VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

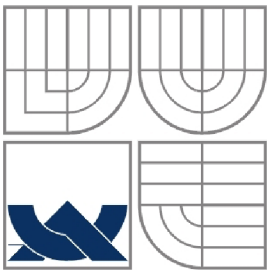
SYSTÉM PRO ZABEZPEČENÍ A STŘEŽENÍ OBJEKTŮ A PROSTOR

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

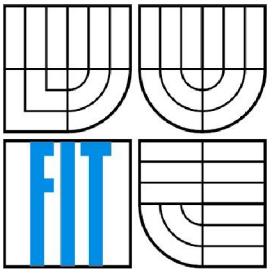
AUTOR PRÁCE
AUTHOR

Bc. DAVID KUCHAŘÍK

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

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. DAVID KUCHAŘÍK

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. JOSEF STRNADEL, Ph.D.

BRNO 2008

Abstrakt

Tento projekt se zabývá existujícími možnostmi zabezpečení, jak mechanickou tak elektronickou cestou. Jako objekt pro zabezpečení byl vybrán řadový rodinný dům se zahradou. Byly rozpracovány dva návrhy na zabezpečení a střežení tohoto objektu. Jeden ve formě kamerového systému a druhý v podobě klasického systému EZS. Bylo provedeno zhodnocení a vyzvednutí nejvýznamnější výhody jednotlivých návrhů. Na základě zadaných kritérií byl vybrán systém založený na ústředně a k ní připojených detektorech. Posléze byl vytvořen model vybraného systému, u kterého byla provedena simulace a verifikace požadovaného chování a nástin implementace v jazyce C.

Klíčová slova

Mechanický zábranný systém, MZS, elektronický zabezpečovací signalizace, EZS, čidlo, ústředna, infračervená čidla, mikrovlnná čidla, kamerový systém, rozšiřující karta, signalizační smyčka, sabotážní smyčka, model, Uppaal, Times Tool, časový automat, úkoly, chování, kanál, simulace, verifikace, analýza plánovatelnosti.

Abstract

This project deals with given safeguard possibilities, both mechanical and electronic. A row house with garden was chosen for being secured. Subsequently, were elaborated two`s proposals of securing and guarding of this object. First, was based on camera`s system and second on common system ESS. Later on they were evaluated and the most considerable benefits were emphasized. A system based on control panel with connected detectors was selected upon specification. Subsequently was created a model of the chosen system, at which the required behaviour was simulated and verified. An outline of an implementation was created in the C language.

Keywords

Mechanic blocking system, MBS, electronic safeguarding signalling, ESS, sensor, control panel, infra-red sensors, microwave sensors, camera system, expansion card, signalling loop, sabotage loop, model, Uppaal, Times Tool, timed automaton, tasks, behaviour, channel, simulation, verification, schedulability analysis.

Citace

Kuchařík David: Systém pro zabezpečení a střežení objektů a prostor. Brno, 2008, diplomová práce, FIT VUT v Brně.

Systém pro zabezpečení a střežení objektů a prostor

Prohlášení

Prohlašuji, že jsem tento semestrální projekt vypracoval samostatně pod vedením Ing. Josefa Strnadele, Ph.d.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
David Kuchařík
7.5.2008

Poděkování

Chtěl bych poděkovat Ing. Josefu Strnadelovi, Ph.d za možnost realizace této práce.

Obsah

1 Úvod

Postupně jak se vyvíjí společnost a narůstá populace, zvyšuje se i podíl nebezpečí, které hrozí jak nám jako fyzickým osobám, našemu stále cennějšímu soukromí a v neposlední řadě majetku, který se snažíme různými způsoby chránit. Všude kolem sebe se setkáváme s různými krádežemi či přepadeními, které se nevyhýbají nikomu. Bylo by pošetilé si myslet, že nám se nemůže nikdy nic takového stát. Proto bychom se nad tím měli zamyslet a následně vykonat alespoň základní opatření pro svoji bezpečnost.

Potřeba ochrany před nebezpečím a s tím spojená potřeba signalizovat toto nebezpečí provází lidstvo od jeho počátku. Nejen, že bylo a je zapotřebí co nejvíce znemožnit vstup a pohyb nežádoucích osob na chráněném pozemku, ale i signalizace, že k narušení došlo a následná reakce je velice důležitá a v některých případech dokonce nezbytná. Nebezpečí hrozby nemusí nutně znamenat zásah jiné osoby do našeho soukromí. Naše bezpečí mohou narušit i přírodních síly, jako je potopa či oheň.

Následující práce se zabývá přehledem, jaké možnosti ochrany majetku v současnosti existují, a to jak mechanické tak elektronické. Následně je vybrán starý řadový rodinný dům v městské zástavbě a proveden dvojí návrh na zabezpečení tohoto objektu. První návrh ukazuje možnost využití kamerového systému a druhý je klasický elektronický zabezpečovací systém. Dále je provedeno zhodnocení výhod jednotlivých navržených systémů a výběr vhodného systému podle kritérií jako je příkon, snadnost instalace či změny struktury. Na vybraném systému založeném na ústředně a k ní připojených detektorů je vytvořen model chování v modelovacím prostředí Times Tool, kde je následně model simulován, verifikován a je také nastíněna implementace pomocí jazyka C.

V poslední kapitole je shrnutí celé práce, uvedeny možné rozšíření a případná návaznost na tento projekt.

2 Historie zabezpečovací techniky

Společně s technickým pokrokem civilizace se vyvíjely i systémy vyhlašování poplachu. Zpočátku bylo zjištění a upozorňování na možnost nebo přímo na nebezpečí v rukou člověka a jeho smyslů. Po zpozorování nebezpečí upozorňoval ostatní křikem, bubnováním, troubením či zvoněním. Jedinou výjimkou byli hlídací psy případně jiná zvířata.

Za průmyslové revoluce na přelomu 18. a 19. století při velkém přílivu obyvatel do měst se možnost vzniku nebezpečí koncentrovala. Zvláště nebezpečí požárů. Velká města řešila tyto problémy postupně zdokonalovanými sítěmi hlásek a požárních stanic, které si předávaly signály posly, zvony, troubením nebo světelnými záblesky.

Zásadním přelomem v přenosu informací na dálku byl vynález telegrafu v roce 1835 a jeho první reálná aplikace v roce 1844 (linka Washingron – Baltimore). Poprvé byl použit v rámci systému pro signalizaci nebezpečí v roce 1847, když hlavní inženýr města New York Cornelius Anderson propojil požární hlásky telegrafem s centrálním stanovištěm. Tato centrála byla dále propojena s jednotlivými požárními stranicemi. Tímto došlo k podstatnému zkrácení doby potřebné k přenosu poplachového signálu od místa ohrožení k „zásahové jednotce“ (tj. nejbližší požární stanici) [1].

Následujícím významným krokem byly tzv. „volací skříňky“ – veřejné hlásiče. Při zatažení za páku hlásiče bylo roztočeno vroubkované kolo a prostřednictvím elektronického kontaktu vyslalo sérii teček a čárek, ve kterých byl obsažen jeho individuální kód. Na centrálním pultu pak primitivní zapisovač zaznamenal zmíněnou sérii, a vytvořil tak záznam o poplachu. Systém byl schválen v Bostonu v roce 1851 a v roce 1854 ve městě fungovalo 42 takových hlásičů. Obdobný systém vybudovaný v Hamburku fungoval až do roku 1976.

První známý elektrický zabezpečovací systém si nechal patentovat v roce 1853 Augustus Pope ze Sommerville (stát Massachusetts, USA). Používal sérii kontaktů instalovaných na dveřích a oknech s baterií a zvonkem. Svůj patent v roce 1857 prodal Edwinovi T. Holmesovi, novoanglickému obchodníkovi s galanterií a šicími potřebami a výrobci krinolín.

V té době ještě nebyl dostatečně rozvinut průmysl a neexistovali dodavatelé elektrických drátů a příslušenství. Proto se Holmes spřátelil s Williamsem, který pro něj začal vyrábět zvonky a kontakty. Musel si také začít vyrábět izolované dráty a vymyslel mnoho dalších základních elektrických součástek, které si patentoval. Ty se později staly základem telefonních systémů. Elektrická zabezpečovací signalizace se zrodila dvacet let před telefonem a čtvrt století před žárovkou. Později pomocí barevných klapek vytvořil „adresový“ systém indikující stav každého zabezpečeného okna nebo dveří. Přidáním hodin systém „programoval“ na zapínání a vypínání ve stanovenou dobu a později i na ovládání domovního osvětlení.

Roku 1858 uvedl Holmes do provozu první centrály elektronické ochrany v Bostonu a New Yorku. 1872 přišel tento vynálezce s „elektrickým sekretářem“ pro ukládání klenotů. Byl to úložní

objekt se stěnami propletenými průběžnou vodivou fólií a s dveřmi opatřenými kontakty, tento systém byl také připojený na centrální stanoviště se 24hodinovou službou schopnou kdykoli zakročit.

Na síti vytvořené pro zabezpečování zkoušel Graham Bell přenos lidského hlasu na velkou vzdálenost a roku 1876 ohlásil vynález telefonu. Zkoušky byly natolik úspěšné, že byl Edwin Holmes požádán o vytvoření první komerční ústředny.

Dlouho se pro elektronickou signalizaci používaly pouze kontakty. Využívaly se různé druhy kontaktů spínacích i rozpínacích, často ve spojení s nástražným drátem, a také destrukční čidla (zabudované vodiče, které se při pokusu o proražení přerušily). Až na počátku 20. století se objevily elektromechanická čidla založená na principu setrvačnosti, případně kyvadla. Speciální kyvadlová čidla pro ochranu trezorových místností, různé typy vibračních kontaktů, používaných až do začátku 80. let, a inerciální senzory, používané dodnes pro zabezpečení a ochranu vozidel (reagují na jejich rozhoupání).

Zabezpečovací ústředny byly až do 50. let 20. stolení založeny na relé. S objevem polarizovaného relé, které umožnilo používání vyvážených smyček, podstatně narostla odolnost zabezpečovacích systémů. Pro signalizaci se používaly převážně zvonky, ty jsou používány dodnes.

Teprve rozvoj elektroniky za druhé světové války a po ní, zejména pak průmyslová výroba tranzistorů a následná miniaturizace elektronických zařízení, a posléze boom nových technologií umožnily vznik nových druhů čidel, jejich elektronizaci a následnou komputerizaci. Výkon současné výpočetní techniky nyní dovoluje nahradit některé činnosti, které dosud bylo možné zajišťovat výlučně lidskou silou.

Elektronická čidla se začala objevovat v 50. letech 20. stolení. Jsou to zejména tzv. trezorové kontakty – akustické snímače připevňované na chráněný objekt a vyhodnocující hluky šířící se materiálem. Byly ale dosti náchylné k planým poplachům způsobených přenosem chvění z okolí. Dalšími čidly byly kapacitní, vyhodnocující kapacitu chráněného objektu proti zemi. Spolehlivost těchto čidel již byla vysoká, ale byla nutná pečlivá příprava a montáž. Dále také první aktivní prostorová čidla na principu vyhodnocování šířeného ultrazvuku v uzavřeném prostoru. Jejich klíčovým problémem byla stabilizace vysílaného kmitočtu a také náročná instalace. V této době začínají být postupně vytlačovány mechanické kontakty magnetickými snímači s kontaktem jazýčkovým [1].

V 60. letech byly polovodičové součástky na takové úrovni, že bylo možné sestrojit VKV prostorová čidla. Pracují na principu pokrytí chráněného prostoru nemodulovaným signálem o frekvenci řádu stovek MHz a vyhodnocování změn elektromagnetického pole. V této době byly velice populární. Byly vyráběny v různých provedeních, jako jedno i víceanténová. Hlavní výhodou byla možnost pokrytí více místností jednou soupravou, ale vzhledem k této vlastnosti vyžadovaly velké zkušenosti techniků při nastavování a ladění v konkrétních podmínkách.

Gunnovy diody jako zdroje generátoru GHz frekvencí a jejich komerční výroba umožnily rozšíření mikrovlnných čidel. Toto umožnilo na přelomu 60. a 70. let vznik systémů s možností

poměrně snadného a cíleného pokrytí střeženého prostoru prakticky neodstínitelným signálem, a tím téměř nepřekonatelnou spolehlivost detekce. Dodnes patří mikrovlnná čidla mezi nejúčinnější zabezpečovací technologie, ovšem s podmínkou jejich perfektního zvládnutí a velkých zkušeností z praktického využívání.

V této době, kdy se již začaly vyrábět různé polovodičové součástky a mezi nimi miniaturní zdroje infračerveného světla, se začínají rozšiřovat i tzv. „světelné závory".

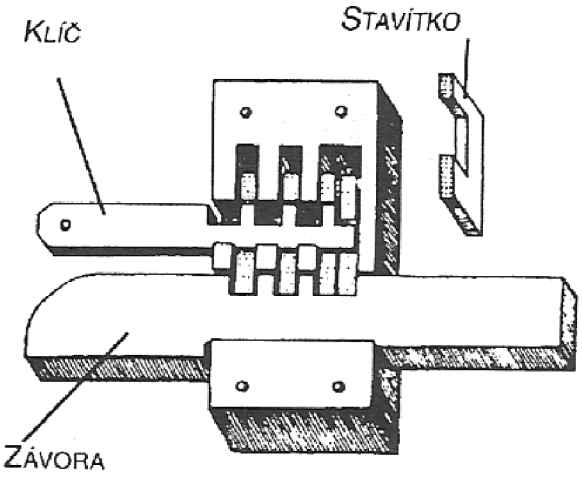
Ve druhé polovině 70. let se na trhu objevuje dodnes nejúspěšnější zabezpečovací prvek – pasivní infračervené čidlo (Passive Infrared Detector – PIR). Jejich původ byl v armádním využití pro samonavádění protiletadlových a protitankových raket. Brzy byla těmito čidly nahrazena mikrovlnná čidla, která byla aplikačně i energeticky náročnější. I když PIR čidla nedosahují bezpečnostní spolehlivosti čidel fungujících na Dopplerově principu, jejich spolehlivost, cena a relativní jednoduchost použití měly brzy za následek vytlačení ostatních typů prostorových čidel.

V poslední době se prudce rozvíjí biometrické systémy využívající různých anatomických a fyziologických vlastností člověka k jeho identifikaci. Zatím byly využívány zejména v přístupových systémech (Access Control Systems), ale rozšiřují se stále více i do bezpečnostních aplikací. Zvláště systémy průmyslové televize (CCTV), po padesát let využívané téměř výlučně jako monitorovací a dokumentační prostředek, s výjimkou aplikace jako detektorů pohybu, zaznamenávají kvalitativní skok do zcela nových dimenzí bezpečnostních aplikací [1].

