezdrátového detektoru

Na obrázku 7.4 je fotografie elektroniky bezdrátového čidla `PARADOX MG-PMD75` s vyznačením jumperů a štítku se sériovým číslem.

Následuje popis způsobu instalace a nastavení bezdrátových detektorů zvolených v kapitole 6.1.2. Z důvodů zamezení vzájemného rušení vysílačů je třeba dodržet minimální vzdálenost 50 cm mezi čidly a 2 m od vysílače/přijímače bezdrátové ústředny. Veškeré poznatky o podmínkách instalace jsou čerpány z instalačního manuálu [14] k ústředně `Magellan MG-5050`.

Bezdrátový PIR detektor MG-PMD1P: Do detektoru je třeba nejdříve vložit 3 AA alkalické baterie. Fyzicky by měl být instalován ve výšce mezi 1,8 m – 2,7 m kdy je zaručeno pokrytí prostoru 11 x 11 m. Pomocí jumperů se pak nastaví jedna ze dvou úrovní citlivosti a zda bude čidlo pracovat v režimu `single` či `dual` (zvýšená odolnost proti falešným poplachům).

Bezdrátový magnetický kontakt MG-DCT2: Vysílací část magnetického kontaktu se instaluje vždy na pevnou část dveří (okna, atd.), druhá část potom přímo na dveře (okno, atd.). Je potřeba dát pozor na to, aby vzdálenost mezi vysílací částí a magnetem byla při klidovém stavu (zavřené dveře, okno, atd.) co nejmenší. K napájení slouží knoflíková baterie CR 2450.

Bezdrátový požární detektor MG-SD738: Správná funkce detektoru je zajištěna jen při použití v místnosti kratší než 12 m. Nejvhodnější umístění je na střed stropu, není-li to z jakéhokoliv důvodu možné pak minimálně 10 cm od rohu. Pro oživení je potřeba do detektoru vložit 9 V baterii a na 5 s podržet tlačítko na čelní straně. Poté dojde k ověření funkčnosti krátkou aktivací sirény a přihlášení do přijímače ústředny.

7.1.3 Zapojení sirény

Poplachová siréna `TEKNIM-720WR` se připojuje kabelem přímo na desku ústředny. Konkrétně na svorky `BELL + -` a napájecí `AUX + -` (viz. obr. 7.1). Je určena pro instalaci do venkovních prostor a je potřeba ji umístit do takové výšky, aby k ní nebyl snadný přístup. Většinou se jako nejvhodnější jeví prostor na obvodové zdi těsně pod střechou objektu. Pro zálohování sirény v případě výpadku elektřiny slouží vnitřní akumulátor.

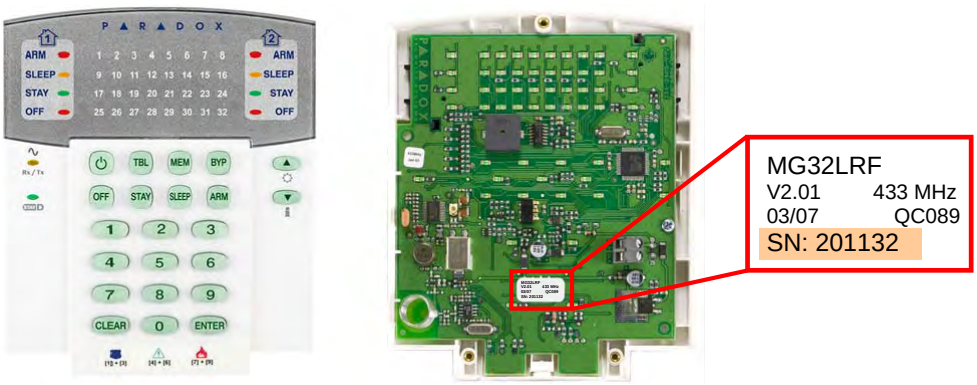
Veškeré nastavení se provádí opět pomocí *jumperů* umístěných na desce s elektronikou. Je možné nastavit rychlost houkání (rychlé `HIGH` nebo pomalé `LOW`) a dobu trvání signalizace poplachu (3 nebo 15 minut). Dále je třeba určit, zda bude siréna pracovat v napájecím módu `SAB` nebo `SCB`. V prvně zmiňovaném slouží baterie jen pro případ zálohy a proud při poplachu je odebírán přímo z ústředny ze svorek `AUX + -`. V našem případě bude použit režim `SCB`, kdy pro kompletní napájení slouží zálohovací baterie a z ústředny je odebíráno pouze 30 mA pro její dobíjení. Díky tomuto řešení dojde ke snížení proudové zátěže výstupů `AUX + -` a ke zvýšení spolehlivosti systému EZS.

7.1.4 Zapojení bezdrátové klávesnice

Pro připojení drátových klávesnic slouží svorky `GRN` a `YEL` desce ústředny (viz. obr. 7.1). V případě použití bezdrátové klávesnice (náš případ) je postup obdobný jako u bezdrátových detektorů.

Klávesnice `Magellan MG32LRF`, jenž je v navrhovaném systému použita, obsahuje akumulátor sloužící jen jako záložní v případě výpadku elektřiny. Pro napájení je třeba použít napájecí zdroj 230 V / 6 V, 300 mA. Při instalaci klávesnice je třeba stejně jako u bezdrátových detektorů dodržet minimální vzdálenosti od vysílače/přijímače ústředny a ostatních čidel. Jelikož je používána hlavně k zapínání a vypínání systému EZS, měla by být umístěna poblíž vchodu do objektu. Většinou tedy do předsíně nebo vstupní chodby.

Od okamžiku zapnutí ústředny EZS je po dobu deseti minut možné provést připojení bezdrátových klávesnic. Současným stisknutím tlačítek `[POWER]` a `[BYP]` na klávesnici na dobu tří sekund dojde k jejímu přihlášení. Poté je potřeba zapsat do ústředny na příslušnou adresu (viz. programování ústředny v kap. 7.1.7) její sériové číslo. Pod tímto jedinečným identifikátorem bude vysílač klávesnice komunikovat s ústřednou EZS. Sériové číslo bývá většinou nalepeno na štítku na desce s elektronikou.

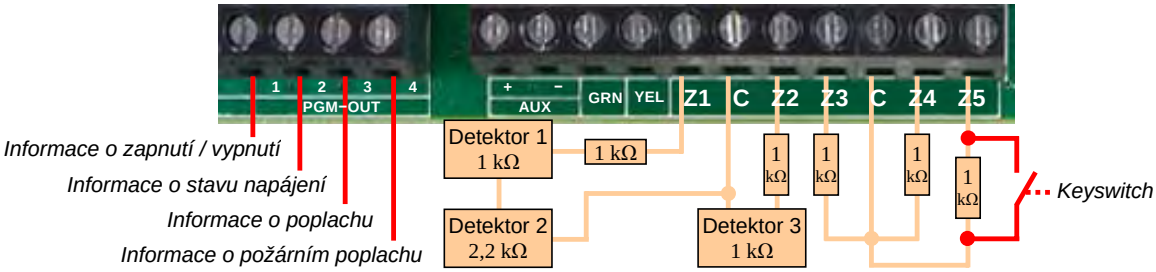


Obrázek 7.5: Sériové číslo na desce klávesnice Magellan MG32LRF

7.1.5 Ovládání pomocí Keyswitch

Pro spolupráci s dalšími moduly je v ústřednách PARADOX® dostupná funkce Keyswitch umožňující zapínání/vypínání systému pomocí obyčejného tlačítka či přepínače. Jako „přepínač“ může sloužit i relé, jež je zabudované ve většině modulů. Díky tomu bude možné realizovat ovládání pomocí GSM brány (popsáno v kap. 7.2) a automatizačního modulu SpringNET (kap. 7.3).

V ústředně Magellan MG-5050 je tato funkce zapouzdřena do typu zóny. Jinými slovy stačí připojit tlačítko (přepínač, relé) podobně jako detektory a jako typ zóny, kterou bude tvořit, programově nastavit Keyswitch. Způsob zapojení je naznačen na obr. 7.6 (vpravo).



Obrázek 7.6: Využití výstupů PGM a způsob zapojení Keyswitch

Pro rozlišení mezi přepínačem (zachovává stav ON nebo OFF) a tlačítkem (stisk = impuls) je možné definovat zóny Keyswitch-spínač a Keyswitch-tlačítko [14]. Při použití prvně jmenované by nastal problém při náhlém odpojení automatizačního modulu nebo GSM brány v době, kdy je systém EZS zapnut. Přerušením napětí by došlo k překlopení relé do pozice OFF a tím k platnému vypnutí systému! S ohledem na vyšší odolnost proti sabotáži bude zóna v našem případě definovaná jako Keyswitch-tlačítko a ovládána krátkým impulzem relé.

7.1.6 Programovatelné výstupy PGM

Na desce ústředny Magellan MG-5050 jsou vyvedeny 4 programovatelné výstupy PGM. Použitím bezdrátových modulů MG-2WPGM lze tento počet zvýšit až na 16. Integrované výstupy jsou realizovány jako polovodičová relé s volitelnou polaritou. Pomocí jumperů lze pro všechny společně zvolit, zda se mají spínat na + (12V) nebo na - (0V). Mohou být zatíženy pouze stejnosměrným proudem z ústředny a to maximálně 100 mA.

Pro každý z výstupů je možné programově nastavit, při jaké situaci dojde k jeho aktivaci a způsob, jakým bude deaktivován. To je možné buďto po uplynutí určitého časového okamžiku, nebo na základě nějaké jiné události. Například k sepnutí může dojít při poplachu a k deaktivaci ihned po jeho skončení. Událostí na které lze reagovat je velice mnoho a jejich úplný přehled je uveden v programovacím manuálu ústředny [16, str. 26]. V realizovaném systému budou výstupy PGM využity (obr. 7.6) k indikaci výskytu a ukončení těchto stavů:

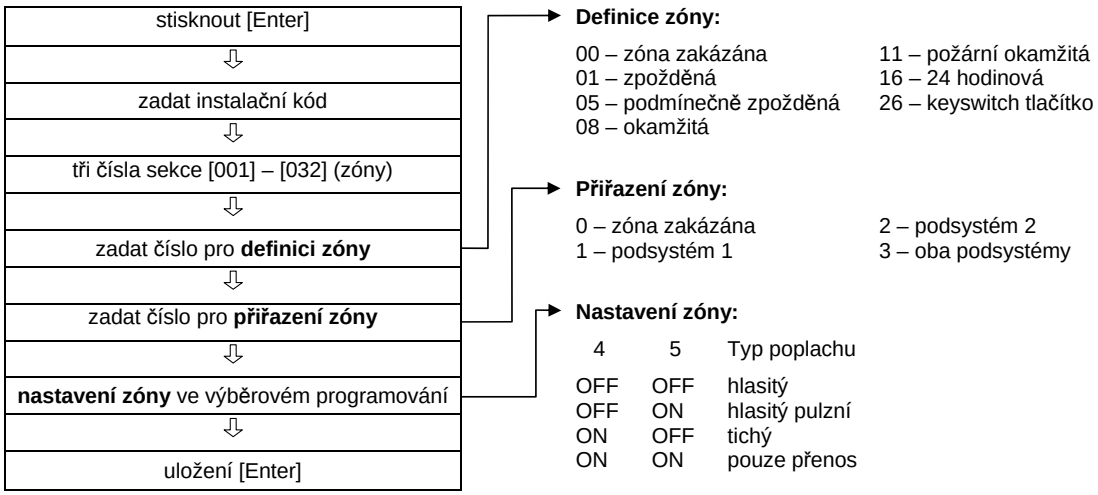
Výstup	Událost	Modul
PGM 1	Zapnutí/vypnutí systému	SpringNET, GSM brána
PGM 2	Porucha napájení	SpringNET
PGM 3	Poplach	SpringNET, GSM brána
PGM 4	Požární poplach	SpringNET

7.1.7 Programování ústředny

Podrobný popis programování ústředny EZS by vydal na samostatnou publikaci. Tato práce se zabývá návrhem a realizací systému pouze z hlediska nejrůznějších požadavků a způsob programování zde bude jen naznačen. Kompletnímu nastavení ústředny `Magellan MG-5050` se věnuje manuál [16], ze kterého byla čerpána většina zde uvedených informací.

Veškerá činnost ústředny EZS je řízena prostřednictvím mikroprocesoru vnitřním programem (tzv. *firmware*). Ten je v ústředně uložen od výrobce. Pomocí klávesnice je možné měnit hodnoty na jednotlivých sekcích (adresách) a tím nastavovat parametry ústředny a definovat její reakce na nejrůznější události. Při programování se uplatňují dva způsoby. Konkrétně *zadávání hodnot* a *výběrové programování*. Prvně zmiňovaným se myslí klasický zápis číselných hodnot (např. příchodový čas, doba trvání poplachu). Při *výběrovém* způsobu reprezentuje svit jednotlivých kláves `[1]` až `[8]` aktivaci požadované funkce. Stiskem příslušné klávesy dojde vždy ke změně stavu (aktivace, deaktivace, aktivace, ...).

Pro demonstraci výše uvedených způsobů poslouží ukázka **programování zón**. Uplatňovaný postup je graficky znázorněn na následujícím schématu (převzato z [16, str. 10]).