3 Mechanické zábranné systémy

Vznik mechanických zábranných systémů (MZS) byl vynucen stále většími požadavky na ochranu nejprve vlastního života a později i majetku. Na základě tohoto začala vznikat a posléze se vyvíjet ochrana osad a obydlí. Prvními zábranami byly ploty, ohrady, příkopy, hradby, dále pak ochrana vstupů – dveře, okenních otvorů, skříně, truhlice a později i zámky a klíče. Tyto poznatky jsou zřejmé z písemných zmínek ve starých záznamech. I když základním výrobním materiálem bylo dřevo, dochovaly se o nich důkazy v archeologických nálezech.

Pro zabezpečovací zábrany byl důležitý vývoj zámkové techniky datovaný od dob řecké a římské kultury. Nejbouřlivější vývoj nastal v 18. a 19. století, kdy se začaly vyrábět precizní zámky a úschovné objekty a také v 20. století, kdy se začala připojovat i elektronika. Příkladem jednoho z prvních zámků může být dřevěný zámek egyptského typu se zásuvným klíčem používaným okolo roku 1500 př. n. l. (obrázek 3.1).



Obrázek 3.1: Dřevěný zámek egyptského typu se zásuvným klíčem 1500 př. n. l.

3.1 Charakteristika MZS

3.1.1 Stupeň pasivní (průlomové) odolnosti

Každý mechanický zábranný systém je překonatelný v nějakém relativním čase. Cílem těchto systémů je prodloužit tento čas na dobu, kdy je již systém pod další kontrolou. Například do příjezdu hlídací služby.

Nejdůležitější parametry pro určení průlomové doby:

- kvalita MZS,
- znalosti konstrukce překonávaného zařízení,
- umístění MZS,

- druh a kvalita techniky použité pro překonání,
- možnost použití vedlejších energetických zdrojů.

Vlastní stupeň pasivní odolnosti vyjadřuje vztah maximálního prodloužení časového intervalu *t*, který je potřebný pro překonání bezpečnostního zařízení. $\Delta \mathbf{t} = \mathbf{t_2} - \mathbf{t_1}\ [\mathbf{min}]$, kde Δt je časový interval potřebný k překonání překážky, *t2* čas zahájení práce na překonání zábrany a *t1* čas ukončení překonávání zábrany.

3.1.1.1 Stanovení minimální doby průlomové odolnosti pro otvorové výplně

Mezi otvorové výplně patří dveře, okna, balkónové dveře, mříže, vrata apod. Čas je přiřazen podle bezpečnostních tříd (BT) a stanoven empiricky podle předpokládaného způsobu napadení. V následující tabulce (tabulka 3.1) je uveden minimální potřebný čas pro překonání podle norem ČSN P ENV 1627 a ČSN P ENV 1630 [1].

Bezpečnostní třída	Kategorie nářadí	Předpokládaný způsob napadení	Odporový čas (min)
1	bez	Příležitostný zloděj; pouze fyzické násilí (rozbití okna)	Neměřen
2	A	Příležitostný zloděj; jednoduché nástroje (kleště, klín)	3
3	B	Další nářadí, druhý šroubovák, páčidlo	5
4	C	Zkušený zloděj; použití pily, kladiva, sekery, aku. vrtačky	10
5	D	Další el. nářadí: vrtačky, přímočará pila, úhlová bruska max. 125 mm kotouč	15
6	E	Výkonné el. nářadí: úhlová bruska max. 230 mm kotouč	20

Tabulka 3.1: Bezpečností třídy a odporový čas otvorových výplní.

3.1.1.2 Stanovení minimální doby průlomové odolnosti pro úschovné objekty

Mezi úschovné objekty patří plechové skříně, mobilní i stabilní trezory, přenosné objekty apod. Minimální doba průlomové odolnosti se stanoví výpočtem při použití bezpečnostních tříd pro klasifikaci skříňových trezorů a hodnot průlomové odolnosti (jednotky RU), dle normy ČSN EN 1143-1 je sestavena tabulka 3.2.

Vztah pro výpočet minimální doby průlomové odolnosti: $\mathbf{T} = [(\mathbf{V_R} - \mathbf{B_V}) : \mathbf{C_1}]$, kde *T* je minimální doba průlomové odolnosti, V_R hodnota průlomové odolnosti v RU, dle charakteru částečného nebo úplného průlomu, B_V základní ohodnocení použitého nářadí $\mathbf{C_1}$ koeficient průlomové odolnosti (tabulka 3.3)

Pro stanovení optimální doby průlomové odolnosti je nutné výslednou hodnotu *T* násobit koeficientem (2 až 3) – koeficient praktického navýšení $\mathbf{T_{opt}} = \mathbf{T} \cdot (\mathbf{2} - \mathbf{3})$ [1].

Bezpečnostní třída	Zkouška napadení		Pevnost ukotvení [1]	Zámky		Doplňkový požadavek pro označení EX [3]
	Hodnosta průlomové odolnosti		Požadovaná síla	Množství	Třída dle EN 1300	Hodnota průlomové odolnosti po výbuchu
	Částečný průlom	Úplný průlom				
	RU	RU	kN			RU
0	30	30	50	1	A	[2]
I	30	50	50	1	A	[2]
II	50	80	50	1	A	4
III	80	120	50	1	B	6
IV	120	180	100	2	B	9
V	180	270	100	2	B	14
VI	270	400	100	2	C	30
VII	400	600	100	2	C	30
VIII	550	825	100	2	C	41
IX	700	1050	100	2	C	53
X	900	1350	100	2	C	68

[1] pouze pro mobilní trezory s hmotností < 1000kg

[2] označení EX není možné pro třídy 0 a I

[3] pro označení EX musí skříňové trezory, trezorové dveře a komorové trezory odpovídat hodnotě průlomové odolnosti v souladu s uvedenými tabulkami.

Tabulka 3.2: Minimální požadavky pro klasifikaci skříňových trezorů do BT.

Bezpečnostní třída úschovného objektu podle ČSN EN 1143-1	Koeficient RU/min C_1
0-I	5
II-III	7,5
IV-VII	10
VIII-X	15

Tabulka 3.3: Koeficienty průlomové odolnosti C_1.

3.2 Rozdělení mechanických zábranných systémů

Mechanické zábranné systémy jsou tvořeny prostředky pro ohraničení prostor, vstupní a bezpečnostní systémy dveří a oken, mříže, bezpečností skla a fólie a vlastní uzamykací systémy. Můžeme je rozdělit do následujících tří skupin.

3.2.1 Prostředky obvodové ochrany

Mechanické zábrany, které nejsou přímou součástí vlastního objektu, ale jsou od něj prostorově odděleny. Nacházejí se na volné ploše a většinou vytvářejí jak fyzickou tak právní hranici pozemku.

Do této kategorie patří zejména zdi a ploty a s nimi související prvky pro vstup jako dveře, vrata, branky, závory či turnikety.

3.2.1.1 Zdi

Aby zeď plnila funkci bariéry, musí znesnadnit přelezení, podlezení či podhrabání. Musí také splňovat parametry na pevnost, minimální výšku 2,5 m a musí stát na podezdívce.

3.2.1.2 Ploty

Ploty se skládají z pevné nosné konstrukce se sloupky zajištěnými proti vyvrácení a výplní ať už z jednotlivých profilů nebo drátěného pletiva. Všechny kovové části plotů musí být povrchově ošetřeny proti působení povětrnostních vlivů. Příklady plotů jsou na následujícím obrázku.

Obrázek 3.2: Příklady plotů.

3.2.1.3 Průchozí prvky zdí a plotů

Mezi průchozí prvky patří zejména dveře, vrata a branky. Musí být pevně a bezpečně usazeny do zdí a plotů tzn., musí mít tuhou konstrukci, pevné uchycení a bezpečný uzamykací systém. Ke speciálním prvkům patří závory, průchody či turnikety, ty ale nedosahují takového stupně bezpečnosti.

Obrázek 3.3: Vrata, branka.

3.2.1.4 Vrcholová ochrana

Představuje ochranu na vrcholu zdi či plotu. Mezi takovou ochranu patří:

- konstrukce z ostnatého drátu,
- konstrukce z tzv. žiletkového drátu,
- pevné hroty na vrcholu plotů či zdí.

Obrázek 3.4: Příklad žiletkového drátu.

3.2.1.5 Visací zámky a petlice

Visací zámky můžeme rozdělit podle funkce:

- zámky se zásuvným klíčem – klíč zasunutím uvolní zábranu závory,
- zámky s otočným klíčkem – klíč se po zasunutí do zámku otáčí kolem své osy.

Zámky se mohou také dělit na zámky se svorníkem a na zámky se třmenem. Svorník se při otevřeném zámku vždy odjímá ale třmen se buď odjímá nebo povytáhne a pootočí.

Dále můžeme zámky rozčlenit podle typu otevíracího elementu – klíče:

- obyčejné – vybavené odpruženou závorkou,
- dozické – mimo závorku mají plochá stavítka, klíč má radiální drážky odpovídající jednotlivým stavítkům,
- motýlkové – závorka i stavítka, uzpůsobená pro oboustranné vedení zubem klíče,
- cylindrické (s cylindrickou vložkou) – válcová odpružená stavítka vedle sebe nebo lamelová nad sebou,
- heslové/kódové – uzamykání bez klíče za pomoci heslových kotoučků.

Petlice je nezbytná součást většiny uzamykacích systémů, kde je využit právě visací zámek. Bezpečné petlice jsou vyráběny z kvalitní legované oceli a plní mimo funkce spojení pohyblivé a nepohyblivé části rovněž funkci ochrany visacího zámku [1].

3.2.2 Prostředky objektové ochrany

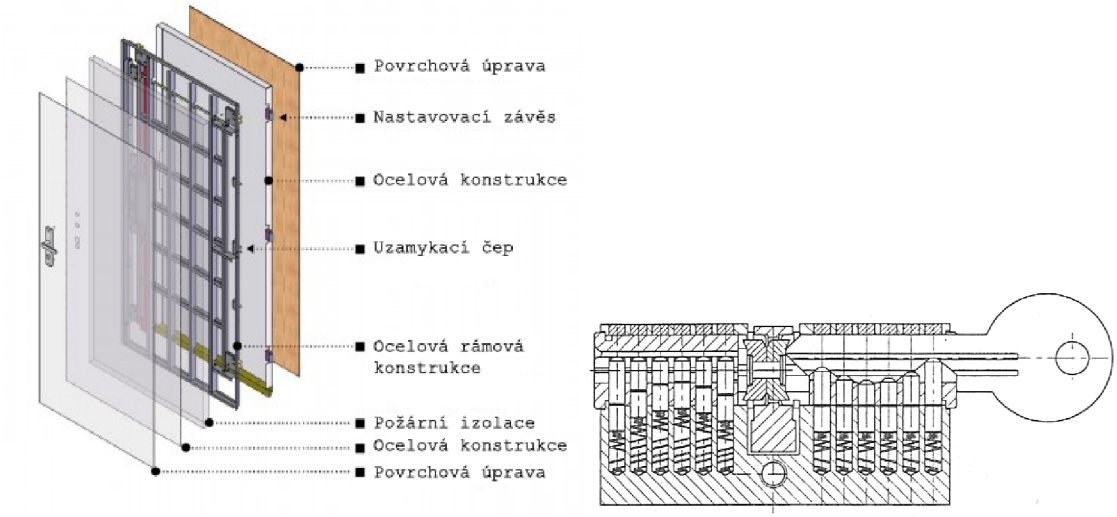
Jedná se o zabezpečení vstupu do všech stavebních otvorů v objektu, tj. dveří, oken, balkónových oken, sklepních oken, vikýřů, zásobovacích a energetických šachet apod.

3.2.2.1 Dveře

Dveřní prostor je nejdůležitějším stavebním otvorem. Je tvořen zárubní a dveřním křídlem. Zárubeň ať už dřevěná či z ocelových profilů musí být dobře ukotvena a být opatřena závěsy pro nasazení a pohyb dveřního křídla. To musí být na tolik pevné, aby zajistilo neprokopnutelnost a nevyvratitelnost dveří.

S dveřmi velmi úzce souvisí uzamykací systém tvořený zadlabacím zámkem s bezpečnou klíčovou sestavou a ochranným kováním. Zámky lze rozdělit na obyčejné a bezpečnostní. Obyčejné využívají jednoduchý mechanizmus v podobě posouvání závory klíčem s plným zubem. Bezpečnostní zámky využívají vložky dozické, motýlkové a hlavně cylindrické.

Bezpečnostní dveře mají následující bezpečnostní prvky: zvýšenou odolnost (sendvičové složení, protipožární), nejméně tři závěsy, zvýšený počet uzamykacích míst po obvodu dveřního křídla (rozvorový systém), nejméně dva uzamykací zámky, vlastní bezpečností zárubeň. Příklad bezpečnostních dveří je uveden na obrázku 3.5.



Obrázek 3.5: Bezpečnostní dveře, cylindrická vložka zámku.

3.2.2.2 Okna

Okno je rámová konstrukce s průhlednou či průsvitnou výplní, osazovaná obvykle do obvodových stěn budov. Hlavní funkcí je osvětlení pomocí denního světla a možnost větrání. Konstrukce může být otevíratelná nebo neotevíratelná, další dělení je podle typu otevírání.

Uzávěry a kování zvláště u přízemních oken musí být kvalitní a nejlépe uzamykatelné. Pro zvýšení bezpečnosti se používají tvrzená skla, skla s bezpečnostní fólií či vrstvená skla.

3.2.2.3 Mříže a další zabezpečovací prvky

Jsou jedny z nejstarších mechanických zabezpečovacích systémů. Nemají normativní podklady, při výrobě i montáži se vychází z empirických zkušeností. Nejdůležitějším parametry jsou velikost ok a průřez materiálu. Velikost mřížového oka by neměla být větší než 10 x 20 cm.

Dalšími zabezpečovacími systémy mohou být rolety, žaluzie nebo posuvné panely.

3.2.3 Prostředky individuální ochrany

Do této kategorie patří zejména úschovné objekty. Primární funkcí je zajištění finanční hotovosti, šperků, sbírek, cenných papírů, důležitých dokumentů a jiných cenností. Patří sem mobilní i stabilní trezory, ohnivzdorné skříně, příruční pokladny manipulační schránky a přenosné kontejnery a kufry. Tyto systémy vyžadují nejvyšší stupeň zabezpečení, např. u trezorů je uzamykací zařízení ukryto uvnitř dveří a skládá se ze závorového systému a vlastního zámku.

Obrázek 3.6: Příklady trezorů.

4 Elektronické zabezpečovací systémy

Zařízení elektronické zabezpečovací signalizace (zařízení EZS) je soubor čidel, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, zapisovacích zařízení a ovládacích zařízení. Prostřednictvím těchto prvků je opticky nebo akusticky signalizováno na předem určeném místě narušení střeženého objektu nebo prostoru.

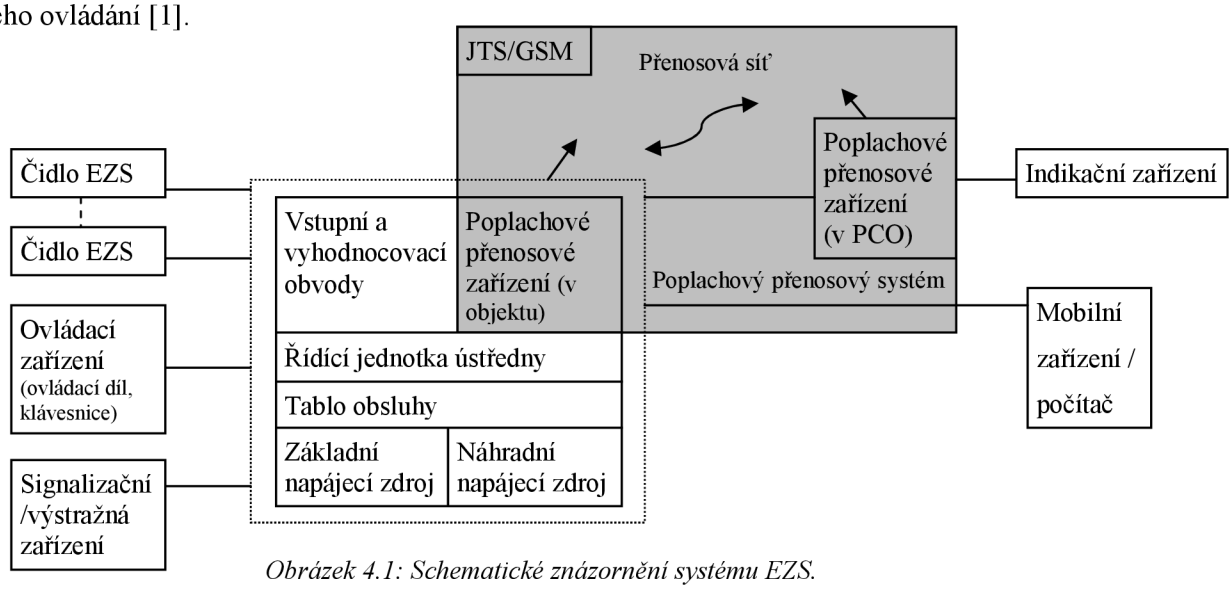
Čidlo EZS je zařízení reagující na vnější vlivy související s narušením střeženého objektu, prostoru nebo s nežádoucí manipulací se střeženým předmětem vytvořením předem daného výstupního signálu.

Ústředna EZS je zařízení určené k příjmu a vyhodnocení signálů z čidel nebo tísňových hlásičů a k vytvoření signálu o narušení.

Pult centralizované ochrany (PCO) je zařízení vyhodnocující a schopné přenést signalizaci o narušení ze zabezpečených objektů do místa centrálního vyhodnocení pomocí linek jednotné telekomunikační sítě (JTS) či sítě GSM.

Zajišťovací/ochranná smyčka je vedení spojující elektricky zajištěné kryty, skříně nebo víka skříní zařízení EZS nebo zajišťovací kontakty zařízení EZS s příslušným vstupem ústředny. Úkolem je identifikace narušení přímo prvku EZS.

Tablo obsluhy je zařízení, které poskytuje informace o výstupních stavech EZS a umožňuje jeho ovládání [1].



Obrázek 4.1: Schematické znázornění systému EZS.

Stupně zabezpečení jednotlivých prvků EZS jsou definovány v normě ČSN EN 50131-1 a stanovují kritéria na výbavu a funkci jednotlivých komponentů i systému jako celku.

4.1 Prvky plášťové ochrany

Tyto prvky hrají roly hlídání otevření případně destrukce vstupních otvorů budov, jako jsou dveře, okna, vrata.

4.1.1 Magnetické kontakty

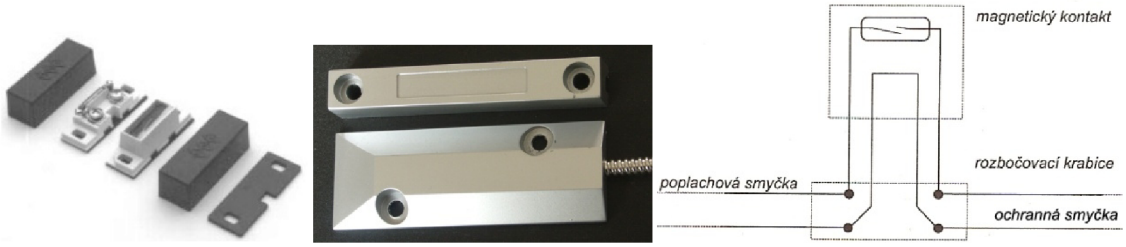
Nejvíce používané jako čidla otevření všech stavebních otvorů, nejčastěji oken a dveří jsou právě magnetické kontakty.

Ty se skládají ze dvou částí. Z jazýčkového kontaktu, který se nachází v zatavené skleněné trubičce naplněné ochrannou atmosférou a permanentního magnetu.

V klidovém stavu je jazýčkový kontakt sepnut vlivem magnetického pole permanentního magnetu. Oddálením magnetu dojde k rozepnutí kontaktu a tím ke spuštění poplachu. Jazýčkový kontakt se montuje na rám a permanentní magnet část pohyblivou.

Pro speciální případy existují bezpečnější varianty, které jsou odolné vůči cizímu magnetickému poli. Využívá se buď polarizovaný jazýčkový kontakt, nebo sérioparalelní kombinace kontaktů.

Příklad konkrétního výrobku může být magnetický kontakt GRI 129A (sepnutí 13 mm, rozměry 38x13x13 mm) vyobrazený v první části obrázku 4.2.



Obrázek 4.2: Příklady magnetických kontaktů, el. zapojení s ochrannou smyčkou.

4.1.2 Čidla pro ochranu skleněných ploch

Tříštění skla vyvolává charakteristický zvuk, který se v něm šíří jako vlnění. Kontaktní čidla přilepená na skle toto vlnění zachycují a vyhodnocují. Praktický dosah je až 3 metry. Využívají se zejména u neotvíratelných skleněných ploch, jako jsou výlohy. Tento typ čidel bývá náchylný na zvuky z dopravního ruchu.

Aktivní čidla pro ochranu skel obsahují vysílací a přijímací část. Zde elektronika vyhodnocuje změnu přenosu oproti stavu uloženému v paměti čidla. Výhodou je velký dosah až 25 m^2 plochy.

Dále existují akustická čidla rozbití skleněných ploch. Vyhodnocují následný akustický efekt při tříštění skla. Využitím pásmových propustí zkoumají jen požadované pásmo frekvencí. Negativní vliv mohou mít všechny zvuky v podobném frekvenčním pásmu. Novější typy vyhodnocují zvukové spektrum ve více diskrétních bodech, tj. přítomnost tříštivého zvuku o vysoké frekvenci a rázové vlny

vzniklé borcením skla o nízkých frekvencích v určitém časovém sledu. Těmito čidly může být chráněno i více ploch najednou.

Praktickým příkladem může být detektor firmy Jablotron GBS-210. K detekci užívá duální metodu, při které jsou vyhodnocovány nepatrné změny tlaku vzduchu v místnosti (náraz do skleněné výplně) a následné zvuky řinčení skla. Parametry a obrázek jsou uvedeny níže [4].

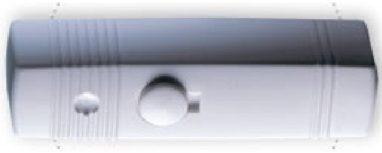
- klidový odběr (bez LED): max.10 mA,
- maximální odběr (včetně LED): max. 35 mA,
- detekční vzdálenost: od 1,5 do 9 m,
- minimální plocha okenní výplně: 0,6 x 0,6 m,
- doba stabilizace po zapnutí: max. 60 s,
- klasifikace dle ČSN EN 50131-1: stupeň 3 (střední až vysoké riziko),
- prostředí dle ČSN EN 50131-1: II. vnitřní všeobecné,
- rozsah pracovních teplot: -10 až +40 °C.

Obrázek 4.3: Detektor Jablotron GBS-210.

4.1.3 Mechanické kontakty a vibrační čidla

Mezi mechanické kontakty patří mikrospínače instalované do rámů proti západkám zámků. Tyto kontakty slouží ke střežení uzamčení prostor. Při vhodném nastavení může zabránit přechodu EZS do střežícího stavu. Patří sem i tzv. nájezdy sloužící pro přenesení proudu k čidlům na posuvných či otočných dílech.

Vibrační čidla se využívají pro střežení průrazu pláště budov v kritických místech. Zástupcem těchto detektorů vibrací může být Vibro od firmy Optex [3].



Obrázek 4.4: Vibrační detektor Optex Vibro.

4.1.4 Další plášťové zabezpečovací prvky

Poplachové fólie, tapety a poplachová skla pracují na principu přerušení tenkých drátků integrovaných v těchto materiálech.

Drátová čidla jsou složena z množství jemných ocelových lanek propojených s citlivým mikrospínačem. Tento typ zabezpečení je vhodný pro střežení prostorů inženýrských sítí či ventilací. Ke stejnému účelu se využívají i rozpěrné tyče, což je miniaturní mechanický spínač aretovaný v klidovém stavu tyčí.

4.2 Prvky prostorové ochrany

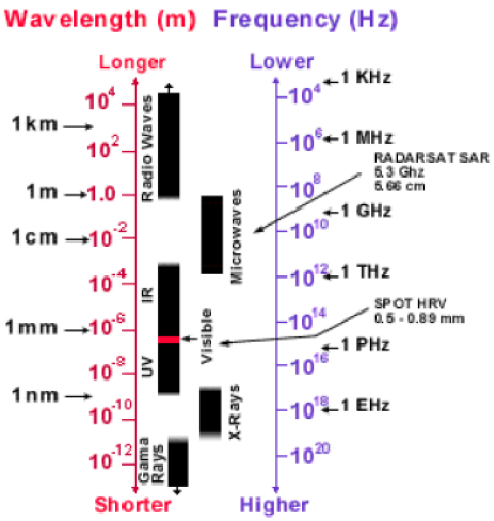
Prostorová čidla jsou velmi dobrým doplněním, ale mnohdy používané i jako náhrada plášťové ochrany objektů. Můžeme je rozdělit na aktivní a pasivní.

- pasivní zjišťují fyzikální změny okolí bez vlastního vlivu,
- aktivní zkoumají fyzikální změny na okolí pokrytém vlastním působením.

V praxi se používají následující čidla pohybu:

- pasivní infračervená čidla (Passive Infra Red – PIR),
- aktivní ultrazvuková čidla (Ultrasonic – US),
- aktivní mikrovlnná čidla (Microwave – MW),
- duální (kombinovaná) čidla (PIR-US, PIR-MW).

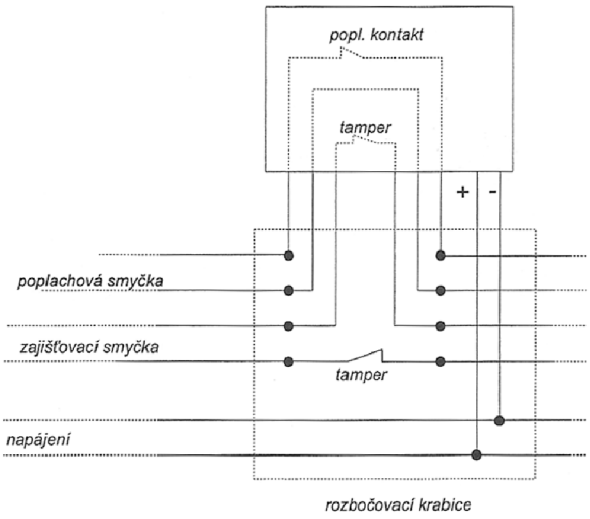
Všechna tato čidla používají elektromagnetické záření, jen s tím rozdílem, že každé využívá jiné frekvenční pásmo.



Obrázek 4.5: Elektromagnetické spektrum.

Některé modely výrobců bývají vybaveny dalšími rozšiřujícími funkcemi zvláště, co se zpracování signálu týče. Jsou to zejména dálkové odpínání indikační LED pro jednodušší instalaci a kontrolu, odpínání MW a US vysílací části čidel kvůli citlivějším osobám, paměť poplachu pro indikaci daného čidla a ochranu proti zastínění. Ta umožňuje kontrolu, zda nebylo čidlo zastíněno (přestříkáno barvou) v klidovém stavu systému [2].

Na následujícím obrázku je zaznamenáno, jak se obecně zapojují detektorů pohybu.



Obrázek 4.6: Elektrické zapojení detektoru pohybu.

4.2.1 Pasivní infračervené čidlo – PIR

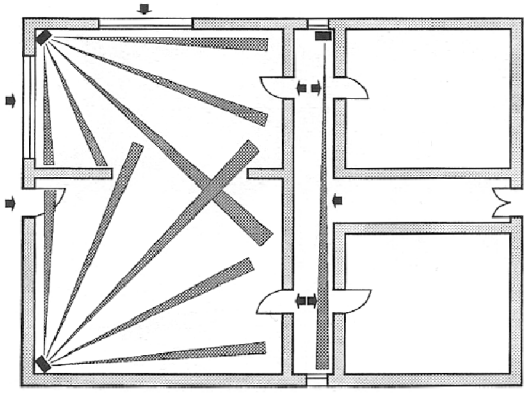
Tato čidla jsou založena na principu změn vyzařování předmětů v infračerveném pásu elektromagnetického spektra. Všechny tělesa o teplotě od -273 °C do 560 °C jsou zdrojem infračerveného záření odpovídající teplotě daného tělesa. Při zvyšující se teplotě se snižuje vlnová délka směrem k viditelné části elektromagnetického spektra. Pro teplotu lidského těla (cca 36,5 °C) je vlnová délka 9,4 mm.

Jako detektory se využívají materiály s pyroelektrickým jevem. Detekční prvek je měnič gradientní povahy, který detekuje pouze změny záření, které na senzor dopadají. O transformaci odrazu střeženého prostoru se stará optická soustava. Zorné pole je rozděleno na aktivní a neaktivní části, a detekce vyzařovaných změn se odehrává na přechodech těchto oblastí.

Tvar zorného pole je závislý na vlastnostech optiky, citlivosti senzoru a způsobu vyhodnocení. Podle použité optiky je možné střežit prostor do vzdálenosti cca 15 m, nebo dlouhé prostory cca 60 m. Při použití kruhové optiky střežit prostor v rozsahu 360°.

Optika se převážně skládá buď z Fresnelových čoček, nebo ze soustavy křivých zrcadel. Fresnelovy čočky jsou velice ekonomické, ale nedosahují kvality zobrazení prostoru jako křivá zrcadla. Určitou alternativou jsou tzv. černá zrcadla, která propouští pouze infračervenou složku elektromagnetického záření, čímž snižují možnost planých poplachů vlivem záření o vysoké energii ve viditelném spektru, například odlesky slunce, reflektory automobilů apod.