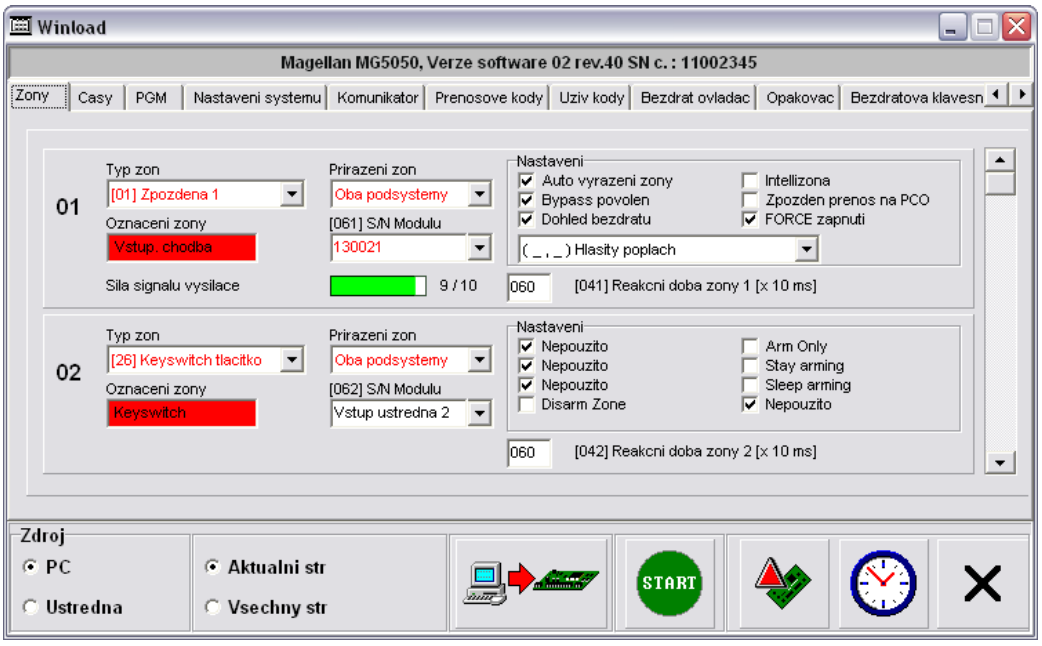


Do programovacího režimu se vstoupí stiskem klávesy `[Enter]` a následným zadáním bezpečnostního kódu (továrně `000000`). Poté je očekáváno trojciferné *číslo sekce*, v níž bude prováděno nastavování konkrétní zóny. To zjistíme v manuálu ústředny, v našem případě tedy v [16]. Chceme-li např. nastavit parametry *zóny 1*, zadáme hodnotu `001` (nebo `061` je-li použit bezdrátový detektor). Dále se pomocí dvojciferného čísla volí *typ zóny* (zpožděná, okamžitá, atd. – viz. kapitola 3.2.2). Následuje *přiřazení do podsystémů*. Není-li aplikováno rozdělení na podsystémy, zadáme hodnotu `1` („*podsystém 1*“ reprezentuje v tomto případě celý systém). Posledním krokem je nastavení dalších parametrů zóny pomocí výběrového programování. Zde je možné mimo jiné definovat i typ poplachu při narušení. Například pokud nastavovanou zónu tvoří tlačítko `PANIK`, nastavíme *tichý poplach* (klávesa `[4]` bude `ON`, `[5]` bude `OFF`). Nakonec je potřeba provedené změny uložit tlačítkem `[Enter]`.

Obdobným způsobem jaký byl demonstrován na ukázce nastavování zón se programují veškeré funkce ústředny. Vždy se tak děje zadáním nebo změnou údajů na příslušné sekci v paměti ústředny. Kompletní seznam sekcí je uveden v již zmiňovaném manuálu [16].

Většinu ústředen PARADOX® je možné programovat i pomocí počítače, díky zdarma dodávanému software WinLoad. Propojení s počítačem je realizováno přes speciální konektor na desce ústředny, do něhož lze zapojit kabel na druhé straně zakončený sériovým rozhraním RS-232 nebo USB. Programování ústředny je možné i na dálku přes telefonní linku napojenou na komunikátor ústředny nebo s využitím modulu Paradox IP100 popsaného v kapitole 6.3).

Software WinLoad je v podstatě databáze umožňující spravovat systémy EZS ve velkém množství objektů z jednoho počítače. K jednotlivým ústřednám je možné se připojit vzdáleně (modem, modul Paradox IP100) nebo lokálně pomocí výše popisovaného kabelu. Po zadání *instalačního hesla* lze v ústředně provádět veškeré programování obdobně jako pomocí klávesnice, avšak mnohem rychleji a pohodlněji. Na místo ručního zadávání sekcí a příslušných dat stačí jen zaškrtnout požadované funkce v konfiguračním okně programu. Ten se poté sám postará o zápis do ústředny na správnou sekci.

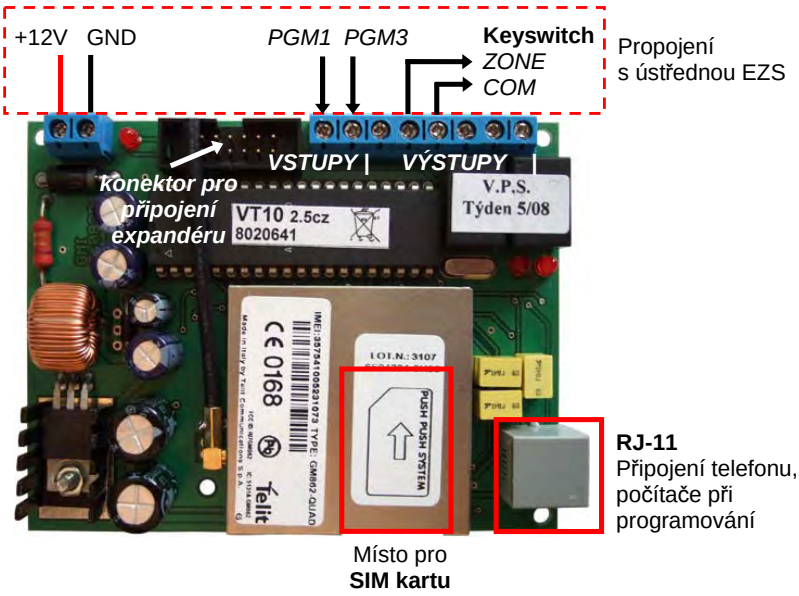


Obrázek 7.7: Programování ústředny EZS pomocí programu WinLoad

Na obrázku 7.7 je zachyceno okno programu WinLoad s volbami pro konfiguraci zón. Bylo vybráno záměrně pro možnost srovnání s ručním programováním zón popsaným na předchozí straně.

7.2 GSM brána

Pro možnost ovládání systému EZS pomocí GSM sítě je použita `GSM brána GSM-VT-10`, která je popsána v kapitole 6.2. Jedná se o modul se dvěma vstupy s dvěma ovladatelnými reléovými výstupy. Jejich počet lze v případě potřeby rozšířit pomocí expandéru. Způsob zapojení a propojení GSM brány s ústřednou systému EZS je patrný z obrázku 7.8.



Obrázek 7.8: Zapojení GSM brány GSM-VT-10

Napájení (+12 V) je dodáváno ze zabezpečovací ústředny ze svorek `AUX + -`. Do vstupů GSM brány jsou napojeny programovatelné výstupy ústředny `PGM1` (informace o zapnutí, vypnutí) a `PGM3` (poplachový stav a jeho ukončení). K aktivaci vstupů dojde při sepnutí příslušného `PGM` a tím propojení na záporný napájecí potenciál (`GND`). Pro zapínání systému EZS je využito relé, jehož výstupy jsou v ústředně zapojeny jako zóna `Keyswitch-tlačítko` (viz. kapitola 7.1.5).

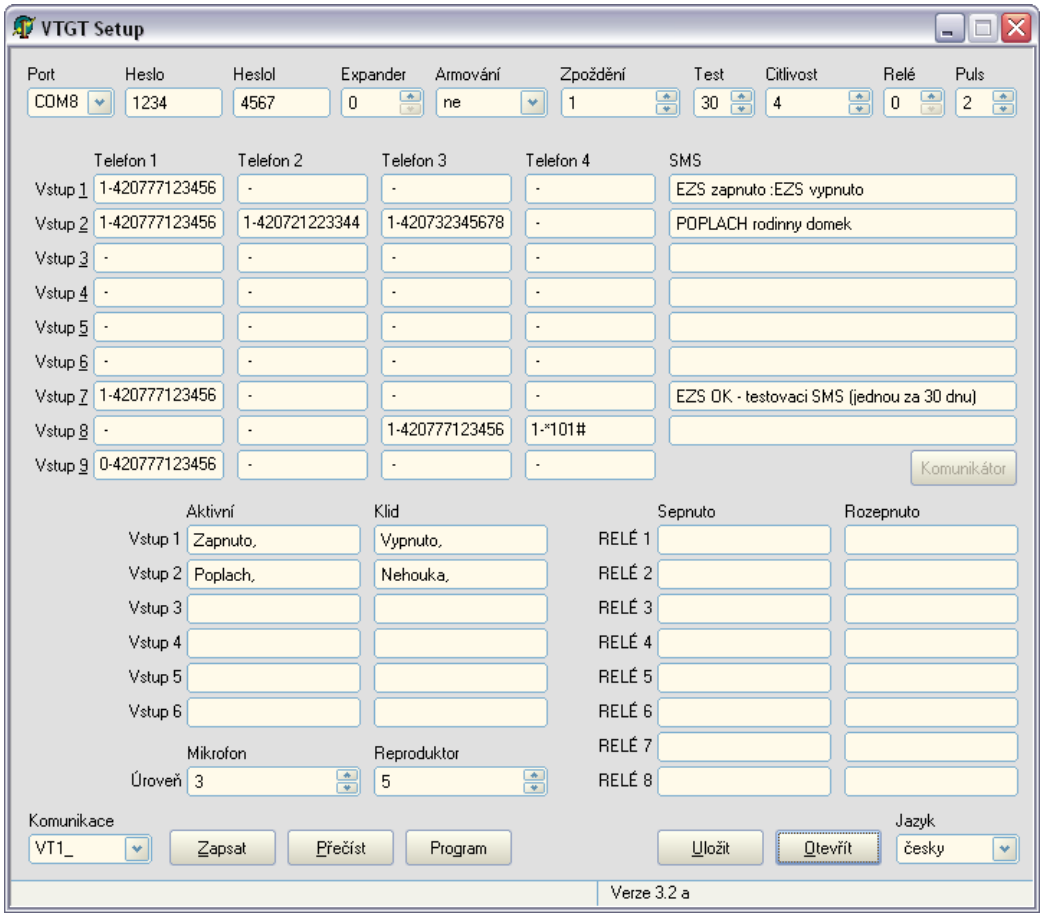
Při výše uvedeném zapojení a po nakonfigurování GSM brány bude možné systém zapínat pomocí SMS zpráv v určitém formátu (viz. dále), nebo prozvoněním z definovaného telefonního čísla. Při každém zapnutí, vypnutí a poplachu odešle GSM brána informační SMS zprávu. Pro zajištění těchto činností je třeba použít SIM kartu sítě GSM. Ta se vkládá do slotu na spodní straně modulu.

Při použití expandéru[1] `VT-04 VOICE` je možné přenášet kromě SMS i hlasové zprávy. GSM bránu `GSM-VT-10` lze navíc využít i pro simulaci „pevné linky“ v objektech, kde není zavedena. K tomuto slouží konektor `RJ-11` (vpravo dole – viz. obr. 7.8). Pro zařízení do něj připojené (telefon, komunikátor ústředny) se potom GSM brána tváří jako „pevná linka“. Výše zmíněný konektor slouží i k propojení s počítačem při programování.

[1] Rozšiřující expandéry se připojují do konektoru na GSM bráně (viz. obrázek 7.8). Jejich účelem je rozšíření stávajícího počtu vstupů a výstupů, nebo přidání nových funkcí. K modulu GSM-VT-10 jsou dostupné 4 typy expandérů. Jsou popsané v manuálu [4].

7.2.1 Konfigurace pomocí počítače

Propojení s počítačem je realizováno přes sériové rozhraní `RS-232` kabelem, zakončeným na druhé straně konektorem `RJ-11`. Ten se v GSM modulu zapojí do konektoru pro připojení telefonu (viz. obr. 7.8). Samotná konfigurace potom probíhá pomocí softwarové utility `VTGT Setup`, jež je zachycená na obrázku 7.9.



Obrázek 7.9: Konfigurace GSM brány pomocí utility VTGT Setup

Pro navázání spojení je třeba nejdříve zvolit **Port**, přes který je GSM brána k počítači připojena (v našem případě `COM8`). Poté v položce **Komunikace** vybereme volbu `VT1_` (komunikujeme s modulem `GSM-VT-10`) a do položek **Heslo** a **HesloI** zadáme zvolená hesla. První bude sloužit pro ovládání vstupů a výstupů pomocí SMS (nastavíme ho na „1234“), druhé pak jako instalační pro změny v konfiguraci (zvolíme „4567“). Po stisku tlačítka `[Program]` přejde modul do programovacího režimu, v němž je možné zapisovat a načítat nastavení z GSM brány. K tomu slouží tlačítka `[Zapsat]` a `[Přečíst]`. Provedené nastavení je možné uložit do externího souboru a v případě potřeby potom kdykoli načíst pomocí příkazů `[Uložit]` a `[Otevřít]`.

Následující popis konfigurace GSM brány bude proveden na základě konkrétních nastavení pro účely našeho systému. Nebudou zde naznačeny všechny dostupné možnosti, ale jen ty použité. Kompletní popis GSM brány `GSM-VT-10` a její konfigurace lze nalézt v uživatelském manuálu [4] ze kterého byla čerpána většina zde uváděných informací.

V hlavním okně programu `VTGT Setup` (obr. 7.9) se kromě již zmiňovaných položek (**Port**, **Heslo** a **HesloI**) nachází mnohé další volby:

Expander: Je potřeba nastavit na hodnotu „0“, což určuje, že není použit žádný rozšiřující modul (expandér).

Test: Určuje dobu, po které je periodicky zasílána testovací zpráva definovaná na řádku **Vstup 7**. Lze zadat hodnoty od 0 (zpráva se neodesílá) do 30. Nastavíme „30“ pro test každých 30 dnů.

Relé: Nastavením hodnoty „0“ definujeme, že `RELE1` a `RELE2` budou ovládány pomocí SMS. Toto je potřeba z důvodu realizace požadavku na ovládání zabezpečovacího systému pomocí SMS.

Puls: Reprezentuje délku pulsu výstupních relé v sekundách. V našem případě bude nastavena hodnota „2“ a výstupní relé se tak bude chovat stejně, jako stisk tlačítka na dobu 2 s. To poslouží ve spolupráci s funkcí `Keyswitch-tlačítko` (viz. kap. 7.1.5) pro zapínání/vypínání systému EZS.

Telefon 1 – 4: Každému ze vstupů lze přiřadit 4 telefonní čísla, na která bude přenášena zpráva. Číslo se zadává ve formátu `X-YYYYYYYYYYYY`, kde `X` určuje typ volání a `YYYYYYYYYYYY` udává telefonní číslo v mezinárodním formátu (např. 420777123456). Typ volání určuje typ reakce na aktivaci daného vstupu. Dostupné možnosti jsou např. „1 - pošle SMS“, „3 - prozvoní zadané tel.číslo“, „8 - odešle SMS a prozvoní zadané tel. číslo, po přijmutí hovoru přehraje hlasovou zprávu“ a další tyto kombinace. Posledně jmenované je dostupné jen při použití hlasového expandéru `VT-04 VOICE`. Pro naše účely bude u všech tel. čísel použit typ volání „1 - pošle SMS“, což se zapíše jako `1-420777123456`.

SMS: Do tohoto pole se zadává text SMS zprávy, která bude odeslána při aktivaci daného vstupu. Použitím znaku „:“ se zpráva rozdělí na 2 části. První se odešle při aktivaci daného vstupu, druhá při jeho opětovném přechodu do klidového stavu.

Řádky „Vstup 1 – 8“: Každý řádek reprezentuje 1 vstup a lze pro něj definovat 4 telefonní čísla s typem volání (viz. výše) a případné texty SMS zpráv. Pokud není připojen některý z expandérů, jsou použitelné pouze vstupy 1, 2 (vstupy na modulu) a 7, 8.

- **Vstup 1** Ke *vstupu 1* je fyzicky připojen výstup `PGM1`, který informuje o zapnutí/vypnutí ústředny EZS. Proto jsou na tomto řádku definovány texty SMS a telefonní číslo pro zasílání zprávy při zapnutí a vypnutí systému EZS.
- **Vstup 2** Totéž jako u **Vstupu 1**, jen s rozdílem, že se definují zprávy a telefonní čísla pro zasílání informací o poplachu. (Na *vstup 2* je připojen výstup `PGM3`.)
- **Vstup 7** Na tomto řádku se definuje testovací zpráva a telefonní číslo, na něž bude zasílána (viz. položka „**Test**“).
- **Vstup 8** Na tomto řádku jsou první dvě kolonky pro telefonní čísla nevyužity, do 3. se zadává telefonní číslo, na které bude zasíláno automatické upozornění o nízkém stavu kreditu na SIM kartě. Do políčka pro 4. tel. číslo se zadává řetězec pro zjišťování stavu kreditu u konkrétního operátora (námi použité `*101#` odpovídá SIM kartě sítě `T-Mobile`).

Řádek „Vstup 9“: Lze zadat až 4 telefonní čísla pro spínání výstupních `RELÉ 1` a `RELÉ 2`. K sepnutí dojde po krátkém „prozvonění“ čísla GSM brány z jednoho z těchto telefonních čísel. Úspěšnost spínací operace je potvrzena tím, že GSM brána hovor cca po dvou vyzvoněních ukončí a poté provede sepnutí příslušného relé. Telefonní čísla se zadávají se opět ve tvaru `X-YYYYYYYYYYYY`, kde `X` tentokrát určuje typ sepnutí. Na výběr jsou např. možnosti „1 - sepne relé 1“, „2 - rozepne relé 1“, „8 - neguje relé 2“ a další kombinace. V našem případě bude uplatněno nastavení „0 - sepne pulsně relé 1“, při kterém dojde k aktivaci `RELÉ 1` na dobu zadanou v položce „**Puls**“. Konkrétně bude tedy nastaveno `0-420777123456`, což určuje, že `RELÉ 1` bude po prozvonění z uvedeného čísla pulsně sepnuto na dobu 2 s. Jelikož je do ústředny zapojeno jako zóna `Keyswitch-tlačítko` dojde při jeho pulsu k zapnutí nebo vypnutí systému EZS (vždy změna předchozího stavu).

Pojmenování vstupů „Vstup 1 – 6“: Stavy jednotlivých vstupů při aktivaci a v klidu je možné pojmenovat. Tyto názvy použije GSM brána do odpovědí na dotaz na stav vstupů a výstupů (viz. dále).

Pojmenování výstupů „RELÉ 1 – 8“: Stejně jako u vstupů lze i u výstupů pojmenovat stav při jejich sepnutí nebo rozepnutí. Tyto názvy použije GSM brána do odpovědí na dotaz na stav vstupů a výstupů. V našem případě zůstanou políčka pro pojmenování výstupů prázdná a názvy výstupů tak nebudou ve zmiňované odpovědi figurovat. Není to totiž potřeba, jelikož je v fyzicky použito pouze `RELÉ 1`, a to navíc pouze na realizaci krátkého pulsu.

Pro dokončení konfigurace je potřeba pomocí tlačítka `[Zapsat]` odeslat nastavení do GSM modulu. Tlačítkem `[Uložit]` je možné provést zálohu do souboru. Konfigurační soubor s výše popisovaným nastavením je přiložen na datovém nosiči k této práci.

7.2.2 Způsoby využití GSM brány při ovládání EZS

Systém EZS, připojený k takto nastavené GSM bráně, lze pomocí telefonu v síti GSM ovládat hned několika způsoby. Následuje krátký popis dostupných možností včetně ukázek zasílaných SMS zpráv.

Zapnutí / vypnutí

- Zapnutí nebo vynutí zabezpečovacího systému pomocí GSM modulu provedeme zavoláním z tel.č. `420777123456`. Volání je po 2 – 3 vyzvoněních ze strany GSM brány samo ukončeno (zapínací/vypínací operace je tedy zdarma).

- V případě potřeby ovládat systém i z jiného telefonního čísla než `420777123456` je toto možné zasláním SMS ve tvaru: `HESLO P 1`
  Na místo „HESLO“ musí být uvedeno čtyřmístné heslo, které bylo zadáno při konfiguraci. Zápis „P 1“ znamená, že dojde k pulsnímu sepnutí `RELÉ 1`.
  V našem případě tedy odešleme: `1234 P 1`

- Při každém zapnutí/vypnutí zabezpečovacího systému je na tel.č. `420777123456` zaslána informační SMS v podobě „*EZS zapnuto*“ popř. „*EZS vypnuto*“. Děje se tak jak při ovládání pomocí GSM brány, tak při jakémkoli zapnutí zapnutí/vypnutí přímo na klávesnici v objektu.

- Pokud chceme kdykoli zjistit, v jakém stavu se systém zrovna nachází, můžeme se na jeho stav „zeptat“ pomocí SMS: `HESLO S`
  Konkrétně tedy: `1234 S`
  Následně nám bude (na tel.č. ze kterého byla SMS odeslána) doručena od GSM modulu zpráva zhruba tohoto znění:
  „*Vstupy: Vypnuto, Nehouka,*“ (EZS vypnut)
  „*Vstupy: Zapnuto, Nehouka,*“ (EZS zapnut a v klidovém stavu)
  „*Vstupy: Zapnuto, Poplach,*“ (EZS zapnut, nastal poplach)

Poplach

- Při poplachu dojde k zaslání SMS zprávy „*POPLACH rodinny domek*“ na tel.čísla `420777123456`, `420721223344` a `420732345678`. Po jeho skončení se nic nezasílá, ale bylo by to v případě potřeby samozřejmě možné.

Testovací zpráva

- Jednou měsíčně (interval lze změnit nebo úplně vypnout) zašle GSM brána na tel.č `420777123456` SMS ve tvaru: „*EZS OK - testovaci SMS (jednou za 30 dnu)*“, čímž je potvrzena kontrola funkčnosti.

- Funkčnost GSM modulu lze otestovat kdykoli z jakéhokoli telefonního čísla zasláním SMS zprávy ve tvaru: `HESLO T`
  V našem případě tedy odešleme: `1234 T`
  Poté nám GSM modul začne volat na číslo, ze kterého jsme SMS posílali. Hovor můžeme odmítnout, protože už jen to, že se modul ozve, je důkazem jeho funkčnosti.

Operace s kreditem

- Každých 24 hodin je prováděna automatická kontrola výše kreditu[2] na SIM kartě. Při zjištění jeho zůstatku pod částku 40 Kč, je na telefonní číslo `420777123456` zasláno upozornění a informace o jeho výši. Kredit je poté potřeba co nejdříve dobít.

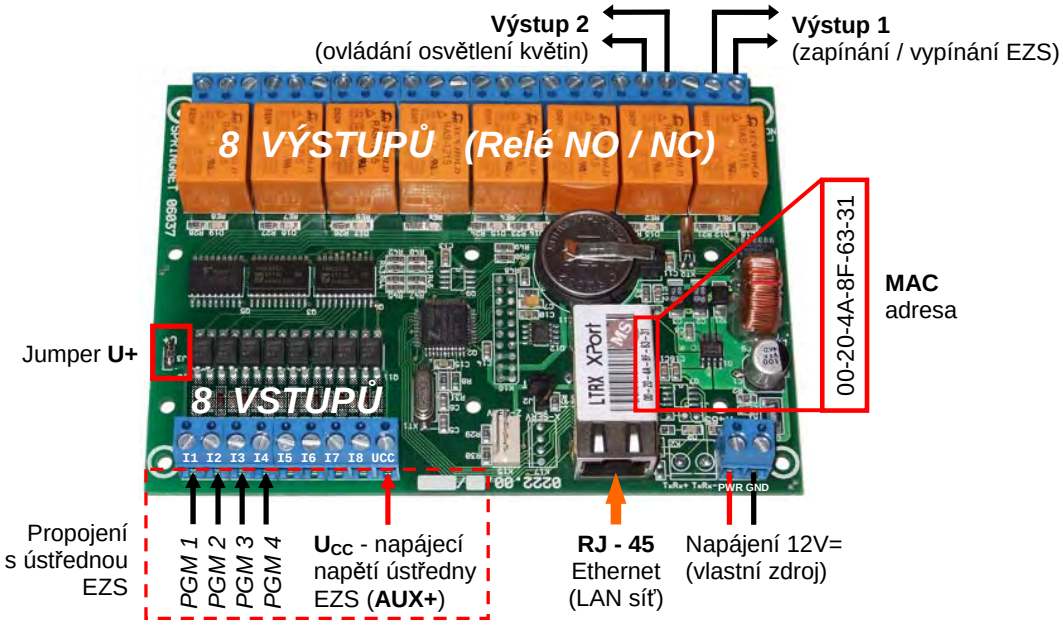
- Výši kreditu lze rovněž zjistit kdykoli z jakéhokoli telefonního čísla zasláním SMS ve tvaru: `HESLO K`
  V našem případě tedy odešleme: `1234 K`
  Po chvíli nám GSM brána odpoví SMS zprávou se zůstatkem kreditu na kartě. Při nízkém stavu by měl být opět co nejdříve dobit.

[2] Kontrolu výše kreditu má smysl provádět jen při použití předplacené SIM karty s kreditem. V případě použití SIM karty s paušální platbou je třeba ji při konfiguraci GSM brány deaktivovat smazáním 3. a 4. telefonního čísla u „Vstupu 8“.

7.3 Automatizační modul

Pro ovládání systému EZS pomocí počítačové sítě nebo Internetu je použit automatizační modul `SpringNET CP-1` obsahující 8 vstupů a 8 výstupů. Podrobně byl popsán v kapitole 6.3. Obsahuje zabudovaný webserver a lze k němu přistupovat přes klasický webový prohlížeč z jakéhokoli počítače připojeného v počítačové síti (nebo Internetu). Aktivace výstupů je možná ručně nebo podle časového kalendáře. Rovněž umožňuje zasílat e-maily při určitých definovaných událostech a poskytuje přístup k historii tisíce posledních událostí.

V našem systému je použit pro zapínání/vypínání ústředny EZS, ukládání událostí v systému do historie a k automatickému ovládání osvětlení květin dle definovaných časů (viz. specifikace v kapitole 5). Způsob zapojení modulu je patrný z obrázku 7.10.