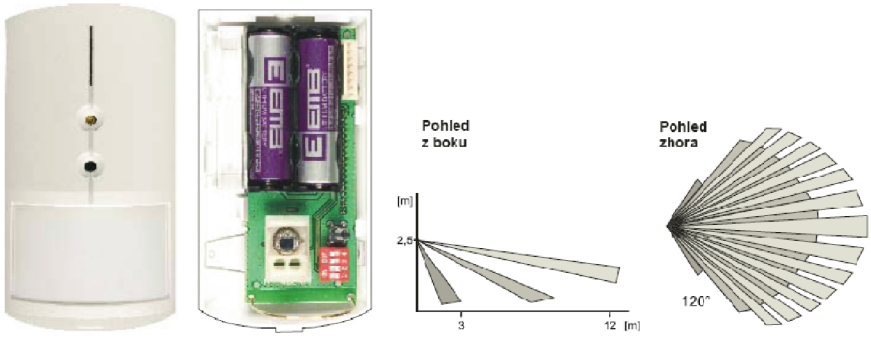
Pro správnou detekci musí být PIR čidla instalována tak, aby pravděpodobný pohyb pachatele byl kolmý na myšlený průmět aktivní/neaktivní zóny od půdorysu střeženého prostoru [1]. Příklad umístění PIR čidel je uveden na následujícím obrázku.



Obrázek 4.7: Příklad správného umístění PIR čidel.

Falešný poplach mohou způsobit vstupy a výstupy ventilace, průvan, sluneční odrazy, reflektory, proměnné zdroje tepla (topení, komíny), spínané rušivé IR zdroje (žárovky). V prostorách s podlahovým topením se tyto čidla nedoporučují.

Příkladem PIR senzoru s pokročilými funkcemi může být Jablotron JA-84P bezdrátový PIR detektor s kamerou. Umožňuje detekovat pohyb ve střeženém prostoru včetně vizuálního potvrzení poplachu. Kamera detektoru je vybavena bleskem pro focení v noci. Je schopna pořizovat černobílé statické snímky v rozlišení 160x128 bodů. Je-li zaznamenán pohyb, je pořízena sekvence fotografií. Ty jsou uloženy v interní paměti detektoru a bezdrátově přenášeny do ústředny v komprimované podobě, odkud jsou posílány mimo objekt. Detektor je napájen z baterií a komunikuje protokolem OASiS [4].



Obrázek 4.8: Jablotron JA-84P a jeho detekční charakteristika.

4.2.2 Ultrazvuková čidla – US

Ultrazvuková čidla využívají část spektra mechanického vlnění o frekvenci, kterou člověk neslyší, ale jiná zvířata jej slyšet mohou, např. pes či netopýr. Vyzařují do prostoru vlnění, tzn., jsou to aktivní detektory.

Vysílač produkuje vlnění s konstantní frekvencí, toto vlnění se odráží od předmětů v prostoru a vrací se zpět, kde je vyhodnoceno elektronikou ve vztahu k původnímu vyslanému signálu. Pokud se pohybuje v prostoru nějaký předmět, mění se fáze vlnění. Jde o aplikaci Dopplerova jevu v pásmu

ultrazvukových frekvencí. Tento jev lze vyjádřit matematicky: $\mathbf{f_1} = \frac{\mathbf{f}}{\mathbf{1}-\left(\frac{\mathbf{v}}{\mathbf{c}}\right)^2}$, kde f_1 je přijatá frekvence, f vyslaná frekvence, v rychlost pohybu odrazné plochy a c rychlost pohybu použitého vlnění.

Čidla by se měla instalovat tak, aby potenciální pohyb pachatele byl směrem k nebo od čidla. Senzory se mohou použít v jednom prostoru jen tehdy, když jsou synchronizovány, nebo jejich frekvence natolik stabilní, že se neovlivňují. Prostor musí být uzavřený kvůli dosahu čidla. Neměla by se instalovat do prostor s častými změnami v interiéru (sklady).

V současné době se používají ultrazvuková čidla spíše pro detekci vzdálenosti např. v automobilovém průmyslu, či úrovně naplnění kapalinou.

4.2.3 Mikrovlnná čidla

Využívají stejný fyzikální princip jako ultrazvuková čidla, ale pracují v jiném frekvenčním pásmu. Nejvyužívanější pásma jsou 2,5 GHz, 10 GHz a 24 GHz. Původně se využívaly vlnovody, u kterých byla nákladná výroba, proto se přešlo k realizaci pomocí mikropáskového vedení integrovaného do desky plošných spojů.

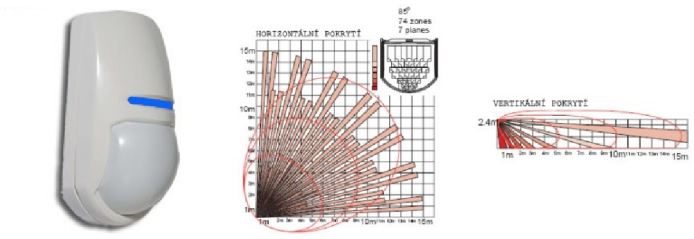
Stejně jako ultrazvuková čidla by se měla mikrovlnná instalovat tak, aby pravděpodobný pohyb pachatele byl k nebo od čidla. Dále se musí dbát na fakt, že mikrovlny pronikají skleněnými plochami a tenkými stěnami (ze dřeva, plastu). Z toho vyplývá, že pohyb za těmito překážkami může vést ke spuštění poplachu.

Tato čidla se často používají v kombinaci s PIR v jednom detekčním zařízení.

4.2.4 Kombinovaná čidla

Zejména tam, kde jsou velice složité podmínky s výraznými negativními vlivy okolního prostření, se využívá kombinovaných čidel PIR-US nebo PIR-MW. Vychází se z toho, že je velmi malá pravděpodobnost, že když použijeme pro detekci dva rozdílné fyzikální principy, vzniku takových jevů, které by ovlivnily oba druhy čidel najednou. Tím se snižuje riziko falešných poplachů.

Příkladem takového kombinovaného detektoru může být Pyroxin KX15DTAM využívající dvě PIR a jedno MW čidlo, systém antimasking 0-1 m, dosah a úhel záběru podle nastavení (15m/85° nebo 18(30)m/20°), rozměry (vxšxh) 117x68x50 mm, vlastní senzor a rozpětí záběru je vyobrazeno na následujícím obrázku [5].



Obrázek 4.9: Kombinované čidlo Pyroxin KX15DTAM a rozsah jeho pokrytí.

4.3 Prvky venkovní obvodové ochrany

Tyto prvky jsou určeny pro signalizaci narušení vnějších částí rozlehlých pozemků a komplexů budov na ohraničeném pozemku.

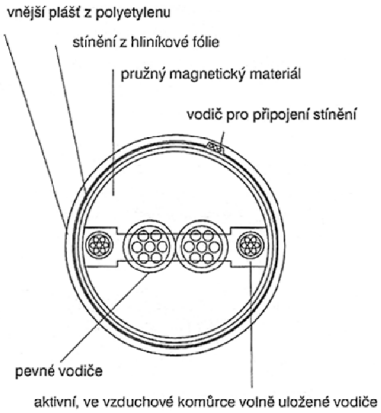
Hlavním rozdílem oproti vnitřním senzorům je jejich mechanická a klimatická odolnost odpovídající místu použití. Další rozdíl je v rozsahu možné detekce, ta byla u vnitřních čidel maximálně řádově desítky metrů, ale u venkovních jsou to 100 metrů. Jak z technických tak i ekonomických důvodů není možné střežit celý prostor s adresací každého místa a řeší se tento problém přímkovými koridory u hranice pozemku.

Důležitou podmínkou pro instalaci elektrické venkovní obvodové ochrany je existence mechanické zábrany (zeď, oplocení) na okraji pozemku. Důležitá je také schopnost eliminovat vlivy prostředí, které nemají vliv na bezpečnost. Těmi jsou například vítr, sníh, déšť, vlnění trávy, pohyb stromů a keřů, vibrace oplocení ve větru, malá volně žijící zvířata či provoz za hranicemi pozemku. Nejen z těchto důvodů se často kombinuje systém venkovní perimetrické ochrany se systémy průmyslové televize (CCTV).

4.3.1 Mikrofonické kabely

Pomocí těchto kabelů je transformováno mechanické namáhání či záchvěvy na elektrický signál, který se následně zpracovává a vyhodnocuje. Akustický odposlech pomáhá k rozpoznání charakteru narušení. Úroveň pro vyhlášení poplachu je nastavitelná.

Může být použito pro ochranu v drátěných plotech, instalovat pod omítku či zalití do betonu. Délka jednoho úseků může být až 300 metrů. Rizikovými faktory jsou silný déšť, krupobití či zvěř.



Obrázek 4.10: Příklad provedení mikrofonického kabelu.

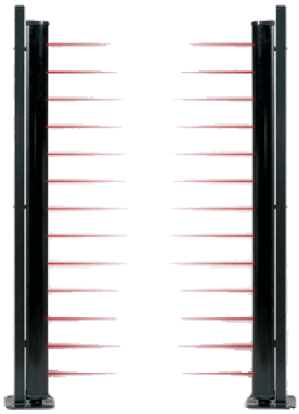
4.3.2 Infračervené závory a bariéry

Nejpopulárnější druh perimetrických obvodových čidel jsou infračervené závory tzv. infrazávory. Mají vysílací a přijímací stranu, mezi kterými je jeden nebo více infračervených paprsků. Na

přijímací straně dochází k vyhodnocování a při přerušení některého (nebo kombinace, pak řízeno logikou) z paprsků dojde k poplachu.

Infrazávory pracují často v pulzním režimu a jsou vyhřívané pro eliminaci nežádoucích vlivů. Navazující úseky se musí překrývat, aby se nevyskytovaly mrtvé zóny. Rizikovými faktory jsou zejména mlha a padající sníh. Prakticky použitelný dosah je 50 až 150 metrů.

Příkladem infrazávory může být sloupová infrazávora MAXIRIS 2000, dosah 100/500 m (venkovní/ vnitřní), 2x6Tx, výstup relé/sběrnice BUS, vyhřívání, napájení 230V, výška sloupu 2,5 m.



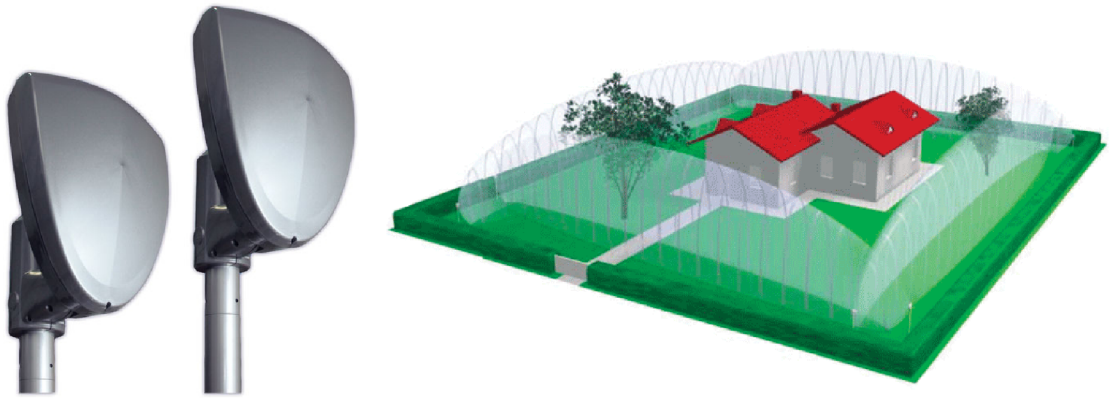
Obrázek 4.11: Sloupová infrazávora MAXIS 2000.

4.3.3 Mikrovlnné bariéry

Princip těchto bariér je založený na vytvoření elektromagnetického pole mezi vysílačem a přijímačem. Přijímač detekuje porušení elektromagnetického pole vniknutím objektu. Mikrovlnný svazek je modulován pro vyšší odolnost proti rušení cizími elektromagnetickými zdroji.

Typický tvar mikrovlnného svazku je elipsoid s výrazným poměrem velké a malé osy. Výhoda těchto bariér je velký dosah 200 až 300 metrů a vysoká odolnost vůči povětrnostním vlivům. Ve střeženém prostoru se nesmí nacházet pohybující se předměty jako větve stromů, keře apod.

Zástupcem mikrovlnných bariér je například Cias Coral 220, dosah až 220 m, pracovní frekvence 9,2 – 10,6 GHz, 16 kanálů, zálohovací baterie [7].



Obrázek 4.12: Mikrovlnná bariéra Cias Coral 220, příklad použití.

4.3.4 Štěrbinové kabely

Speciálně upravený koaxiální kabel, instalován většinou jako pár v daném rozestupu. Ve stínění jsou daným způsobem rozmístěny štěrbiny. Jeden kabel vyzařuje elektromagnetické pole a druhý detekuje případné změny vytvořené narušením.

Tento typ perimetrické ochrany je vhodný zejména pro schopnost kopírovat povrch terénu. Délka jednoho úseku může být až 200 metrů. Tyto systémy jsou citlivé na pohyb zvěře.

4.3.5 Zemní tlakové hadice

Jde o diferenciální tlakové čidlo, které je založené na dvou paralelně uložených hadicích ve vzdálenosti cca 1 metr po celém obvodu pozemku. Nemrznoucí kapalina v hadicích slouží k přenosu změn tlaku vyvolaným vnějšími vlivy. Změny tlaku jsou vyhodnocovány v diferenciálním tlakovém čidle, které je převádí na elektrický signál. Délka jednoho úseku může být až 200 metrů. Lze použít i pod tvrdé povrchy například vozovky či beton. Nejsou ovlivňovány elektromagnetickými poli.

4.3.6 Další systémy venkovního zabezpečení

Perimetrická pasivní infračervená čidla, infrateleskopy, jsou principielně shodná s PIR uvedenými výše, jen přizpůsobeny provozu v exteriérech (čočky, odolné a vyhřívané konstrukce). Typický dosah je 150 metrů, ale konec není explicitně dán, proto musíme zajistit, aby nedetekovali mimo střežený pozemek.

Existují i další systémy založené například detekci pomocí rotujících laserů, nebo vplétání optických vláken do pletiva. V současné době se čím dál víc rozšiřuje detekce pomocí kamer a zpracování pomocí výpočetní techniky.

4.4 Ústředny EZS

Ústředna elektrické zabezpečovací signalizace je centrální jednotka, která má následující funkce:

- přijímá a vyhodnocuje výstupní signály od čidel EZS,
- ovládá signalizační, přenosová, zapisovací a jiná připojená zařízení,
- napájení čidel a dalších prvků EZS,
- uvádění celého systému EZS nebo jeho části do stavu střežení či klidu,
- umožňuje diagnostiku stavu systému EZS.

4.4.1 Rozdělení ústředen

4.4.1.1 Smyčkové ústředny

Pro každou poplachovou smyčku má ústředna vstupní vyhodnocovací obvod. Smyčka je zakončena předepsaným odporem, a změna odporu na smyčce znamená aktivaci čidla či sabotážní smyčky a tím vyhlášení poplachu. Poplachové smyčky systému jsou nejčastěji tvořeny sériovým zapojením rozpínacích kontaktů čidel.