Obrázek 7.10: Zapojení modulu SpringNET CP-1

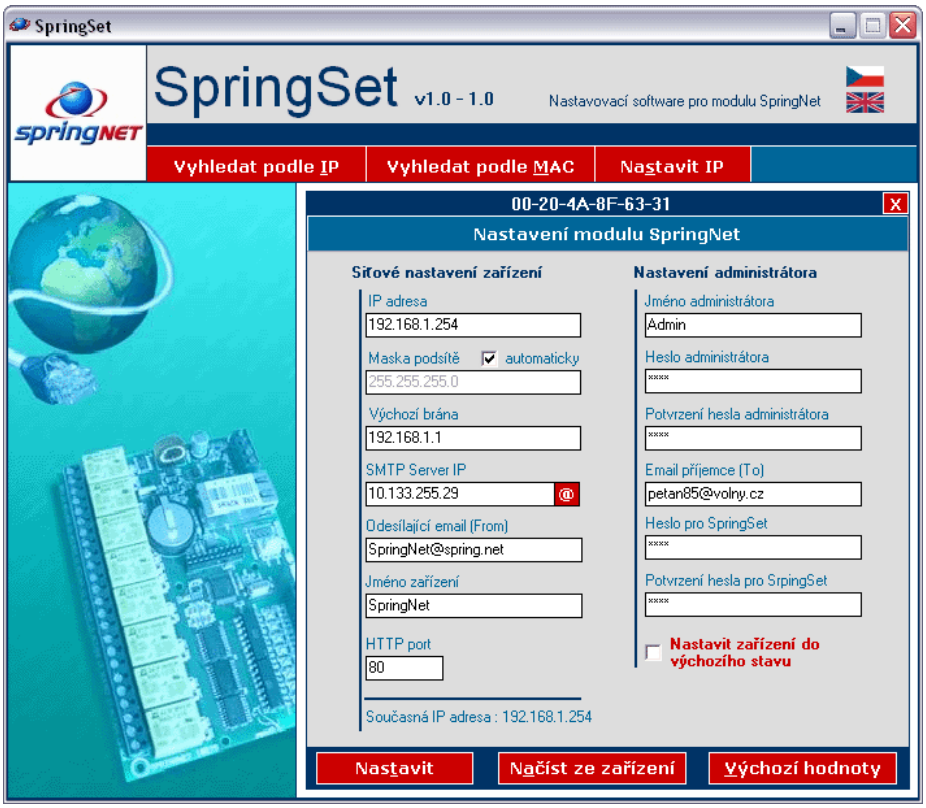
Napájení modulu může být řešeno dvěma způsoby. Buďto jako společné se systémem EZS (odebíráno na ústředně ze svorek `AUX + -`), nebo realizováno vlastním zdrojem stejnosměrného napětí 12 V. Jelikož je k ústředně již připojena GSM brána s relativně velkým špičkovým proudovým odběrem, jeví se jako vhodnější použití druhého způsobu. Díky samostatnému napájení je možné modul umístit do jiných prostor než ústřednu EZS a navíc je tím i zvýšena celková stabilita systému. K rozlišení použitého způsobu je na modulu vyveden `Jumper U+`, který musí být v tomto případě rozpojen.

Fyzické připojení modulu do počítačové sítě se realizuje stejně jako u jakéhokoli jiného síťového prvku. Tedy přímým UTP kabelem `Cat 5e` zakončeným konektorem `RJ-45`. V levé spodní části se dále nachází svorkovnice pro zapojení osmi vstupů (`I1` až `I8`) a svorka `Ucc`, do níž je v případě použití samostatného napájení (náš případ) potřeba přivést +12 V z externího zařízení. K aktivaci jednotlivých vstupů pak dojde připojením záporného potenciálu (0 V nebo též `GND`) napětí z tohoto externího zařízení. Konkrétně jsou tedy do vstupů `I1` až `I4` zapojeny výstupy EZS ústředny `PGM1` až `PGM4` a do vstupu `Ucc` pak napájecí napětí ústředny (odebírané ze svorky `AUX +`).

Horní straně automatizačního modulu vévodí 8 releových NO / NC výstupů zatížitelných maximálně proudem 5 A při napětí 60 V. Pro zapínání systému EZS je využito `RELÉ 1`, jehož výstupy jsou v ústředně zapojeny jako zóna `Keyswitch-tlačítko` (viz. kapitola 7.1.5). Výstup `RELÉ 2` je určen pro ovládání osvětlení květin, jak bylo požadováno ve specifikaci (kapitola 5). Konkrétním návrhem osvětlení se již tato práce nezabývá. Realizováno by mohlo být např. pomocí spínací jednotky a sérií zářivek.

7.3.1 Síťové nastavení pomocí programu SpringSet

Pro nastavení modulu `SpringNET CP-1` pro počítačovou síť slouží program `SpringSet`, jehož hlavní okno je znázorněno na obrázku 7.11.



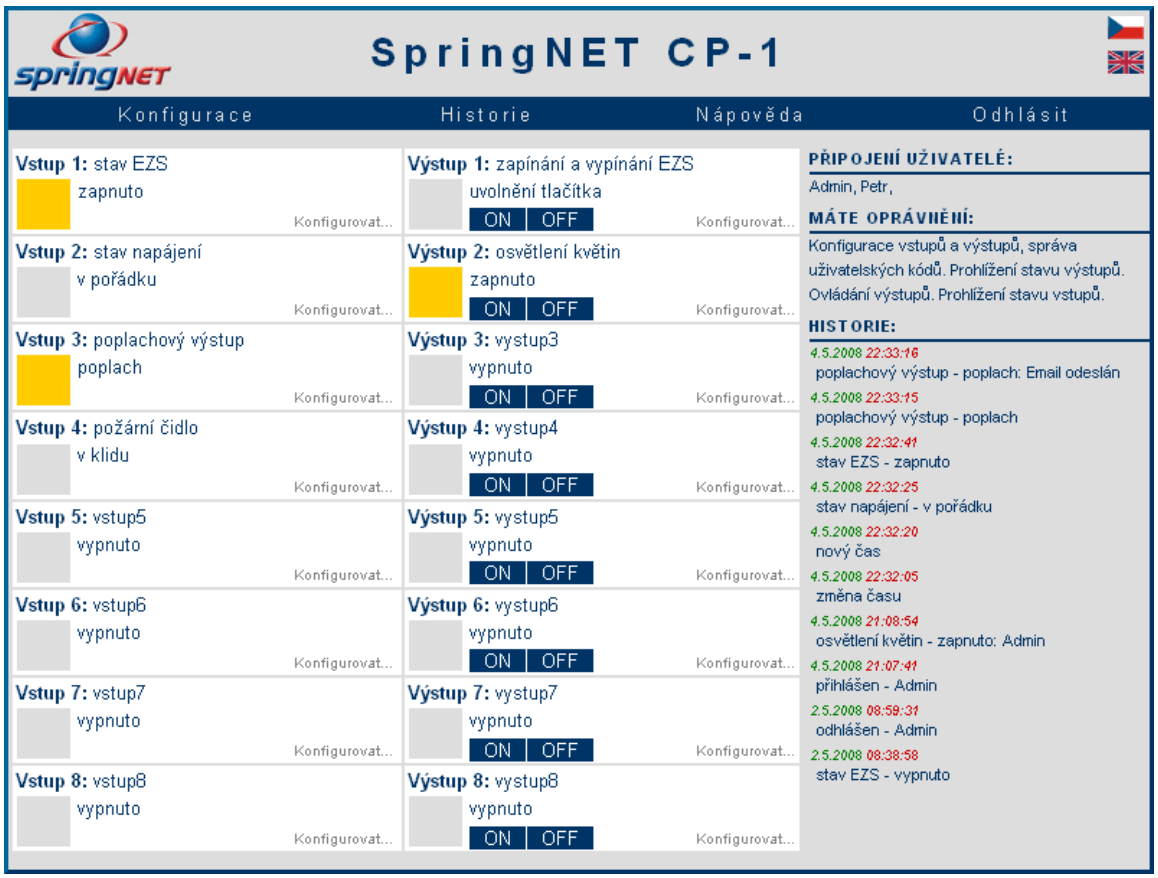
Obrázek 7.11: Konfigurace pomocí programu SpringSet

Pro vyhledání automatizačního modulu v síti slouží tlačítka `[Vyhledat podle IP]` nebo `[Vyhledat podle MAC]`. `IP adresa` je z výroby nastavena na hodnotu `192.168.1.254` a `MAC adresa` konkrétního zařízení je uvedena na síťovém konektoru (viz. obr. 7.10).

Ve sloupečku „**Síťové nastavení zařízení**“ lze měnit *jméno zařízení*, *port* na kterém bude modul dostupný, *IP adresu*, *masku podsítě*, *výchozí bránu* a *adresu SMTP serveru* pro odesílání e-mailů. Adresa, která bude uvedena jako odesílatel e-mailu se zadává do políčka „*Odesílající email (From)*“. Sloupeček „**Nastavení administrátora**“ slouží pro definici *jména a hesla administrátora*, *adresy* pro zasílání e-mailů (při událostech na vstupech) a *hesla* pro program `SpringSet` (zamezení změn nastavení neoprávněnou osobou-útočníkem). Provedené změny budou do zařízení odeslány po stisku tlačítka `[Nastavit]`. Automatizační modul použitý v našem systému je nakonfigurován přesně jako je zachyceno na obrázku 7.11.

7.3.2 Konfigurace a ovládání přes webové rozhraní

Veškerá další konfigurace a uživatelské ovládání potom probíhá přes webové rozhraní. Automatizační modul je v lokální síti dostupný na adrese `http://192.168.1.254:80`. Po zadání *uživatelského jména* a *hesla* se načte stránka podobná obr. 7.12.

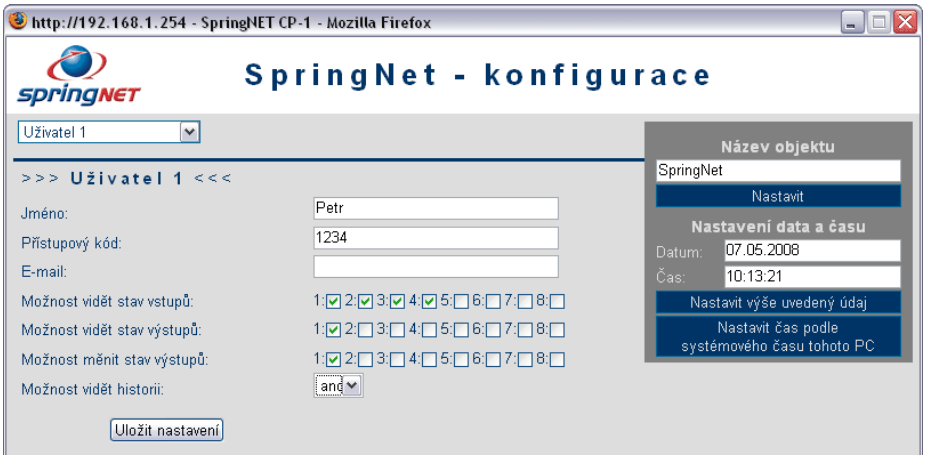


Obrázek 7.12: SpringNET CP-1 – webové rozhraní

V levém sloupečku jsou pod sebou přehledně zobrazeny *vstupy*. Podle jejich aktuálního stavu se mění jejich popis a barva (aktivní jsou označeny žlutě). Ve sloupečku uprostřed okna jsou pod sebou seřazeny *výstupy*. Opět s barevným označením a popisem odpovídajícím aktuálnímu stavu. Jednotlivé výstupy lze přímo ovládat pomocí tlačítek `[ON]` a `[OFF]`. U každého ze vstupů i výstupů jsou navíc dostupné položky `[Konfigurovat...]`, umožňující nejrůznější nastavení (bude popsáno dále). V pravé části se zobrazují jména *aktuálně přihlášených uživatelů*, výčet *oprávnění* jež má uživatel prohlížející toto okno a 10 posledních záznamů z historie. Všech 1 000 položek *historie* se zobrazí po kliknutí na tlačítko `[Historie]` v horním menu. Zde jsou dále tlačítka `[Odhlásit]`, `[Nápověda]` a `[Konfigurace]`.

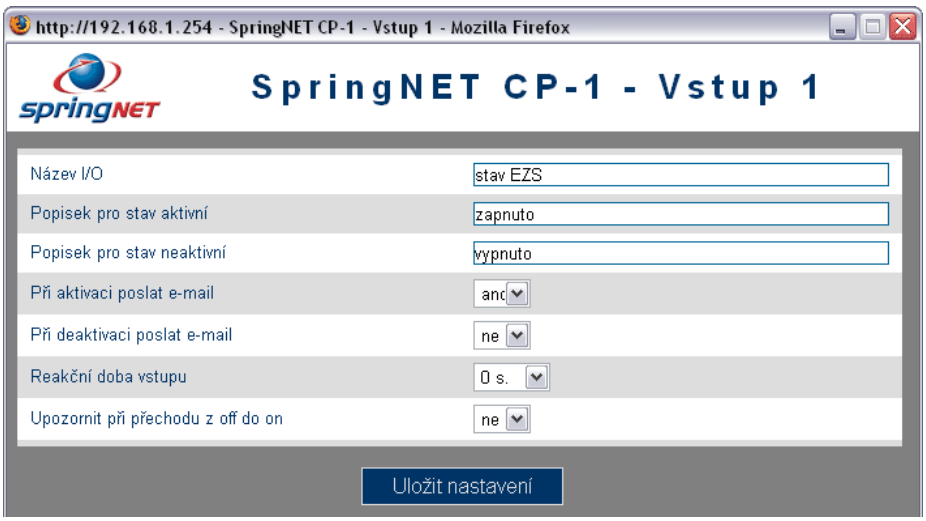
Po kliknutí na tlačítko `[Konfigurace]` se zobrazí okno, ve kterém je možné definovat až *8 uživatelských účtů*, měnit název modulu a datum a čas. Tato nastavení může provádět pouze „Administrator“, jehož přihlašovací jméno a heslo bylo definováno pomocí programu `SpringSet`. Vzhled konfiguračního okna je znázorněn na obrázku 7.13. Pomocí nabídky

vlevo se zvolí jeden z osmi uživatelů, pro nějž se budou definovat změny. Každému je možné přiřadit libovolné *přihlašovací jméno a heslo*, určit u kterých vstupů a výstupů uvidí jejich stav a které výstupy bude moci ovládat. Toto nastavení se realizuje pomocí zatrhávacích políček. Pokud bude vyplněno políčko „E-mail“, budou uživateli zasílány e-maily při aktivaci nebo deaktivaci vstupů, u nichž má právo vidět jejich stav. Pravidla pro odesílání e-mailů platí globálně pro všechny uživatele a nastavují se pro každý vstup zvlášť.



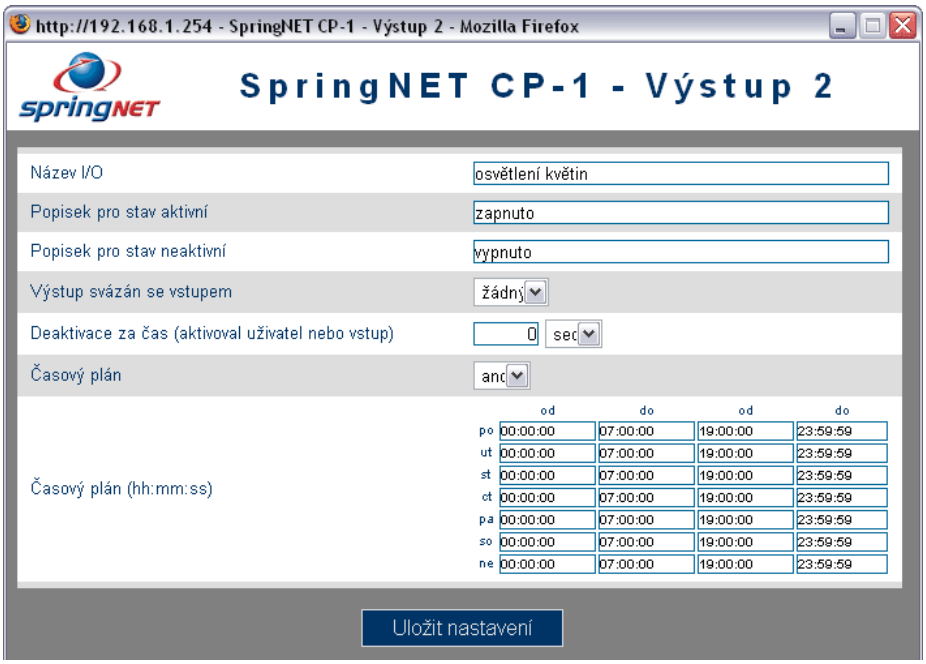
Obrázek 7.13: SpringNET CP-1 – konfigurace

Nastavení jednotlivých vstupů se provádí na stránce zobrazené po stisknutí tlačítka `[Konfigurovat...]` v hlavním okně (obr. 7.12) u konkrétního vstupu. Vzhled okna pro konfiguraci vybraného vstupu (v tomto případě `Vstupu 1` určujícího stav systému EZS) je znázorněn na obrázku 7.14. Je zde možné provést jeho pojmenování a určit popisky pro aktivní a neaktivní stav. Dále lze definovat reakční dobu (od 0 do 255 s) a to zda mají být při aktivaci nebo deaktivaci odesílány e-maily.



Obrázek 7.14: SpringNET CP-1 – nastavení vstupu

Pro nastavování výstupů slouží opět tlačítko `[Konfigurovat...]`. Vzhled okna pro konfiguraci konkrétního výstupu (v tomto případě `Výstupu 2` použitého pro ovládání osvětlení květin) je znázorněn na obrázku 7.15.



Obrázek 7.15: SpringNET CP-1 – nastavení výstupu, časový plán

Opět je zde možné provést jeho pojmenování a určit popisky pro aktivní a neaktivní stav. Zajímavá je položka „Deaktivace za čas“, jejíž hodnotu lze stanovit v rozmezí 0 sekund až 255 hodin. V našem případě bude pro `Výstup 1` (určený pro zapínání/vypínání systému EZS) nastavena na 2 s. Tímto bude „simulován stisk tlačítka“ (viz. kapitola 7.1.5). Dále je možné volbou „Výstup svázán ze vstupem“ stanovit závislost výstupu na kterýmkoli vstupu a díky tomu realizovat nejrůznější požadavky. Poslední položkou je „Časový plán“, ve kterém lze pro jednotlivé dny v týdnu určit 2 časy automatického zapnutí a vypnutí výstupu. Časový plán `Výstupu 2` bude nastaven dle obr.7.15 a poslouží pro ovládání osvětlení květin.

7.3.3 Způsob použití při ovládání EZS

Následuje krátký popis možností ovládání systému EZS a osvětlení květin pomocí webového rozhraní (obr. 7.12) automatizačního modulu `SpringNET CP-1`.

Zapnutí/vypnutí EZS

- K zapnutí nebo vypnutí systému EZS dojde po stisku tlačítka `[ON]` u položky „**Výstup 1: zapínání a vypínání EZS**“. Tento výstup je nastaven tak, aby došlo ke krátkému pulsu (2 s) `RELÉ 1` připojeného do ústředny EZS jako zóna `Keyswitch-tlačítko`. Automatizační modul tedy simuluje „stisk tlačítka `Keyswitch`“ na dobu 2 s. Při každé aktivaci výstupu (tlačítkem `[ON]`) dojde ke změně předchozího stavu zabezpečovacího systému (zapnuto, vypnuto, zapnuto, ...).

Stav EZS, porucha napájení, poplach, požární poplach

- **Vstup 1: stav EZS**:
  Zapnutí je signalizováno žlutou barvou, popisem „*zapnuto*“ a odesláním e-mailu ve tvaru: „*4.5.2008 12:00:00, stav EZS - zapnuto*“. Vypnutí šedou barvou, popisem „*vypnuto*“ a odesláním e-mailu „*4.5.2008 12:00:00, stav EZS - vypnuto*“.
- **Vstup 2: stav napájení**:
  Porucha je signalizována žlutou barvou, popisem „*zapnuto*“ a odesláním e-mailu ve tvaru: „*4.5.2008 12:00:00, stav napájení - výpadek*“. Normální stav je signalizován šedou barvou a popisem „*v pořádku*“.
- **Vstup 3: poplachový výstup**:
  Poplach v systému EZS je signalizován žlutou barvou, popisem „*poplach*“ a odesláním e-mailu ve tvaru: „*4.5.2008 12:00:00, poplachový výstup - poplach*“. Klidový stav je signalizován šedou barvou a popisem „*v klidu*“.
- **Vstup 4: požární čidlo**:
  Požární poplach je signalizován žlutou barvou, popisem „*požár*“ a odesláním e-mailu ve tvaru: „*4.5.2008 12:00:00, požární čidlo - požár*“. Klidový stav je signalizován šedou barvou a popisem „*v klidu*“.

Historie

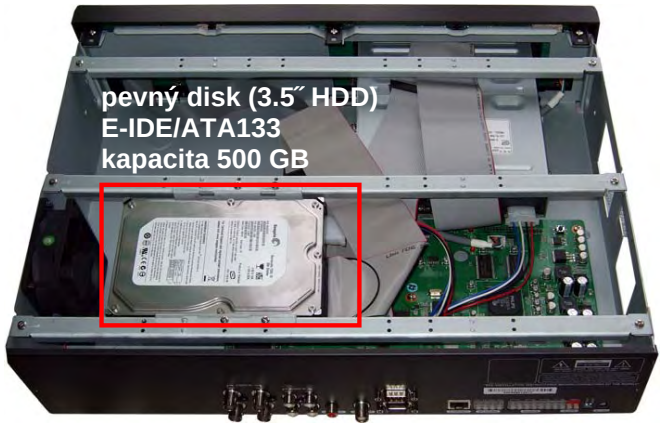
Všechny události jsou v automatizačním modulu zaznamenávány do historie čítající 1 000 položek. Prohlížet ji mohou jen uživatelé s příslušným oprávněním. Ukázka stránky s historií je na obrázku 7.16.

Obrázek 7.16: SpringNET CP-1 – historie

7.4 Kamerový systém

K realizaci kamerového systému je dle návrhu z kapitoly 6.4 použit digitální videorekordér `Nadatel SDVR-4500C`, tři barevné kamery `Avideo ACC-90X` a AV modulátor `MD-5s`. Zapojení všech těchto komponent je provedeno víceméně podle obr. 6.6 a odpovídá tomu, co bylo popsáno v návrhu.

Před uvedením videorekordéru `Nadatel SDVR-4500C` do provozu je třeba do něj instalovat pevný disk. V našem případě je použit 3.5″ HDD s kapacitou 500 GB, jež poskytuje dostatek prostoru pro splnění požadavku archivace záznamu po dobu alespoň třiceti dnů. Způsob instalace pevného disku je patrný z obr. 7.17.



Obrázek 7.17: Instalace HDD do videorekordéru

Veškerá konfigurace videorekordéru se provádí prostřednictvím menu zobrazeného na připojeném televizoru nebo VGA monitoru. K ovládání lze využít buďto tlačítka na předním panelu, nebo dálkový ovladač (viz. obr. 7.18). Možností nastavení je velice mnoho a jsou podrobně popsány v manuálu [9]. Pro účely našeho systému postačí pouze pro všechny tři kamery definovat následující parametry záznamu[3]:

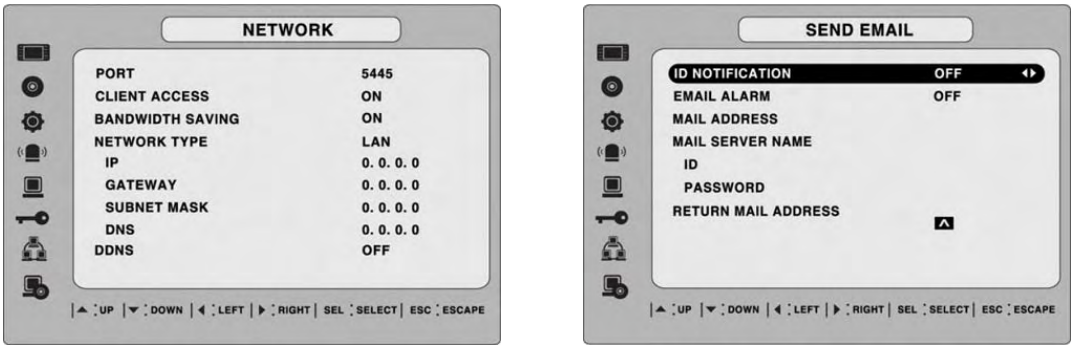
- Rozlišení obrazu 704x576 (PAL)
- Frekvence snímání 8 snímků za sekundu
- Kvalita komprese „high“

Obrázek 7.18: Nadatel SDVR-4500C a dálkový ovladač

[3]Při tomto nastavení se na použitý HDD vejde až 40 dnů nepřetržitého záznamu ze všech tří kamer.

7.4.1 Síťová nastavení a odesílání e-mailů

Pro přístup k videorekordéru přes počítačovou síť je potřeba nejdříve nastavit síťové parametry. To se provádí v menu dostupném na monitoru po stisknutí tlačítka `[SETUP]`. Konkrétně na záložce `NETWORK` zobrazené na obr. 7.19 vlevo.



Obrázek 7.19: Menu pro nastavení parametrů sítě a zasílání e-mailů

Zde je možné definovat:

Port: Udává číslo portu, na kterém bude videorekordér dostupný přes síťové rozhraní. Ponecháme defaultní hodnotu `5445`.

Client access: Pro povolení přístupu k videorekordéru přes síťové rozhraní je třeba nastavit na `ON`.

Bandwidth Saving: Umožňuje nastavit úsporný režim přenosu videa po síti (sníží se snímkovací frekvence). Toto je užitečné zvláště při spojení přes Internet, máme-li pomalou linku. Nastavíme na hodnotu `ON`.

Network type: Nastavení síťových parametrů (*IP adresa, maska podsítě, výchozí brána, DNS server*). Dostupné volby jsou `LAN` (parametry potřeba nastavit ručně viz. obr. 7.19 vlevo), `ADSL` a `DHCP`. Jelikož bude použit síťový router s DHCP serverem (konfigurace viz. kapitola 7.5), zvolíme možnost `DHCP` pro automatické nastavení.

DDNS: „Dynamic DNS“ umožňuje přístup přes Internet i v případě připojení s *dynamicky se měnící IP adresou*. Pro náš případ toto není uvažováno, proto nastavíme `OFF`.

Videorekordér nabízí možnost zasílat krátké informační e-maily při jeho zapnutí a při detekci pohybu v příslušném prostoru. Potřebné údaje se nastavují v menu `SYSTEM` v položce `SEND EMAIL` (viz. obr. 7.19 vpravo).

Dostupné jsou následující položky:

Mail address: Sem se zadává e-mailová adresa, na níž bude videorekordér zasílat e-maily.

Return mail address: V této položce se definuje e-mailová adresa, která bude uvedena jako odesílatel (v našem případě tedy `dvr@dvr.cz`). Budou na ni rovněž vraceny případné nedoručené e-maily.