Nevýhodou těchto ústředen je poměrně rozsáhlá kabelová síť. Ke každému čidlu vede kabel příslušné smyčky, ve kterém musí být dva napájecí vodiče, dva vodiče pro poplachový kontakt, dva pro sabotážní kontakt a další pro přidružené funkce jako je paměť poplachu, antimasking či odpojení vysílače MW/US detektorů [1].

4.4.1.2 Ústředna s přímou adresací čidel

U těchto ústředen je komunikace mezi ústřednou a čidly po datové sběrnici. Ústředna periodicky generuje adresy jednotlivých čidel a přijímá odezvy. Každé čidlo má komunikační modul a může jich být na sběrnici řádově desítky. Obvykle se využívá vedení se čtyřmi vodiči (2 napájení, 2 sběrnice).

Velkou výhodou je, že při poplachu je známo které čidlo jej vyvolalo a z jakého důvodu. Vedení může mít řádově stovky metrů, ale kvůli jednoduchosti je nemožná realizace některých doplňkových funkcí čidel.

4.4.1.3 Smíšené ústředny

Komunikace těchto ústředen je kombinovaná, mezi ústřednou a koncentrátorem je komunikace datová, koncentrátory jsou s čidly propojeny smyčkami. Modelů pro vyhodnocování je více. Jedním je využití analogového multiplexu, v tomto případě se na sběrnici připojují postupně jednotlivé smyčky a vyhodnocování provádí ústředna. Jinou možností je provádět vyhodnocení v koncentrátorech a vybavit je vyrovnávací pamětí, další komunikace je už jen datová. Připojíme-li čidla přímo na vstupy koncentrátorů, vznikne plně adresovatelný systém se všemi výhodami.

4.4.1.4 Ústředny s bezdrátovým přenosem

Tyto ústředny umožňují bezdrátovou komunikaci s čidly, většinou v pásmu telemetrie, tj. 433 MHz. Komunikace bývá 8bitová s 4bitovou adresou vzdáleného senzoru. Dosah těchto ústředen se uvádí ve volném prostoru cca 100 až 200 metrů.

Hlavními výhodami bezdrátových ústředen jsou: rychlá a snadná instalace, možnost instalace do hotových objektů bez stavebních prací, snadné rozšiřování o další prvky a snadná změna konfigurace čidel.

Komunikace mezi ústřednou a detektory může být buď jednosměrná, nebo obousměrná.

Jednosměrná komunikace se využívá u jednodušších systémů. Zde je v detektoru umístěn vysílač, který periodicky vysílá do ústředny informace o střežení. Čidlo nemá žádnou odezvu z ústředny ani informace jestli je systém ve stavu střežení či nikoli. Z tohoto důvodu jsou čidla energeticky náročná, a aby se spotřeba snížila, využívá se delší doba mezi „hlášeními“. Ale tím vzniká prodleva, ve které ústředna neví co se děje. V případě komunikace tohoto typu je relativně snadné zjistit frekvenci a modulaci, kterou systém využívá.

V případě obousměrné (duplexní) komunikace jsou všechny prvky vybaveny moduly přijímač-vysílač. Tyto moduly mají integrovanou určitou logiku, která umožňuje automaticky naladit na volné a nezarušené kanály v dostupném frekvenčním pásmu, případně i přeladit tyto kanály. Duplexní komunikace vyřešila většinu problému jednosměrné komunikace. Hlavními přednostmi je kontrola stavu všech prvků při zapnutí systému, čidla v klidovém stavu nevysílají (tedy neplýtvají energií) a mají schopnost automatického přeladění při rušení.

Důležité je i kódování komunikace a adresace jednotlivých prvků. U jednodušších systémů se kódování realizuje naprogramováním přepínačů, u sofistikovanějších systémů mají prvky z výroby dán svůj jedinečný kód, který se zaznamená v ústředně.

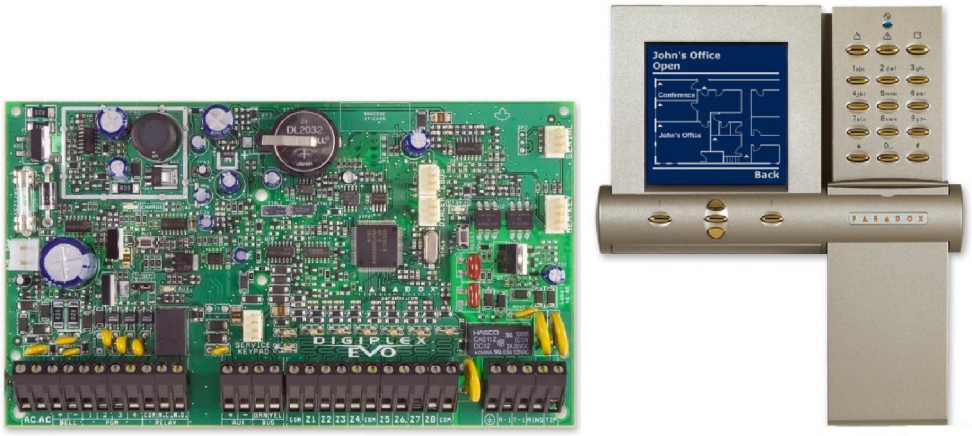
V bezdrátových verzích se vyrábějí například čidla pohybu, tísňová tlačítka, magnetické kontakty, sirény, různé ovládací prvky a univerzální moduly pro připojení libovolných čidel.

4.4.1.5 Příklad ústředny a přidružených prvků

Ústředna z nabídky PARADOX DIGIPLEX EVO-192 vhodná i pro velké objekty, se zabudovaným systémem pro kontrolu přístupu. Možno rozšířit o bezdrátovou či hlasovou nástavbu.

Parametry a funkce:

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



Obrázek 4.13: Ústředna PARADOX DIGIPLEX EVO-192, možná klávesnice.

4.5 Signalizace a doplňková zařízení EZS

Nejčastěji instalovaným doplňkovým zařízením k ústřednám jsou akustická signalizační zařízení tj. sirény, optická (vizuální) signalizace a GSM či jiné komunikační moduly. U větších systémů se využívají tzv. grafická tabla, což jsou panely s vyznačenými plány objektu a v nich indikační prvky schopné zobrazit místo případně i způsob narušení.

4.5.1 Interiérové sirény

Vnitřní sirény mají vysoký pronikavý zvuk a jejich hlavním cílem je odradit pachatele. Ze zkušenosti vyplývá, že pokud je pachatel překvapen ječivým zvukem sirény, ve většině případů se dá okamžitě na útěk. Doba signalizace by měla být omezena.

4.5.2 Venkovní sirény

Tyto sirény mají za úkol v případě poplachu upozornit okolí na výjimečný stav. K tomu účelu bývá výkonná siréna doplněna intenzivní optickou signalizací. Často se integruje akumulátor k zajištění funkce při přerušení napájení. Obecně je doporučována oranžová barva.

5 Systémy průmyslové televize

Systém průmyslové televize (CCTV) je někdy nazýván jako kamerový systém. Využívá snímání okolí pomocí kamer, u kterých se konstrukčně vychází z analogie s lidským okem a využívá jeho nedokonalostí.

Z těchto nedokonalostí vychází frekvence splývání 50 Hz, což je minimální počet snímků za sekundu takový, aby vjem byl bez blikání. Ve spojení s 625 řádky úplného TV snímku vychází šířka kmitočtového pásma 13 MHz. Což je velmi vysoká hodnota při současných technologických podmínkách. Díky rozdělení každého snímku na dva, tj. na zobrazení lichých a následně sudých řádků došlo k poloviční náročnosti, tj. 6,5 MHz. Standardy udávají mnoho parametrů, jako jsou řádkový kmitočet, doby zatemňovacích pulzů, šířka pásma videosignálu, výkonový poměr obraz/zvuk a jiné. Standardů existuje více, u nás a ve většině Evropy je používán standard CCIR.

Bez ohledu na typ normy byly vyvinuty tři základní systémy pro přenos barevného signálu. NTSC (National Television Systém Comittee) vytvořen v USA, SECAM (Sequentiel á mémoire) vynalezen ve Francii a PAL (Phase Alternatin Line) v SRN. Ve všech případech je zachována kompatibilita s černobílými systémy. Tři barevné složky jsou přenášeny v podobě rozdílových signálů spolu s jasovou složkou. Principielně stačí přenášet pouze dvě tyto složky a třetí může být matematicky dopočítána. Pro barevnou CCTV se v Evropě používá systém PAL [1].

5.1 Snímání obrazu

Scéna v zorném poli kamery musí být opticky transformována do roviny světlocitlivé plochy snímacího prvku a musí být převedena na elektrický signál. Pro tento převod se v současné době využívají až na výjimky polovodičové struktury CCD čipu. Dříve se využívaly snímací elektronky, ale ty jsou dnes určené jen pro speciální aplikace, jako je primární zóna jaderných elektráren. V následujících odstavcích budou popsány základní vlastnosti kamer využívaných v CCTV.

Základní vlastností kamer je jejich rozlišovací schopnost, což je hranice ostrosti snímané scény. Hlavním kritériem je počet obrazových bodů (pixelů) na čipu CCD. Rozlišení se udává v počtu řádků či počtu pixelů. Maximální rozlišení dle standardu CCIR je 625 řádků, z toho 575 viditelných a formát obrazu 4:3. Při digitálním zpracování je nutné, při zachování stejného rozlišení ve vertikálním směru, 767 obrazových bodů. Což dává celkové rozlišení 767x575 = 441 025 pixelů. S rozlišovací schopností úzce souvisí paměťová náročnost na snímek. V případě 256 odstínů šedé je to 3,5 Mb a pro barevný obraz s 1024 odstíny 8,8 Mb [8].

Jedním z nejdůležitějších parametrů u kamer je jejich citlivost. Je to údaj o minimálním osvětlení v luxech (lx), při kterém je na výstupu kamery signál o amplitudě rovné 50% jmenovité hodnoty. Jde o intenzitu světla odraženého od daného objektu měřenou na objektivu kamery.

V současné době existují kamery, které s přisvícením v infračerveném spektru dokáží snímat i při osvětlení 0 lx.

Velmi podstatným aspektem s vlivem na konečný výsledek je odstup signál/šum. Každý pracující elektronický obvod je zdrojem šumového napětí, to se následně superponuje na užitečný signál a při zpracování videosignálu se projeví jako zrnitost či padající sníh v obraze. Interference vzniká i z jiných externích zdrojů jako je elektrické vedení či datové kabely. Obvykle se tento jev zvyšuje se snižující se úrovní osvětlení snímané scény. Nejdříve se projeví jako zrnitost v obraze, která se následně zhoršuje a na obraze se projeví jako sněžení, posléze se obraz natolik zhorší, že se stane nepoužitelným. Pro výpočet se udává vzorec B = 20 x log (videosignál/šumový signál). Výsledek je udán v decibelech (dB). Na úrovni 60 dB tj. poměr signál/šum je 1000:1 je obraz výborný s neznatelným množstvím šumu. Při 40 dB (poměr 100:1) se ztrácejí detaily a je viditelný šum a při 30 dB (32:1) je již špatný obraz s výrazným šumem [8].

Postupem vývoje se do kamer integrují různé doplňkové funkce jako elektronická uzávěrka, schopnost kompenzovat protisvětlo, nastavení vyvážení bílé či digitální rozhraní pro nastavování parametrů při snímání.

Ke kamerám se připojují objektivy, u kterých jsou důležitými vlastnostmi zejména ohnisková vzdálenost, zde se volí mezi objektivy s pevnou a pohyblivou ohniskovou vzdáleností a rozsah nastavení clony. Obě tyto vlastnosti mohou být regulovány ručně nebo motoricky. Také spolu s kvalitou optiky mají vliv na optickou ostrost, což je subjektivně definovaný rozsah, kdy jsou detaily u snímaných objektů ještě ostré.

Mezi příslušenství kamer v této oblasti patří zejména kryty, ať už miniaturní či určené proti vlhku, prachu, do venkovních podmínek se slunečními štíty a vyhříváním či odolnými vůči úmyslnému poškození. Dále také systémy pro vzdálené řízení funkcí těchto kamer.

5.2 Přenos videosignálu

Největším problémem v oblasti přenosu signálu je útlum při přenosu a z toho vycházející výběr vhodné varianty média. V současné době máme na výběr koaxiální či symetrické vedení, bezdrátový přenos a přenos po optických vláknech.

Přenos po koaxiálním kabelu s plnou rozlišovací schopností vyžaduje šířku přenosového pásma 6,5 MHz. Délka vedení je omezena úbytkem signálu podél vedení, které je dáno parametry použitého kabelu. Každý koncový bod musí mít charakteristickou impedanci 75 Ω. Tento druh kabeláže lze použít pro přenos na vzdálenost řádově stovky metrů, při použití korekčních videozesilovačů až jednotky kilometrů.

Druhou možností přenosu po metalických kabelech je využití dvoudrátového systému. Zde lze využít i nevyužité páry ve víceżilových rozvodech. Nevýhodou je nutnost použít převaděče na obou stranách vedení, které převedou nesymetrický 75 Ω signál na symetrický a naopak. Velkou předností

oproti koaxiálnímu vedení je vyšší odolnost proti rušení vnějšími elektromagnetickými poli. Což je jeden z důvodů umožňující délku vedení až cca 2,5 kilometru.

Variantu bezdrátového přenosu je možné realizovat pomocí směrovaných spojů. Tento způsob přenosu je rozšířen v profesionální praxi pro přenos TV signálu z mobilních stanic na stacionární (např. přímý přenos z terénu). Zde lze využít modulace signálů na subnosné frekvence pro vícekanálový přenos. Do této kategorie můžeme zařadit i optický přenos pomocí modulovaných laserů. Toho se využívá pro překlenutí určitého území (až stovky metrů), kde z nějakého důvodu není možné vybudovat závěsné ani pozemní vedení.

V poslední době nabývá na významu přenos po optickém kabelu. Hlavními výhodami je v podstatě nemožnost rušení, rychlost přenosu a dlouhý dosah. Bez průběžných optických zesilovačů až 4 kilometry a u profesionálních systémů až 100 km bez průběžného zesílení.

5.2.1 Přenos digitalizovaného videosignálu

Další možností jak přenášet obrazový signál je jej digitalizovat a přenášet v datové podobě po telefonních linkách, ISDN linkách, nebo jiných datových sítích.

Dodržíme-li standard CCIR, 25 snímků za sekundu a 10 bitů pro úroveň jasu a odstín barvy, dostáváme datový tok 220 Mb/s. Pokud vezmeme v úvahu běžné propustnosti současných sítí například: modem 56 kb/s, ISDN 64 kb/s až 2 Mb/s, sítě LAN 100 Mb/s případně 1 Gb/s, je zřejmé, že je nutné datový tok zredukovat, než bude transportován datovou sítí.

Z výše zmíněného důvodu je mimořádně důležitá komprese dat a tím snížení náročnosti na propustnost datové sítě. Všem postupům komprese videa je společné, že odstraňují redundantní a irelevantní informace z obrazu. Nadbytečné informace reprezentují sousední obrazové body s často stejným jasem a barevným odstínem. Efektivním algoritmem lze tyto redundantní informace odstranit bez vlivu na kvalitu obrazu. Zbytečné informace jsou takové, které pozorovatel není schopen postřehnout, nebo jsou mimo rozsah zájmu. Tyto úpravy však mohou vést po opětovném dekódování na vznik chyb tzv. artefaktů [8].

Často používanými standardy komprese videodat jsou:

- **M-JPEG** (Motion Joint Photographic Expert Group) – snadný přístup ke snímkům, vhodný pro archivaci, není standardizován, neobsahuje přenosový formát, algoritmus je založen na DCT (Discrete Cosines Transformation), který postupuje po jednom snímku,
- **MPEG** (Moving Pictures Expert Group) – využívá prostorovou a časovou redundanci, k níž dochází v obrazu, prediktivní algoritmy, konstantní kvalita obrazu,
- **H.261** – podmnožina telekomunikačního doporučení H.320 vydaných ITU pro kódování videosignálu, optimalizováno pro přenos po ISDN linkách, velký rozsah šířky pásma (64 až 1920 kb/s), rozlišení až 704 x 576, konstantní datový tok – vhodné pro přenos,

- **Wavelet** – založen na Fouriově transformaci, může být konstantní přenosová rychlost nebo kvalita obrazu, vynikající kvalita při kompresi 50:1, použitelný i při 80:1, vhodný jak pro přenos, tak pro archivaci.

5.3 Zobrazování, zpracování a záznam obrazu

Pro zobrazování snímané scény se využívají jak klasické CRT monitory či televize, tak v současné době LCD nebo plazmové panely. Pro zobrazení scén z více kamer je zapotřebí zařízení, které bude buď přepínat, nebo slučovat vstupy na výstupy.

Prvním prvkem, který umí zobrazit pohled z více kamer na jediný monitor je kamerový přepínač. Nedokáže ale tyto pohledy zobrazit současně, ale lze nastavit přepínání vstupů. Některé mají i poplachové vstupy, pomocí kterých je možné je propojit s EZS a řídit tak aktuální zobrazení.

Dalším rozšířením základního přepínače je kvadrantový selektor, ten dokáže na jednom monitoru zobrazit scény z více kamer najednou. Pracuje s digitalizací vstupních signálů a nejde tedy o zobrazení v reálném čase.

Multiplexery jsou zařízení, které umožňují realizaci multikamerových systémů s dokonalejším záznamem. Multiplexer je přímo spojen se záznamovým zařízením (videorekordérem) a spolupracuje s ním jak při záznamu, tak při přehrávání. Zaznamenává se po snímcích spolu s kódem pro každou kameru. Při přehrávání přebírá multiplexer roli dekodéru [8].

Všechna tato uvedená zařízení pracují většinou s maximálně 16 kamerami. Pokud bychom chtěli vytvořit větší systém s více kamerami a monitory musíme použít křížové přepínací pole. Tato zařízení pracují bez digitalizace tedy v reálném čase. Do velikosti cca 32 vstupů a 16 výstupů jsou řešena jako kompaktní zařízení s pevně daným hardwarem. Při požadavku na více vstupů či výstupů je systém modulární, tj. obsahuje centrální jednotku a k ní se přidávají moduly se vstupy a výstupy.

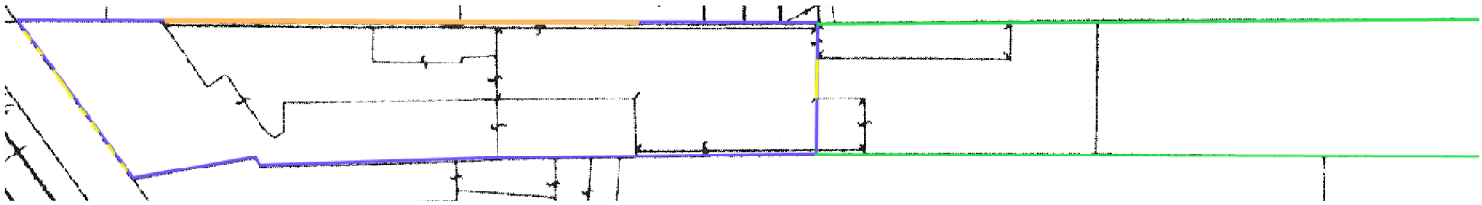
Záznam obrazu je důležitý k dokumentování dějů v, případně kolem zkoumaného objektu. V současnosti existují pro archivaci záznamů tři technické prostředky:

- **videorekordér s dlouhou dobou záznamu** – speciálně vyvinut pro CCTV, krom nahrávání v reálném čase dokáže nahrávat ve vzorkovacím režimu, který prodlužuje záznam na kazetu E 180 (3 hod.) podle nastavení na 24, 48, 72, 120, 168, 240, 480 až 960 hodin, pomocí poplachového vstupu může v případě potřeby změnit záznamový režim na záznam v reálném čase,
- **videotiskárna** – umožňuje převést videosignál do digitální podoby a tento pak vytisknout,
- **digitální záznam obrazu** – tato kategorie lze rozdělit na tři podskupiny, PC s rozšiřující kartou a příslušným softwarem, hardwarová zařízení na bázi PC, a čistě hardwarová záznamová zařízení například DSR od Sony.

6 Návrh zabezpečení objektu

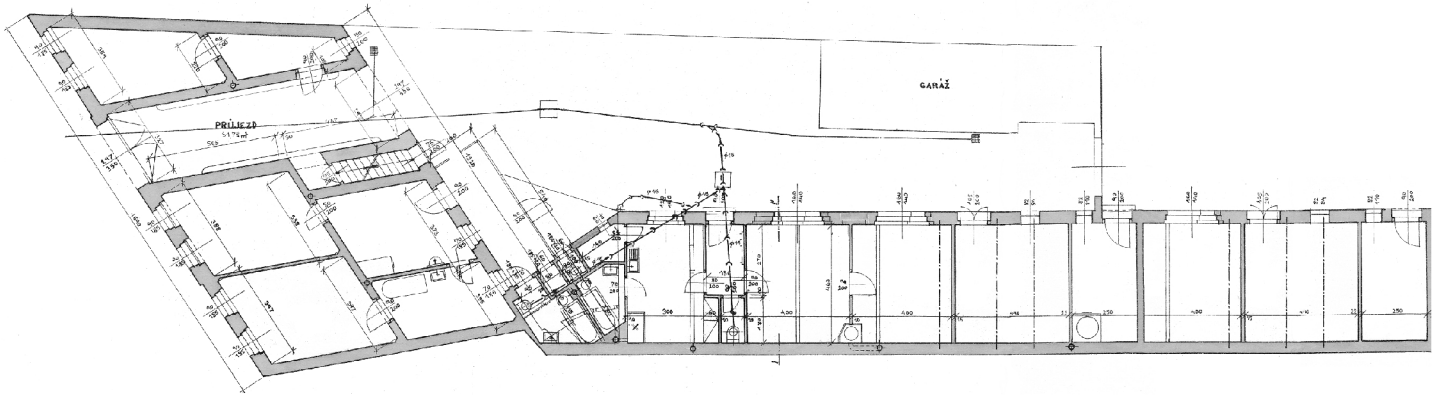
Zabezpečovací zařízení bude navrhováno na rodinný dům, který byl postaven na začátku 20. stolení jako malá zemědělská usedlost. Objekt od svého postavení nebyl ve větším měřítku rekonstruován až na malé změny převážně v interiéru. V současnosti je to jednopatrový řadový dům v zástavbě se zahradou a prvky zemědělské usedlosti, jako jsou velká zastřešená plocha či rozsáhlá půdní prostora volně přístupná zvenčí. Tento objekt je velice zajímavý a má i svoji historii.

Na následujícím obrázku je zjednodušeně technicky zakreslen celý pozemek a barevně je vyznačena zastavěná plocha (modrá barva), plocha zahrady (zelená), vstupní otvory (žlutá) a také je zde znázorněna část (oranžová), kde je zeď do výšky cca 2,5 m.



Obrázek 6.1: Zjednodušený technický výkres pozemku.

Zde je technický plán vlastního objektu podrobněji.



Obrázek 6.2: Zjednodušený technický výkres objektu.

Návrh bude vycházet ze současných technologických možností a bude rozdělen do dvou nezávislých částí, jedna bude založena na využití výpočetní techniky a kamerového systému a druhá bude využívat klasický systém EZS, tedy ústřednu a k ní připojená čidla a signalizační prvky.

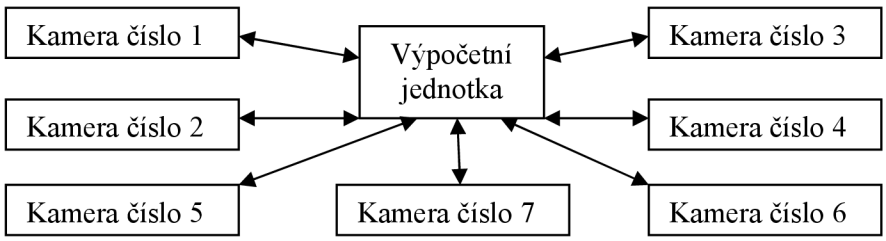
6.1 Návrh kamerového systému

Jako výpočetní centrum v tomto návrhu by mohl sloužit libovolný, dnes prodávaný, počítač s volným PCI slotem (případně více sloty podle požadavku na počet kamer) pro rozšiřující kartu a dostatečným diskovým prostorem pro záznam. Rozšiřující karta zde slouží jako vstup video případně i audio

signálu. Z důvodu spolehlivosti, možnosti rozšíření, víceúčelovosti a potřeby mít dostatečný výkon je dobré zvolit jeden ze základních serverů, např. HP Proliant ML150G3, ten poskytuje možnost připojení systému až 4 rozšiřujících karet (většinou až 16 kamer). Při použití serveru s operačním systémem MS Windows Server můžeme využít tento server krom monitorovací a nahrávací činnosti také jako doménový řadič a poštovní server ve vlastní síti. Dále v této části bude toto centrum označováno jako výpočetní jednotka.

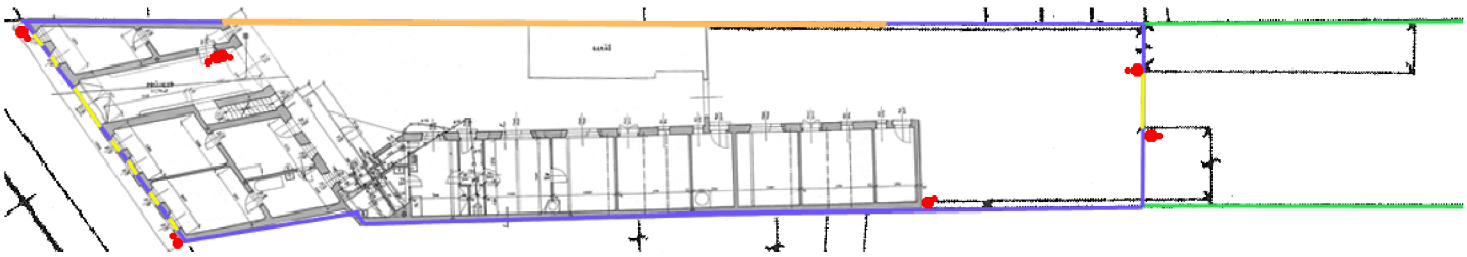
V této koncepci můžeme využít i jiné, obecnější principy komunikace, a to využití například protokolu IP. Pokud bychom využili kamery komunikující prostřednictvím IP, ať už prostřednictvím jakéhokoli nižšího protokolu (ethernet, wifi apod.), nebudeme potřebovat žádné rozšiřující karty. Toto lze využít při již vybudované rychlé lokální síti. Nevýhodami jsou zejména zálohování síťových prvků, zatížení sítě a další problémy z toho vyplývající jako nutnost řízení QoS apod. Touto variantou se zde nebudeme dále zabývat.

6.1.1 Blokové schéma systému a rozmístění kamer



Obrázek 6.3: Blokový diagram návrhu kamerového systému.

Počet a rozmístění kamer může být různé i vzhledem k tomu, kterou část objektu chceme nejvíce chránit či sledovat pohyb kolem ní. Jedno z možných rozmístění je zobrazeno na následujícím obrázku. Kamer je sedm a jsou zobrazeny jako červené tečky se zvýrazněnou orientací.



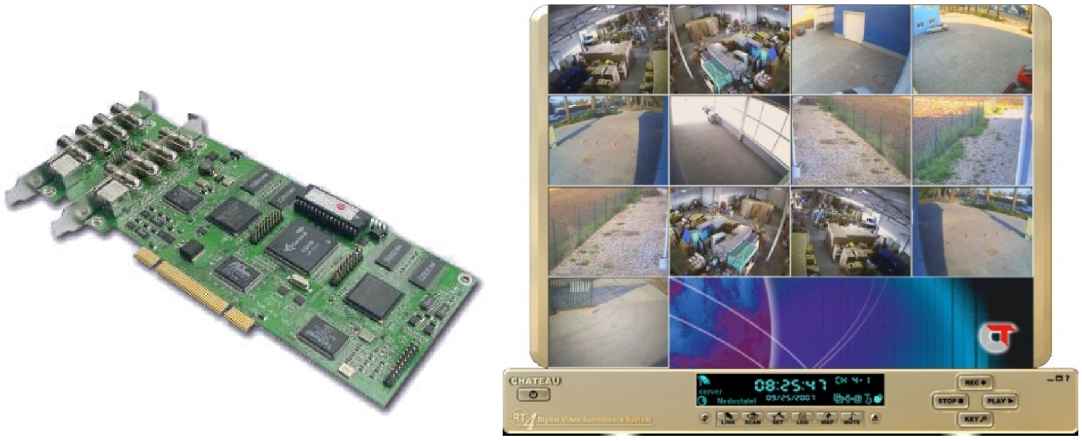
Obrázek 6.4: Pozice kamer na pozemku.

Pozice kamer byly zvoleny tak, aby veškerá možná místa vstupu byla pod jejich zorným úhlem. Pokud by se použili kamery s natáčením, byl by pokryt celý prostor pozemku.

6.1.2 Příklady produktů pro případnou realizaci návrhu

Jako výpočetní jednotku můžeme zvolit (jak bylo psáno výše) například server HP Proliant ML150 G3, nebo libovolný dnes prodávaný počítač. Podmínkou je pouze jeden či více volných PCI slotů.