ID notification: Při volbě `ON` bude videorekordér každý den posílat e-mail obsahující informace o nastavení sítě zhruba v následující podobě:

```
From: dvr@dvr.cz
To: petan85@volny.cz
Subject: [DOMA] IP Notify (mac address 00:02:69:01:34:17)

IP Address : 192.168.1.250
Gateway : 192.168.1.1
Subnet  : 255.255.255.0
```

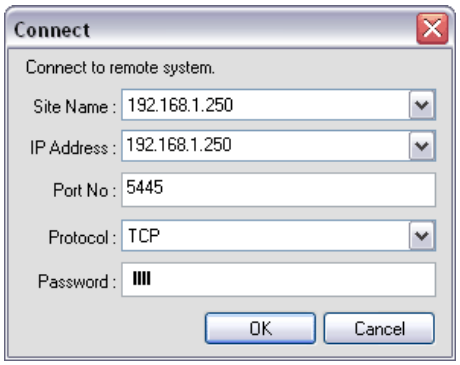
Email alarm: Při nastavení na `ON` dojde při detekci pohybu v určeném video-kanálu k odeslání e-mailu. Pro daný video-kanál musí být nastaveny parametry detekce a povolena aktivace alarmového výstupu. Odesílaný e-mail obsahuje v příloze statický snímek zachycující událost, jež způsobila poplach a má následující podobu:
(Z řádku `Motion detected CH[1]` *je patrné, že došlo k detekci pohybu ve video-kanálu 1. Na snímku v příloze by tato událost byla zachycena. Ukázky odesílaných e-mailů jsou uloženy na datovém nosiči přiloženém k této práci.)*

```
From: dvr@dvr.cz
To: petan85@volny.cz
Subject: Alarm occurred

Motion detected CH[1]
DVR ID : DOMA
IP Address : 192.168.1.250
```

7.4.2 Přístup a ovládání přes LAN/Internet

Pro přístup k videorekordéru přes počítačovou síť LAN nebo přes Internet je možno využít dodávaný software `Network Client`. Aby bylo možné se připojit ke konkrétnímu zařízení, je třeba znát jeho IP adresu, číslo portu a uživatelské heslo. V našem případě je použita IP adresa `192.168.1.250`, port číslo `5445` a defaultní heslo `0000`.



Obrázek 7.20: Dialog "Connect" programu Network Client

Hlavní okno programu `Network Client` vypadá po připojení obdobně jako na obrázku 7.21. Program umožňuje provádět následující činnosti:

Živé prohlížení: V tomto režimu lze sledovat aktuální dění snímané kamerami. Mezi jednotlivými kanály je možné ručně či automaticky (sekvenčně s definovanou dobou) přepínat, nebo je zobrazit všechny najednou v tzv. „quad zobrazení“. Pomocí tlačítek `[PT]` (pan/tilt), `[ZF]` (zoom/focus) a přilehlých směrových ikonek je možné ovládat pohyb PTZ kamer (jsou-li připojeny).

Vyhledávání a přehrávání uloženého záznamu: Po klepnutí na tlačítko `Search` se program přepne do režimu, ve kterém je podle přehledného kalendáře umožněno vyhledávání a přehrávání uloženého záznamu.

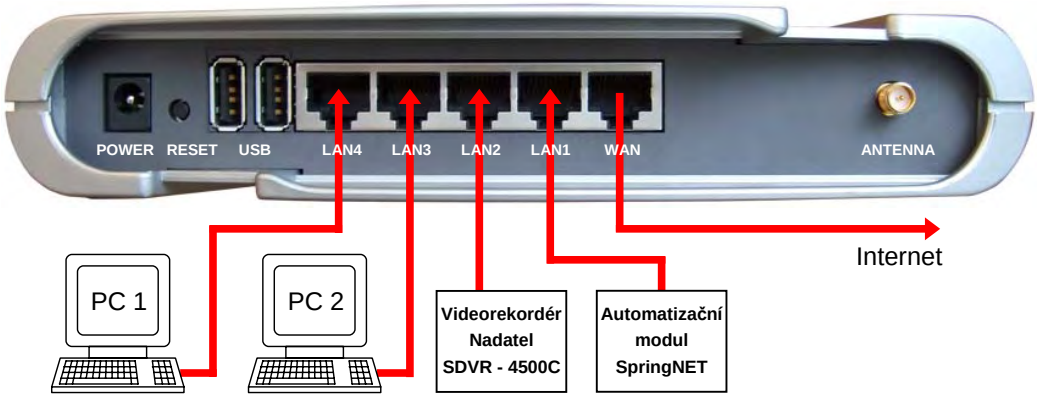
Záloha videa a statických snímků do počítače: V obou výše zmíněných režimech je možné ukládat statické snímky a záznam videa z videorekordéru do počítače. Snímky se ukládají pomocí tlačítka `Capture`, videozáznam při „živém sledování“ tlačítkem `Rcord`. Pro zálohu videozáznam v režimu „vyhledávání a přehrávání“ je nejprve nutné vymezit požadovaný úsek a poté jej lze nahrát pomocí tlačítka `Bacup`.

Kompletní popis ovládání a možností využití klientského software `Network Client` v kombinaci s digitálním videorekordérem `Nadatel SDVR-4500C` lze nalézt v manuálu [9].

Obrázek 7.21: Režim živého prohlížení v programu Network Client

7.5 Počítačová síť

V realizovaném systému je požadavek propojení automatizačního modulu `SpringNET CP-1` a videorekordéru `Nadatel SDVR-4500C` do místní počítačové sítě a Internetu. K tomuto účelu poslouží (dle návrhu. z kapitoly 6.5) router `ASUS WL-500g Deluxe`. Způsob jeho zapojení a příklad propojení s jednotlivými síťovými prvky (počítače, automatizační modul, videorekordér) je znázorněn na obrázku 7.22.



Obrázek 7.22: Možné zapojení zařízení do počítačové sítě LAN

Síťové kabely vedoucí od zmiňovaných zařízení se zapojí do konektorů `LAN1` – `LAN4`. Jejich počet je možné v případě potřeby rozšířit použitím *síťového přepínače*, nebo-li *switche*. Připojení lze realizovat i bezdrátově pomocí technologie `WiFi`. Konektor označený jako `WAN` poslouží pro připojení k Internetu.

Způsobů připojení k Internetu je velmi mnoho a touto problematikou se práce dále nezabývá. Při realizaci navrhnutého systému se počítá s již zavedeným a funkčním připojením. Pro splnění podmínky přístupu do sítě odkudkoli z Internetu se předpokládá poskytovatelem přidělená veřejná statická IP adresa.

7.5.1 Nastavení routeru (DHCP, Virtual Server)

Pro požadovanou funkci je potřeba router nejdříve nakonfigurovat. To se provádí pomocí webového prohlížeče po zadání jeho IP adresy a následném přihlášení. IP adresa je továrně nastavena na `http://192.168.1.1` (lze použít i `http://my.router`), uživatelské jméno a heslo je `admin`. Vzhled konfiguračního webového rozhraní je zachycen na obrázku 7.23.

Pro potřeby realizace navrhnutého systému je třeba nastavit následující parametry:

Zařízení	MAC adresa	IP adresa	Port (lokální)	Port
`SpringNET`	`00204A8F6331`	`192.168.1.254`	`80`	`8080`
`Nadatel SDVR-4500C`	`000269013417`	`192.168.1.250`	`5445`	`5445`

Tabulka 7.1: Přehled síťových parametrů jednotlivých zařízení

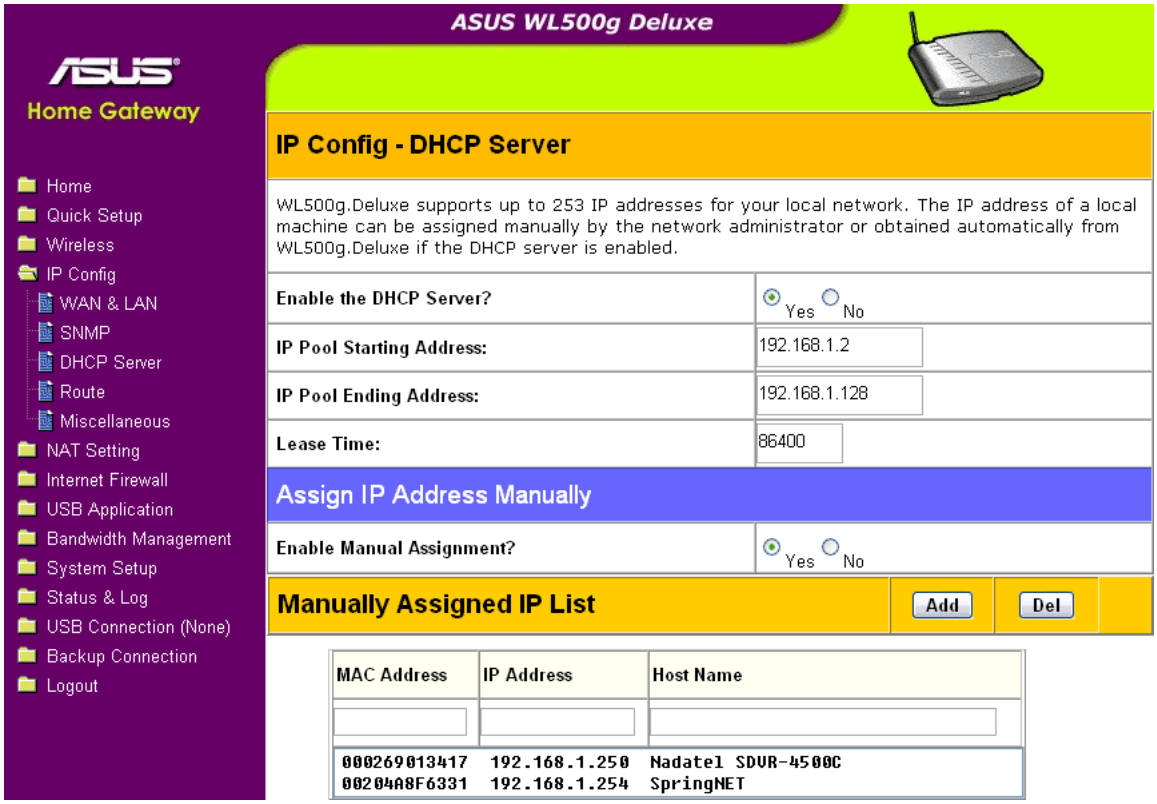
DHCP Server: Tato položka se nachází v menu `IP Config` (viz obr. 7.23) a slouží pro konfiguraci DHCP serveru. Zde je třeba zadat MAC adresy automatizačního modulu a videorekordéru a určit IP adresy, jež jim budou DHCP serverem přiděleny. Konkrétní hodnoty jsou uvedeny ve 2. a 3. sloupci tabulky 7.1.

Virtual Server: Tato položka se nachází v menu `NAT Setting` a slouží k tzv. „publikaci portů“. Pro každé lokální síťové zařízení (určené IP adresou a číslem portu) je třeba definovat číslo portu, na kterém bude dostupné při přístupu „zvenčí“ (odkudkoli mimo vnitřní síť LAN). Konkrétní zvolené hodnoty jsou uvedeny ve 3. – 5. sloupci tabulky 7.1.

Předpokládejme výše uvedená nastavení a připojení k Internetu s poskytovatelem přidělenou veřejnou IP adresou (např. `147.229.206.34`). Ovládací rozhraní automatizačního modulu `SpringNET CP-1` bude potom dostupné na adrese `http://147.229.206.34:8080`, a to z libovolného počítače připojeného kdekoli v Internetu. Přes uvedenou adresu se bude možné připojit i k videorekordéru `Nadatel SDVR-4500C`, ovšem na portu č. `5445`.

Kompletní popis všech možností nastavení a použití routeru `ASUS WL-500g Deluxe` lze nalézt v manuálu [6].

Provedená konfigurace byla uložena do souboru `WL500g.Deluxe.CFG`*, který je umístěn na datovém nosiči přiloženém k této práci. Nahrání do routeru je možné přes webové rozhraní. Pro zaručení funkčnosti je doporučená verze firmware* `1.9.2.7-10-USB-1.69`.



Obrázek 7.23: Webové konfigurační rozhraní routeru ASUS WL-500g Deluxe

Kapitola 8

Závěr

Návrh systému byl proveden s ohledem na požadavky stanovené v zadání a specifikaci systému. Požadavky na *nízký příkon* a na *snadnost instalace a případných změn struktury systému* byly splněny použitím bezdrátové nadstavby ústředny EZS. Každý bezdrátový detektor a periferie jsou napájeny vlastní baterií s maximální výdrží až několik roků. Z elektrické sítě je napájeno minimum komponent a celkový *příkon systému EZS je tak minimální*. Díky bezdrátovému přenosu mezi ústřednou a periferiemi lze tyto v případě potřeby kdykoli *snadno přemístit*. Rovněž *rozšíření systému je možné* pouhým přidáním dalšího bezdrátového prvku a jeho programovým nastavením v ústředně. Pro *zasílání uživatelem upřesněných informací* a pro možnost ovládání pomocí mobilního telefonu a přes Internet byla zařazena GSM brána a automatizační modul. Systém tak může zasláním SMS zprávy nebo e-mailu informovat uživatele o určitých situacích. Automatizační modul navíc obsahuje *historii* zaznamenávající až 1 000 posledních událostí, a to včetně jejich data a času. Střežení okolních prostor bylo realizováno pomocí infrazávory napojené na systém EZS. Dále byl zařazen samostatný *kamerový systém CCTV* se třemi barevnými kamerami a digitálním videorekordérem, schopným poměrně dlouhého záznamu. Aktuální dění i zaznamenané události je možné sledovat na libovolném televizoru, nebo přes Internet z libovolného počítače s nainstalovaným příslušným softwarem. Pro účely namodulování obrazu a zvuku do anténního systému byl použit AV modulátor. Jelikož jsou v systému použita zařízení se síťovým rozhraním a mají být dostupná z Internetu, byl proveden *návrh jednoduché domácí počítačové sítě*. Seznam všech použitých komponent včetně jejich cen a celkové finanční kalkulace systému je uveden v příloze B.