Jako rozšiřující kartu můžeme použít Chateau V-GUARD 8RT4 pro 8 kamer a 8 audio kanálů (4 vstupy na kartě, 4 na přídavném modulu). Umožňuje zaznamenávat i on-line sledovat v rozlišení až 704x576 a lze volit kvalitu i rozlišení, rychlost 25snímků/s každá kamera. Různé druhy a úrovně komprese MPEG4, SMICT. Detekce pohybu v obraze, akustický alarm, vzdálený přístup pod heslem buď po místní síti, nebo přes internet, funkce WEB kamer, funkce prerecording (zaznamená i místo, než vznikne pohyb v obraze), ovládání otočných kamer. Možnost maskování části obrazu kvůli detekci pohybu (silnice v pozadí, strom ve větru), možnost odeslání snímků na zadaný e-mail při pohybu v určené zóně. Připojení video přes BNC, audio přes CINCH. Potřebný diskový prostor je cca 1-7 MB/min záznamu podle okolních podmínek v maximální kvalitě v kódování H.264. Dodávaný software ChateauXP umožňuje lokální ovládání a nastavení kamer, ChateauXPServer je centrální síťová aplikace, ke které lze přistupovat jako klient [6].



Obrázek 6.5: Rozšiřující karta Chateau V-GUARD 8RT4 a ukázka softwaru.

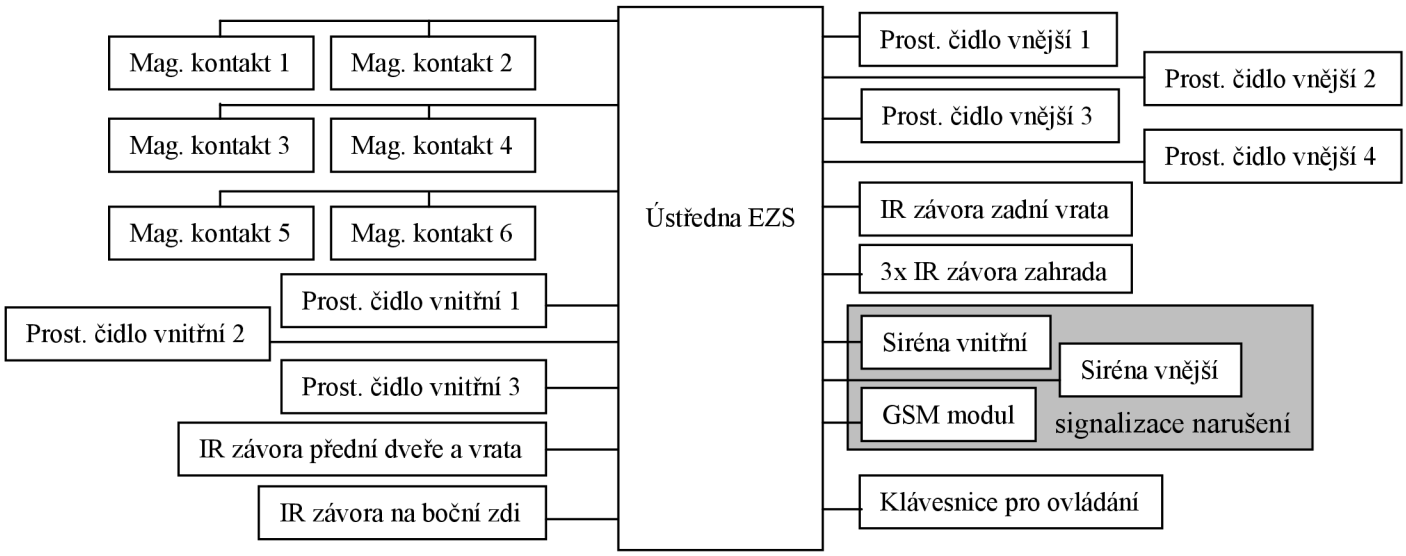
Možnost výběru kamer je široký počínaje černobílými modely a konče barevnými s nočním viděním, natáčením a možností nastavení ohniska. V tomto případě by mohly být využity barevné s infračerveným přisvícením v noci. Tři s proměnným ohniskem Hires IR-50 rozlišení 752x582 se snímači Sony SUPER HAD CCD, snímání od 0 Lux s přisvícením až 50 metrů. A tři s pevným ohniskem Hires IR-40 se stejnými parametry a dosvitem 40 metrů.

Obrázek 6.6: Kamery Hires IR-50 a IR-40.

6.2 Návrh tradičního systému EZS

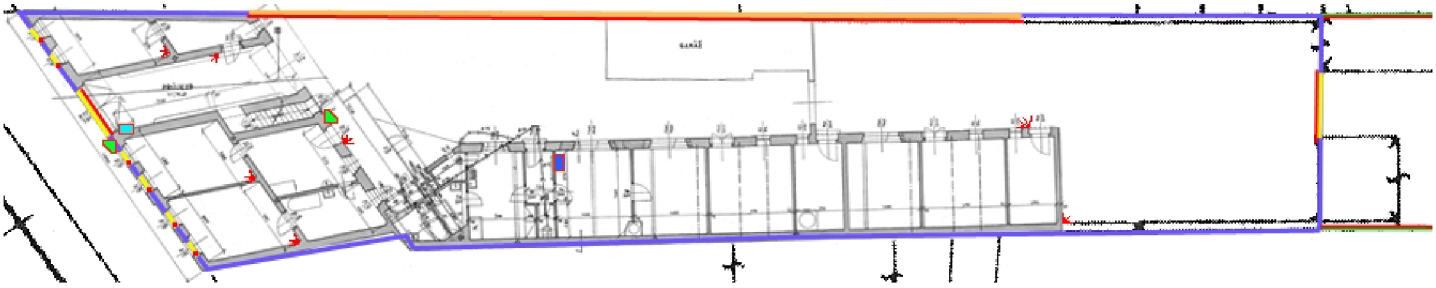
Tento návrh využívá určitou volnost, která je dána tím, že případná realizace bude prováděna v rámci větší rekonstrukce celého objektu. Základem bude ústředna, ke které budou připojeny magnetické kontakty, senzory pohybu, infračervené závory, vnitřní a venkovní siréna, GSM modul pro informování o narušení a přídavná klávesnice pro ovládání celého systému.

6.2.1 Blokové schéma systému a rozmístění prvků



Obrázek 6.7: Blokový diagram návrhu systému EZS.

Na následujícím obrázku je mapa objektu, kde jsou znázorněna možná místa instalace jednotlivých prvků systému. Jsou zobrazeny převážně červenou barvou, magnetické kontakty čtvercem, IR závory úsečkou a prostorová čidla tečkou s naznačenou orientací. Vlastní ústředna by měla být umístěna na těžko dostupném místě pro narušitele, zde je naznačena jako modrý obdélník ohraničený červenou barvou a umístěna ve sklepních prostorách. Přídavná klávesnice pro aktivaci a deaktivaci systému by měla být umístěna poblíž vstupních dveří, na obrázku je vyobrazena jako světlomodrý obdélník ohraničený červenou barvou. Vnější siréna by měla být umístěna tak, aby byla vidět z prostředí před domem a upozorňovala okolí na výjimečný stav. Pozice vnější i vnitřní sirény jsou naznačeny zeleně s červeným ohraničením.



Obrázek 6.8: Mapa objektu s vyznačenými místy instalace jednotlivých senzorů.

6.2.2 Příklady produktů pro případnou realizaci návrhu

Celý systém EZS může být založen na systému Dominus-Millennium firmy Spelza. Konkrétně můžeme zvolit ústřednou MU1, která má jednu linku pro až 32 rozšiřujících modulů, 2 sériová rozhraní RS232 pro připojení PC nebo komunikátoru, 1 paralelní port pro připojení tiskárny, 8 bezpotenciálových a 8 dvojitě vyvážených vstupů, lze definovat 400 podsystémů, počet položek historie, neomezený počet uživatelských kódů atd. V našem případě je ještě nutno doplnit o rozšiřující modul MM1-8NO pro dostatečný počet vstupů a výstupů. Součástí dodávky s ústřednou je i odpovídající napájecí zdroj a záložní akumulátor. To vše se instaluje do kovové schránky. Z tohoto systému použijeme i ovládací klávesnici MP4-GW s dvouřádkovým displejem a 9 indikačními diodami [13].

Interiérová prostorová čidla mohou být DSC Force F2, obsahují dvojitý detektor, ve kterém spolupracují mikrovlnný snímač s pasivním infračerveným senzorem pohybu. Činnost těchto senzorů je řízena pomocí mikroprocesoru, čímž je zajištěna určitá inteligentní detekce pohybu, která snižuje možnost vzniku falešných poplachů.

Ve venkovním prostření je detekce složitější, ale existují například detektory firmy Rokonet WatchOUT DT, které poskytují spolehlivou detekci ve venkovním prostoru. Používá výběrové rozpoznání událostí, které rozlišuje skutečné vniknutí do střeženého prostoru od planého poplachu v nestabilních venkovních podmínkách. Detektor vyhodnocuje 4 detekční kanály – 2 MW (mikrovlnné) kanály pro rozpoznání kymácejících se stromů, křoví apod. a 2 PIR kanály s oddělenými optikami a s eliminací zvířat do výšky 70 cm, rychlých teplotních změn a světelných odrazů.

Infrazávory je možné použít například PARADOX BRAND BP 40/60/150m podle potřebné délky pokrytí. Využívají třípaprskový systém se schopností eliminovat rušení způsobená pohybem malých zvířat (nezbytnou podmínkou pro aktivaci je současné narušení všech paprsků). Tvoří je vysílač a přijímač.

Pro signalizaci o narušení slouží GSM komunikátor jehož vstupy lze přímo připojit k programovatelným výstupům ústředen. Má dva reléové výstupy ovládané SMS zprávami, kterými je možné dálkově ovládat dvě různá zařízení. Dva nezávislé poplachové vstupy, předávání poplachů na 4 čísla voláním či SMS a možnost programování z PC. K tomuto komunikátoru je zapotřebí připojit ještě GSM duální anténu. Dalšími signalizačními prvky mohou být vnitřní siréna MINI 82 s 105 bB, a vnější Combell 3 s blikačem a záložním zdrojem [5].

Všechny prvky navrženého systému je ideální propojit pomocí 6 žilového kabelu FI-H06, ale lze využít i 4 žilový FI-H04. Pro propojení ústředny s rozšiřujícím modulem je určen 4+2 žilový kabel SUPERBUS AB01.

Programová podpora systému, na kterém je tento návrh postaven se skládá z několika konfiguračních a monitorovacích nástrojů. Program SetTermW umožňuje přehledně nastavit všechny

konfigurační parametry instalace, spravovat kompletní historii systému, archivovat veškeré informace (konfigurační, historie, obsah paměti) v otevřené i šifrované podobě, definovat uživatele, monitorovat a ovládat celý systém apod. vše v grafickém prostředí. Program HisTermW určený i koncovým zákazníkům pro kompletní správu historie událostí zahrnující filtraci i archivaci, synchronizaci času a definování uživatelů systému. Dále například PanTermW, který umožňuje centralizovaně z jednoho počítače monitorovat a ovládat systém pomocí simulování ovládacích prvků. K dispozici jsou i další užitečné nástroje [13].

Na následujícím obrázku jsou vyobrazeny prvky navrženého systému EZS.

Obrázek 6.9: Zleva vlastní ústředna, klávesnice, vnitřní a vnější detektory, infrazávora a venkovní siréna.

6.3 Výhody a nevýhody jednotlivých návrhů

Hlavní výhodou kamerového systému je možnost on-line monitorovat co se v objektu a jeho blízkém okolí děje a to nejen z vnitřní sítě, ale za pomoci internetu odkudkoli, tj. není to jednoúčelové zabezpečovací zařízení. Dále také možnost využít hardware, který už máme (počítač, server). Hlavní nevýhodou je energetická náročnost, každá kamera má vlastní napájecí zdroj, a tím je velmi problematické zálohování všech prvků při výpadku elektrické energie. Také problém správné detekce narušení není v současné době ještě na takové úrovni jako v případě klasického systému EZS.

Velkou výhodou klasického systému EZS je schopnost napájet všechny detektory přímo z ústředny, která je zálohována. A tudíž určitá elektrická soběstačnost a nezávislost na jiných systémech. Také se zde využívá sabotážní vodič pro případ přímého zničení čidel. Díky GSM modulu máme možnost určitého řízení systému na dálku.

Oba systémy lze rozšířit či změnit strukturu pomocí bezdrátových prvků, u kterých je jednodušší instalace bez nutnosti stavebních zásahů do objektu.

Celkově lze říci, že oba systémy lze využít pro střežení objektu, ale jejich funkce se částečně liší. V praxi lze tyto dva systémy kombinovat, respektive jeden doplňuje funkce druhého a naopak.

Další část bude věnována pouze klasickému zabezpečovacímu systému s ústřednou, k ní připojeným detektorům a signalizačním prvkům.

7 Model systému

V této části práce je uveden podrobný popis činnosti systému a jeho interakce s uživateli a okolím. Dále jsou uvedeny dva simulační nástroje Uppaal a Times Tool, které jsou schopny pracovat s časovými automaty, provádět jejich návrh, analýzu i verifikaci. Následuje implementace abstrakce modelu v modelačním nástroji Times Tool. Cílem této abstrakce, jakožto metody pro redukci stavového prostoru, je vytvoření abstraktního modelu systému, který bude mít menší složitost než reálný model.

7.1 Slovní specifikace funkce systému

Vstupní vrata a v nich integrované dveře jsou zabezpečeny pomocí infračervené závory, která signalizuje jejich otevření. Pokud je systém aktivován tímto prvkem, zahájí se odpočítávání časové prodlevy a zároveň přepne detektor pohybu v průjezdu do zpožděného režimu, během této doby je možné vložit bezpečnostní kód a systém vypnout, respektive přepnout do režimu nestřežení.

V průjezdu je detektor pohybu. Pokud zjistí pohyb ve střeženém prostoru, aniž by byly nejdříve otevřeny vstupní dveře či vrata, vyhlásí okamžitě poplach. Jsou-li nejprve otevřeny vstupní dveře a pak je teprve zjištěn pohyb, poskytne detektor nastavený čas na vypnutí bezpečnostního systému.

Ostatní detektory pohybu uvnitř místností, infračervená bariéra na boční zdi a infračervená závora u zadních vrat vyhlásí poplach okamžitě při zjištění pohybu ve střežených prostorách. Detektory pohybu ve volné vnitřní části objektu jsou vybavena maskovacími funkcemi a eliminací malých zvířat pro případ vlétnutí drobného ptactva či pohybu keřů a listí.

Všechna okna v přední části domu jsou opatřena magnetickými snímači uzavření, které vyvolají poplach ihned po otevření okna.

Infračervené závory instalované v zahradní části pozemku mají spíše informativní charakter a nezpůsobují rovnou poplach, ale jen stav zvýšeného rizika a na základě jejich podnětu se odešlou majiteli informace o způsobu narušení. Nemá smysl kvůli zakopnutému míči od sousedů hned vyhlašovat poplach.

Poplach je signalizován interní sirénou a externí zálohovanou sirénou, instalovanou tak, aby byla vidět z přilehlé komunikace.