V podstatě téměř celý navržený *systém byl prakticky realizován*. To bylo zdokumentováno pomocí fotografií, jež se nachází v příloze A a na přiloženém datovém médiu. Oproti návrhu byla použita odlišná ústředna EZS a jiné typy detektorů. Namísto bezdrátové ústředny `PARADOX® Magellan MG-5050` byla tedy využita smyčková ústředna `PARADOX® ESPRIT 748`. Použití odlišných komponent pro praktické ověření bylo způsobeno tím, že jsem byl limitován dostupností potřebných prvků. Všechny komponenty mi byly zapůjčeny instalační firmou, avšak u některých se jednalo o jiné typy, než jsou použity v návrhu. To ovšem nevadí, protože princip zapojení a konfigurace zůstal obdobný. Ostatní prvky (GSM brána, automatizační modul, kamery, atd.) byly použity shodně s návrhem.

Pro demonstraci funkcí realizovaného systému zabezpečení a střežení byla natočena krátká, asi patnáctiminutová *video prezentace*. Ta je umístěna na přiloženém datovém médiu. Digitální videorekordér a kamery jsem musel bohužel během tvorby práce vrátit a

jejich demonstraci jsem tak již do videozáznamu nemohl zařadit. Kamerový systém je tedy zdokumentován pouze pomocí fotografií.

Za vlastní a inovativní přínos v tomto směru považuji sestavení komplexního systému z poměrně *různorodých komponent*. K možnostem zabezpečovacího systému díky tomu přibyly mnohé další. Byl obohacen o možnost ovládání (a zpětné vazby k uživateli) pomocí GSM sítě a Internetu. Díky schopnosti ovládání na dálku se tak *zvýšila jeho celková užitná hodnota* a komfort při obsluze. Jako „třešnička na dortu“ přibyla možnost sledovat aktuální i zaznamenané dění v objektu přes Internet a pomocí automatizačního modulu ovládat kromě systému EZS i další libovolná zařízení. Toto už ovšem není předmětem této práce.

Možnosti návrhu zabezpečovacího systému byly poměrně vyčerpány. Vždy se v podstatě jedná jen o vhodné použití a nakonfigurování dostupných komponent. Vymýšlet a programovat si vlastní nemá pravděpodobně přílišný smysl. To by bylo nutné asi jen v případě potřeby uspokojit určité dosti specifické požadavky. Jak bylo při tvorbě této práce zjištěno, běžně kladené nároky totiž uspokojí drtivá většina zařízení dostupných na trhu. Možný další vývoj by se tedy měl dle mého názoru ubírat spíše směrem automatizace a řízení domácnosti na dálku. Zhruba tak, jak bylo naznačeno u ovládání osvětlení květin. Zde se nabízí velice zajímavá myšlenka realizace tzv. „*inteligentního domu*“. Jednalo by se o centrální jednotku, pomocí níž by bylo možné *lokálně a na dálku ovládat nejrůznější spotřebiče v objektu*. Možná se právě toto stane námětem pro moji diplomovou práci.

Literatura

[1] *ČSN EN 50131-1/Z1: Poplachové systémy – Elektrické zabezpečovací systémy – Všeobecné požadavky.* Praha: Český normalizační institut, 2000, 86 s.

[2] BURDA, K.: *Čidla EZS.* 2007, [online], [cit. 2008-04-17].
URL
<http://adela.utko.feec.vutbr.cz/mzsy/prednaska/03_Cidla%20EZS.pdf>

[3] DUDÁČEK, A.: *Požárně bezpečnostní zařízení (EPS).* Vysoká škola báňská-Technická univerzita Ostrava, 1996, 53 s., skripta VŠB-TUO, ISBN 80-7078-312-5.

[4] EUROSAT cs: *Uživatelský manuál VT-GSM-10.* [online], [cit. 2008-04-25].
URL <http://www.eurosat.cz/UserFiles/Manual/Ostatni/GSM_brany/Navody/gsm-vt-10.pdf>

[5] HW.cz: Přenos dat po linkách RS485 a RS422 – HW.cz: Vše o elektronice a programování. [online], 2008, [rev. 1999-08-25], [cit. 2008-04-12].
URL <http://hw.cz/Teorie-a-praxe/Dokumentace/ART705-Prenos-dat-po-linkach-RS485-a-RS422>

[6] Joice: *Uživatelská příručka – ASUS WL-500b / WL-500g / WL-500g Deluxe, bezdrátový router pro sítě 802.11b/g.* 2005, [online], Verze v106CZ, [cit. 2008-05-10].
URL <http://www.joyce.cz/f/joyce/p/download/technicka_podpora/asus_wl-500_manual_cz.pdf>

[7] KŘEČEK, S.; a kolektiv: *Příručka zabezpečovací techniky.* Cricetus, 2002, iSBN 80-902938-2-4.

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

[9] Nadatel: *SDVR-4500C User's Guide – 4 Channel MPEG-4 Digital Video Recorder.* [online], Verze 2.2, [cit. 2008-04-27].
URL <http://www.nadatel.com/nadatel/main/open_download_3_ENG.asp?code=P20081212246&mode=3>

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

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

[12] VARIANT: Magellan MG-5050 – VARIANT plus, bezpečnostní systémy. [online], 2008, [cit. 2008-04-16].
URL <http://www.variant.cz/index.php4?product=2150>

[13] VARIANT plus: *Instalační manuál DIGIPLEX DGP 48*. [online], Verze 3.00, [cit. 2008-04-01].
URL <http://www.variant.cz/src/get.php4?id=/DATA/DGP%2048%20ver.%203,xx%20-%20IM.pdf>

[14] VARIANT plus: *Instalační manuál Magellan a Spectra SP*. [online], Verze 2.40, [cit. 2008-04-30].
URL <http://www.variant.cz/src/get.php4?id=/DATA/MG%20a%20SP%20v2.40%20-%20IM-b.pdf>

[15] VARIANT plus: *Instalační manuál SpringNET – Univerzální modul automatizace a dálkové správy objektů*. [online], [cit. 2008-04-25].
URL <http://www.variant.cz/src/get.php4?id=/DATA/SpringNET%20-%20man-a5.pdf>

[16] VARIANT plus: *Rychlé programování Magellan a Spectra SP*. [online], Verze 2.40, [cit. 2008-05-02].
URL <http://www.variant.cz/src/get.php4?id=/DATA/MG%20a%20SP%20v2.40%20-%20RP-b.pdf>

[17] Wikipedia: Closed-circuit television – Wikipedia, The Free Encyclopedia. [online], 2008, [rev. 2008-04-10], [cit. 2008-04-11].
URL <http://en.wikipedia.org/w/index.php?title=Closed-circuit_television&oldid=204797443>

[18] Wikipedia: Digital video recorder – Wikipedia, The Free Encyclopedia. [online], 2008, [rev. 2008-04-10], [cit. 2008-04-12].
URL <http://en.wikipedia.org/w/index.php?title=Digital_video_recorder&oldid=204660557>

[19] Wikipedia: Moving Picture Experts Group – Wikipedia, The Free Encyclopedia. [online], 2008, [rev. 2008-04-07], [cit. 2008-04-12].
URL <http://en.wikipedia.org/w/index.php?title=Moving_Picture_Experts_Group&oldid=203945655>

[20] Wikipedie: Fresnelova čočka – Wikipedie: Otevřená encyklopedie. [online], 2007, [rev. 2007-12-27], [cit. 2008-04-18].
URL <http://cs.wikipedia.org/w/index.php?title=Fresnelova_%C4%8Do%C4%8Dka&oldid=2099704>

[21] Wikipedie: CCD – Wikipedie: Otevřená encyklopedie. [online], 2008, [rev. 2008-01-29], [cit. 2008-04-11].
URL <http://cs.wikipedia.org/w/index.php?title=CCD&oldid=2200722>

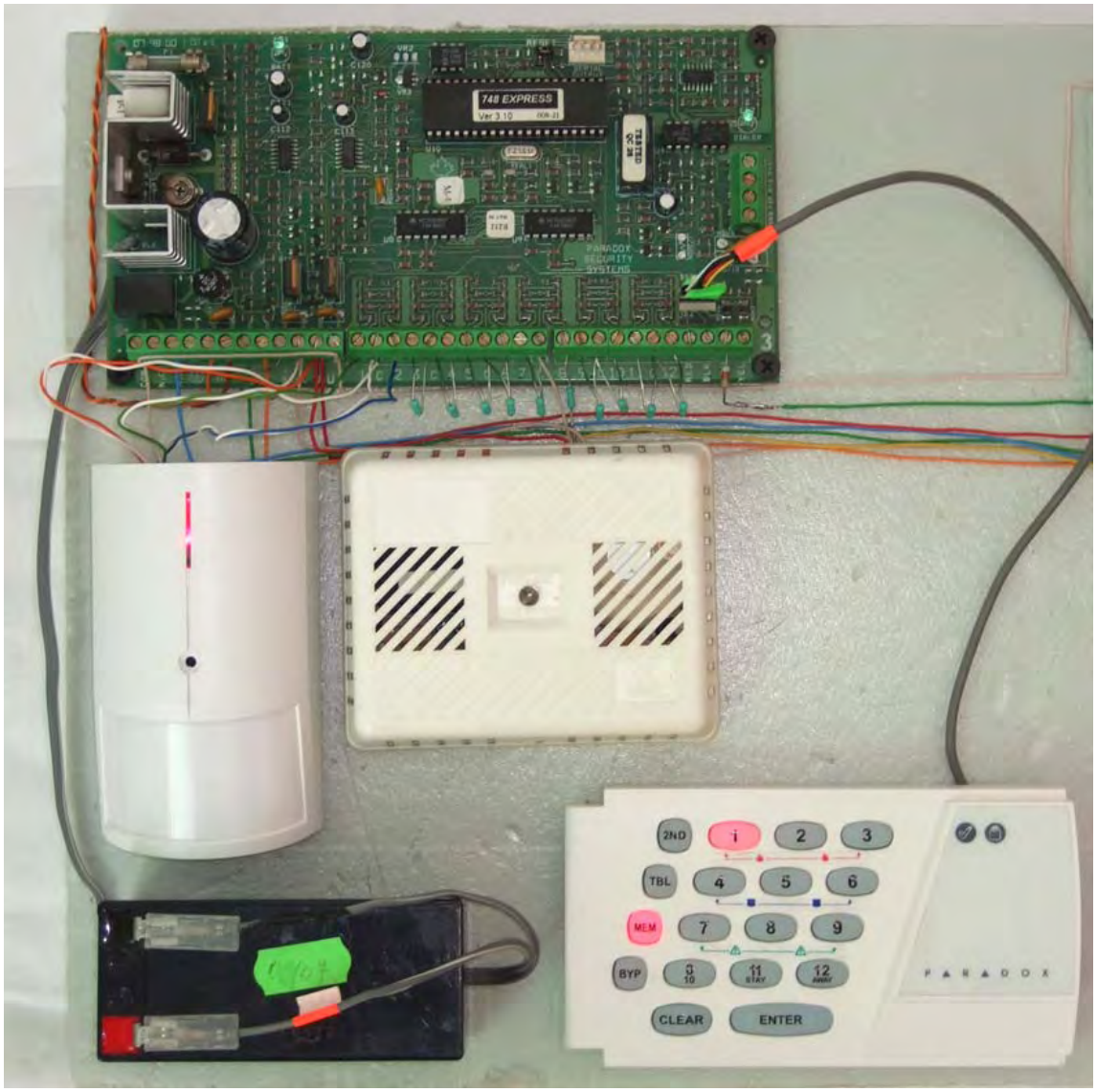
[22] ZAHRÁDKA, J.: *Začínáme s EZS*. 2005, [online], [cit. 2008-04-03].
URL
<http://www.variant.cz/src/get.php4?id=/DATA/Zaciname%20s%20EZS.pdf>

Seznam příloh

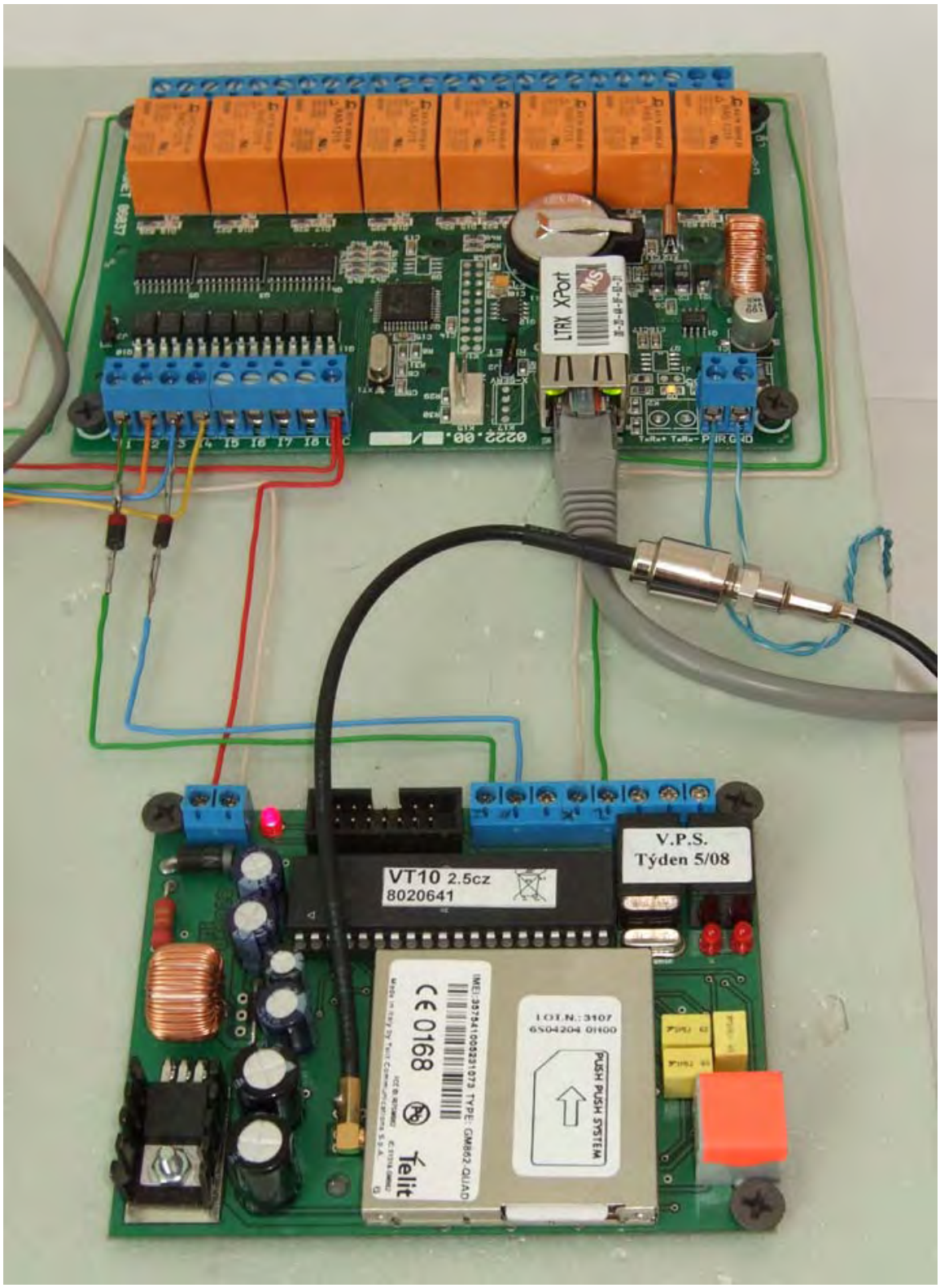
Příloha 1 - Fotodokumentace realizovaného systému
Příloha 2 - Finanční kalkulace navrženého systému
Příloha 3 - Adresářová struktura a obsah přiloženého CD

Dodatek A

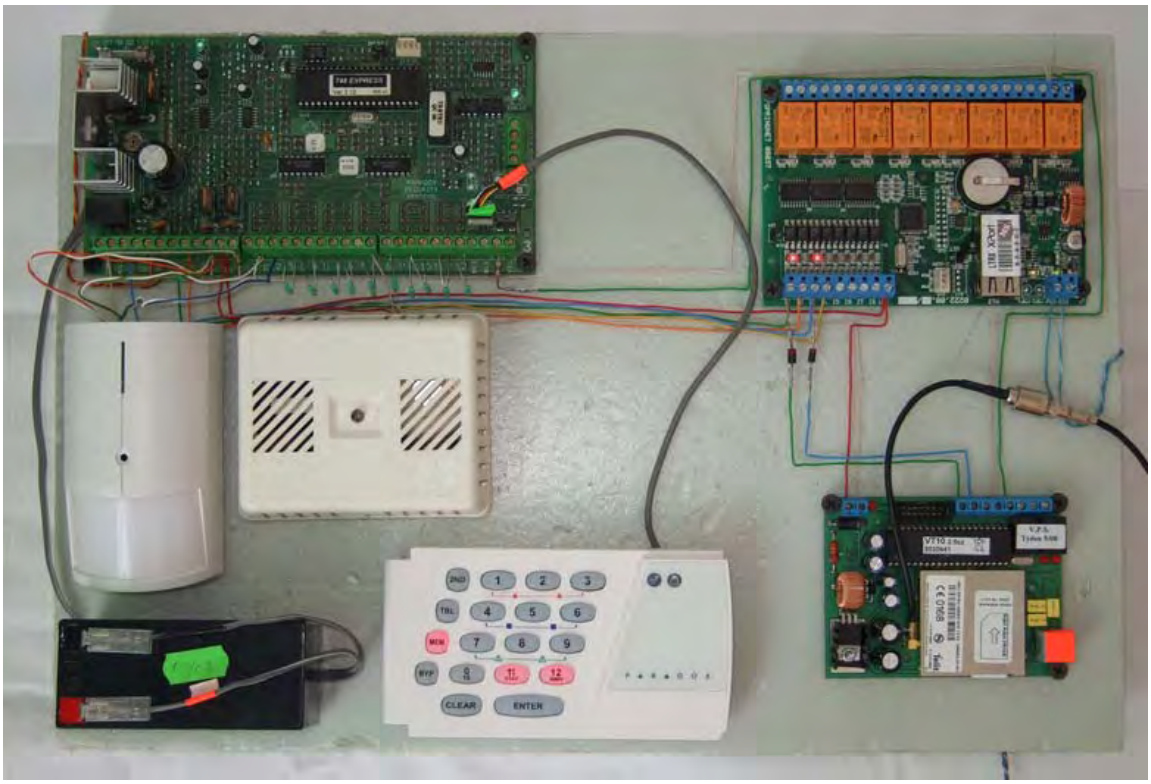
Příloha 1 - Fotodokumentace



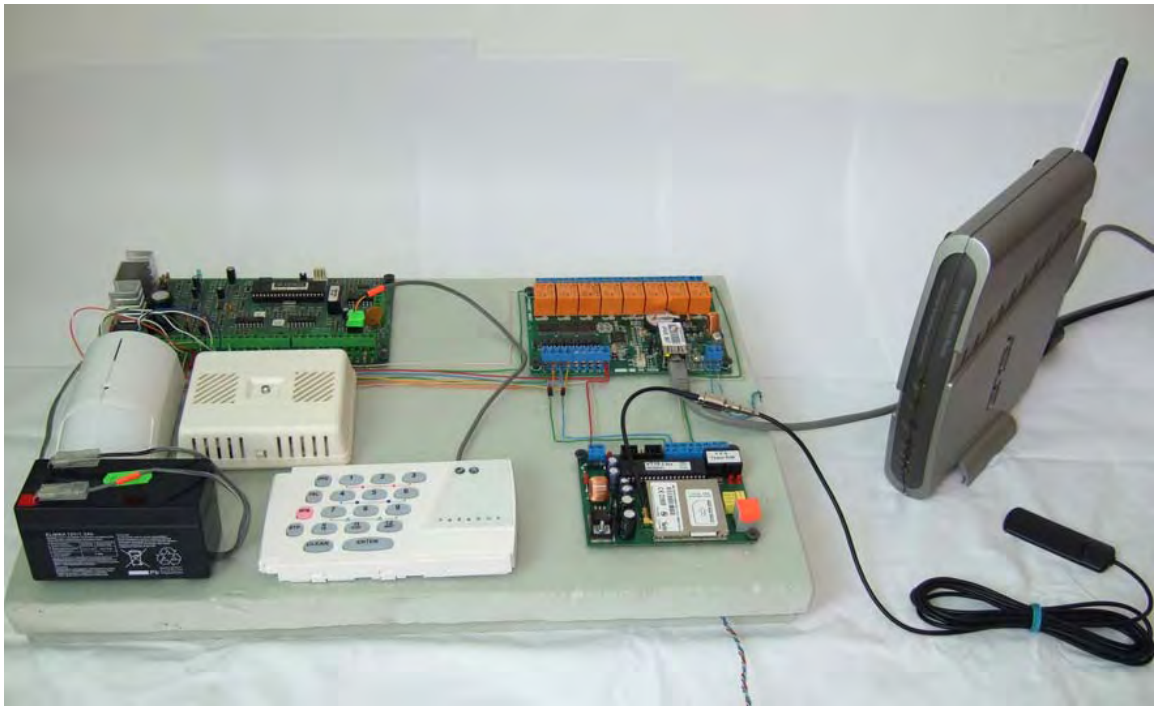
Obrázek A.1: Hlavní prvky Elektronického Zabezpečovacího Systému (EZS)



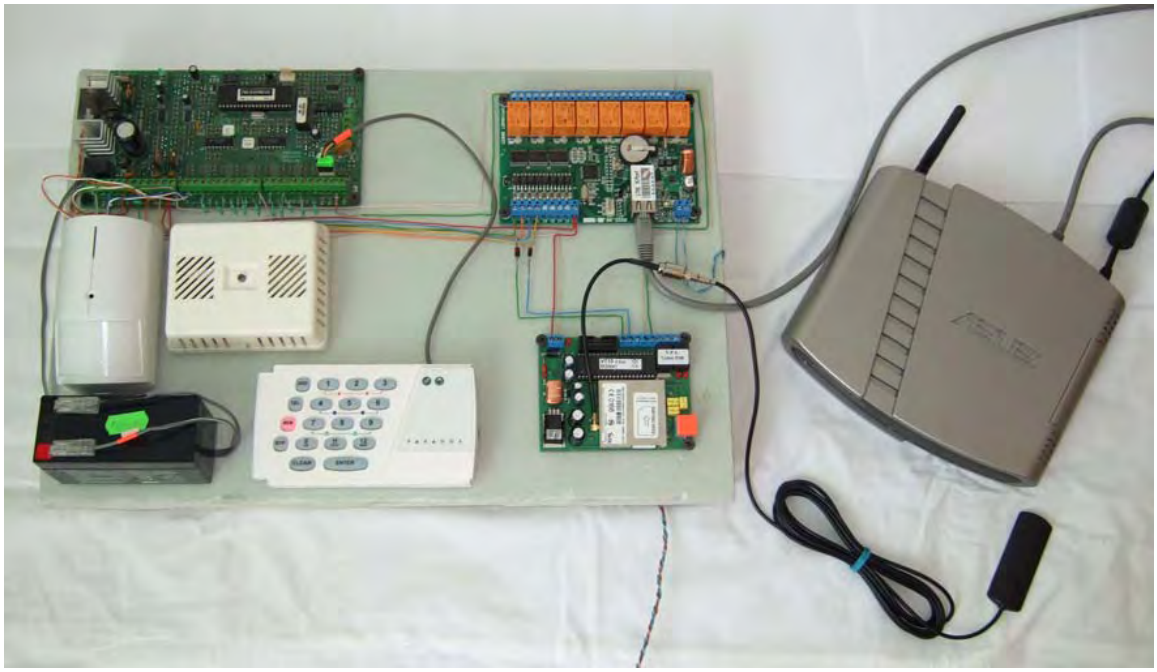
Obrázek A.2: Automatizační modul SpringNET CP-1 a GSM brána GSM-VT-10



Obrázek A.3: Celkový pohled na realizovaný systém



Obrázek A.4: Připojení systému do počítačové sítě pomocí routeru



Obrázek A.5: Připojení systému do počítačové sítě pomocí routeru

Obrázek A.6: Kompaktní provedení určené pro demonstrační účely

Obrázek A.7: Ukázka realizace kamerového systému

Obrázek A.8: Digitální videorekordér Nadatel SDVR-4500C

Dodatek B

Příloha 2 - Finanční kalkulace navrženého systému

Použitá komponenta	**Typ/model**	**Počet**	**Cena v Kč**
Automatizační modul	SpringNET CP-1	1	5 000
AV modulátor	MD-5s	1	1 900
Bezdrátová klávesnice	Magellan MG32LRF	1	2 500
Bezdrátová ústředna	Magellan MG-5050	1	4 500
Bezdrátový magnetický kontakt	MG-DCT2	1	1 100
Bezdrátový PIR detektor	MG-PMD1P	3	1 600
Bezdrátový požární detektor	MG-SD738	1	2 100
Detektor rozbití skla	Glasstrek 457	3	760
Digitální videorekordér 4 kanálový	Nadatel SDVR-4500C	1	15 900
GSM brána	GSM-VT-10	1	6 300
Napájecí zdroj	230 V/16 V, 50 Hz	1	500
Router	Asus WL-500g Deluxe	1	1 700
Venkovní barevná kamera	Avideo ACC-90X	3	4 900
Venkovní infrazávora	VAR-TEC TRIPLE PB-150	1	4 000
Venkovní zálohovaná siréna	TEKNIM-720WR	1	1 200
Zálohovací akumulátor	7 Ah	1	370
Cena v Kč celkem (včetně DPH):			**68 850**

Tabulka B.1: Finanční kalkulace navrženého systému

Dodatek C

Příloha 3 - Adresářová struktura a obsah přiloženého CD

Soubor/adresář	Popis
`CD_potisk.pdf`	Potisk CD ve formátu `*.pdf`
`README.txt`	Soubor s informacemi o adresářové struktuře CD
`\01_technicka_zprava`	Zdrojový kód v LaTeXu, použité obrázky v plném rozlišení
`\02_fotogalerie`	Fotodokumentace realizovaného systému a dílčích komponent
`\03_videogalerie`	Video prezentace realizovaného systému
`\04_ukazky_e-mailu`	Ukázky e-mailů odesílaných realizovaným systémem
`\05_konfigurace`	Soubory s konfigurací některých dílčích komponent systému
`\06_manualy`	Manuály (viz. Literatura) ve formátu `*.pdf`

Tabulka C.1: Adresářová struktura a obsah přiloženého CD