Celý systém je řízen ústřednou, která je instalována v kovové krabici společně se záložním zdrojem, umístěné na zdi ve sklepení domu. Řídící ústředna je vybavena GSM komunikátorem, který umožňuje spojení s pultem centralizované ochrany dozorové bezpečnostní agentury. Je schopna zasílat informační SMS na zvolená čísla a provádět jednoduché akce na základě příchozích zpráv.

Pro ovládání je použita klávesnice s LCD displejem pro ovládání systému umístěná u vstupních vrat s dveřmi.

Bezpečnostní systém lze zapnout do stavu tzv. částečného střežení, i když je uživatel v objektu, například v noci. Ústředna automaticky odpojí detektory pohybu, takže je možné se po domě bez problémů pohybovat, ale jakmile někdo otevře střežené dveře, dojde k poplachu.

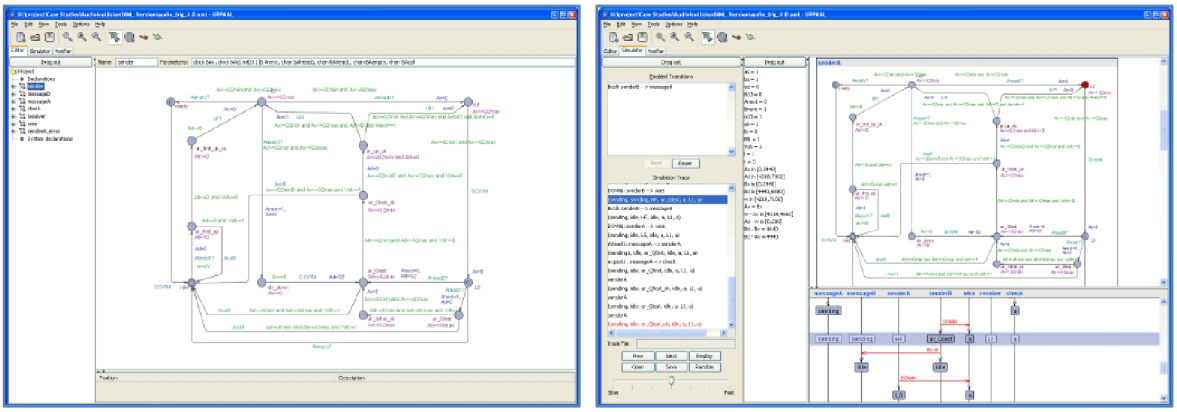
7.2 Simulační nástroje

7.2.1 Uppaal

Uppal je prostředí s integrovanými nástroji pro modelování, validaci a verifikaci systémů pracujících v reálném čase jako sítě časových automatů rozšířených o datové typy.

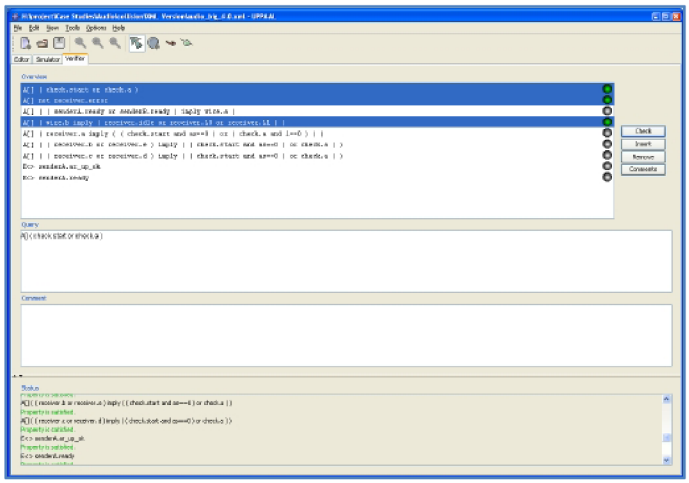
Je vhodný pro systémy, které mohou být modelovány jako kolekce nedeterministických procesů s konečnou strukturou řízení a reálným časem, komunikující přes kanály nebo sdílené proměnné. Typické využití zahrnuje kontroléry pracující v reálném čase a komunikační protokoly, kde je hledisko času kritické.

Uppaal se skládá ze tří hlavních částí: popisovací jazyk, simulátor a verifikátor. Popisovací jazyk je nedeterministický řídící jazyk s datovými typy. Slouží k návrhu modelu, popisu chování jako síťový automat rozšířený o čas a proměnné. Simulátor je validační nástroj, který umožňuje vidět dynamické vykonávání za běhu navrženého systému a umožňuje odstranění poruch před verifikací. Verifikátor umožňuje kontrolovat neměnné a dosažitelné vlastnosti zkoumáním stavového prostoru systému [9].



Obrázek 7.1: Uppaal návrhové a simulační okno.

Vývoj tohoto nástroje měl dvě hlavní kritéria a to efektivitu a snadnost použití. Aplikace využívá on-the-fly vyhledávací techniky, symbolickou techniku k redukci verifikačních problémů, generuje diagnostický strom při verifikačních dotazech, podle kterého lze nasimulovat tuto situaci.



Obrázek 7.2: Uppaal verifikační okno.

Nástroj je vyvinutý v spolupráci Fakulty informačních technologií na Uppsala University ve Švédsku a Fakulty počítačových věd v Aalborg University v Dánsku [9].

7.2.2 Times Tool

Times tool je množina nástrojů pro modelování a implementaci vestavěných systémů. V tomto programu lze modelovat, analyzovat plánování, provádět syntézy návrhů a generovat vykonavatelný kód. Je vhodný pro systémy, které lze popsat jako množiny úloh, které jsou spouštěny pravidelně, sporadicky, nebo na vnější podnět. V určitém směru je zde rozšíření oproti nástroji uvedenému výše.

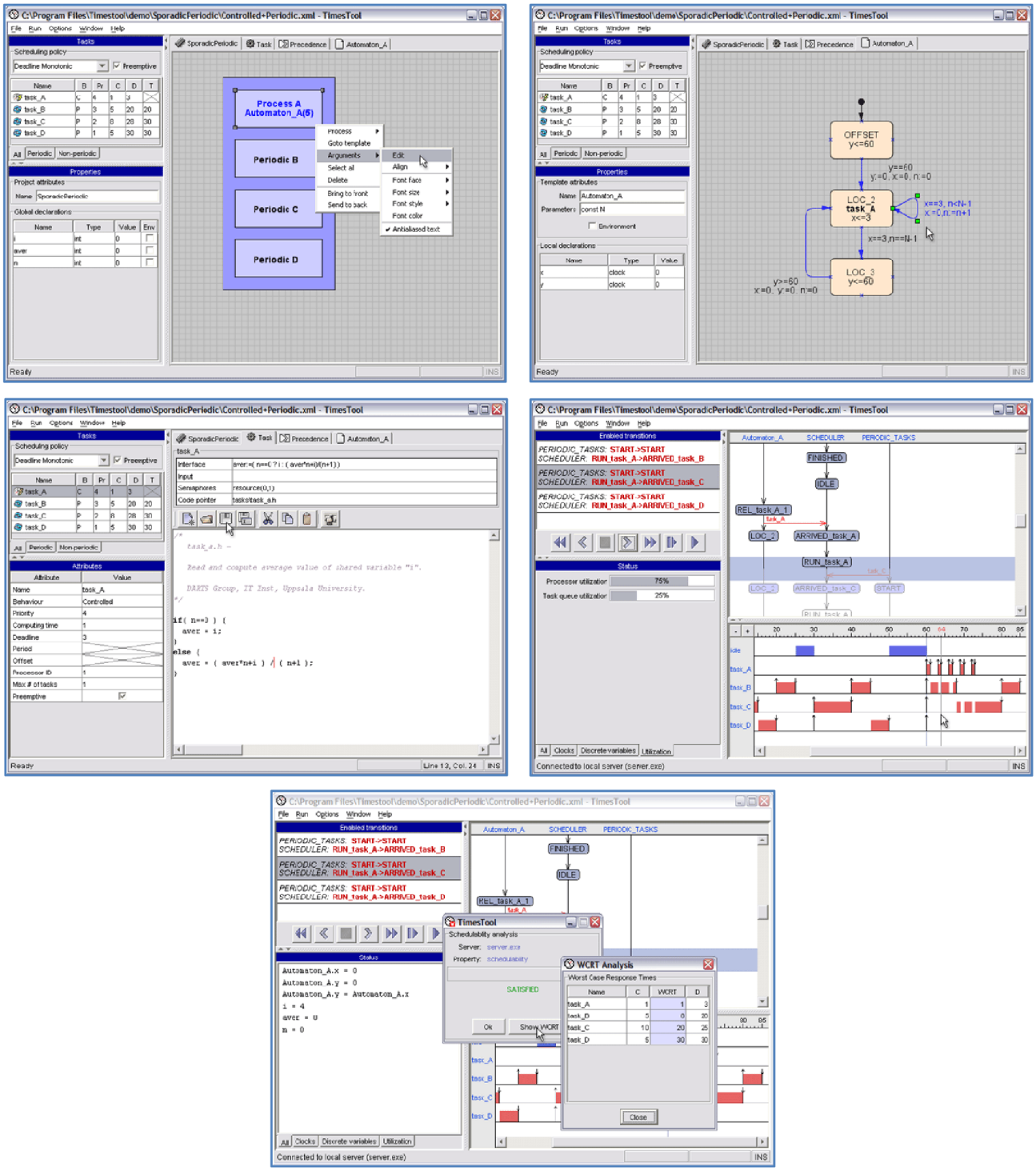
Specifikace systému se skládá ze tří částí: kontrolní automaty modelované jako síť časových automatů rozšířených o úlohy, tabuli úkolů, kde jsou informace o vydávání úkolů pomocí kontrolních automatů a plánovací politiku.

Jednotlivé nástroje:

- Grafický editor – vytváření časových automatů rozšířených o úkoly, které umožňují modelovat systém a abstrahovat chování jeho prostředí. Navíc lze definovat sadu preemptivních nebo nepreemptivních úkolů s parametry jako doba vykonání, hraniční doba vykonání, priorita, atd.
- Simulátor – zde lze ověřit dynamické chování systému a je viditelné, kdy jsou jednotlivé úlohy zpracovávány podle parametrů a dané plánovací politiky. Simulátor ukazuje grafickou reprezentaci generované posloupnosti úkonů, které jsou vidět v časových krocích.
- Verifikátor pro analýzu plánovatelnosti – používán pro kontrolu, zda všechny dosažitelné stavy systému jsou naplánovatelné včetně všech úloh, které musí být dokončeny do hraniční doby. Využívá symbolický algoritmus, což je základ DBM techniky, na které je verifikátor založen.

- Generátor kódu – automatická syntéza C kódu pro platformu LegoOS z modelu. Pokud je model naplánovatelný podle analýzy plánovatelnosti, bude vygenerovaný kód vykonatelný v hardwaru.

V současné době Times Tool podporuje specifikaci, systémovou analýzu a generování kódu pro LegoOS platformu [10].



Obrázek 7.3: Times Tool postupně projektový editor, editor pro časové automaty s úkoly, editor úkolů, simulátor a verifikace plánovatelnosti s WCRT analýzou.

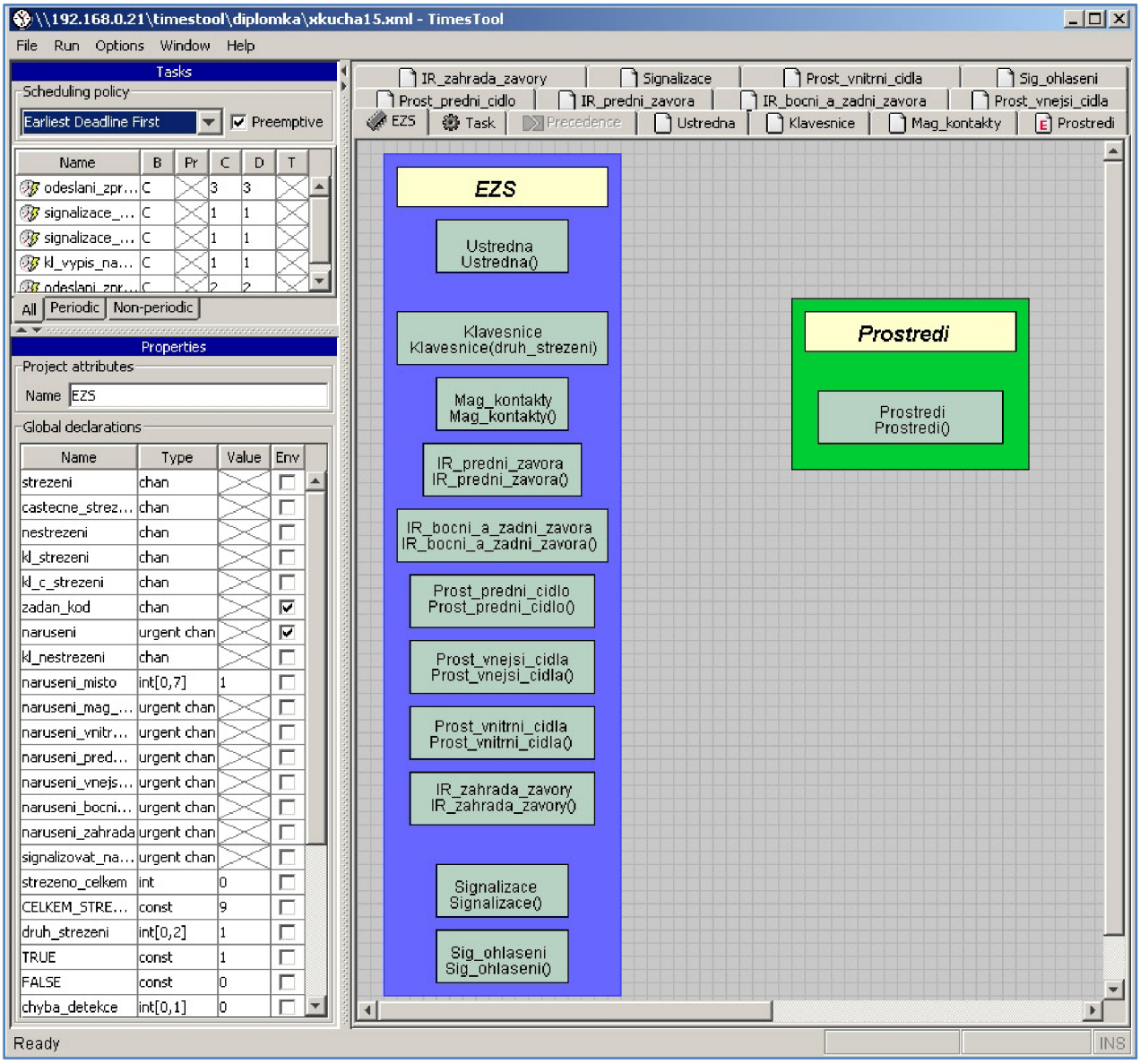
7.3 Implementace modelu systému

Pro implementaci modelu byl zvolen nástroj Times Tool v současné verzi 1.3 beta hlavně kvůli větším modelovacím schopnostem, i když je výrazně složitější než nástroj Uppaal.

7.3.1 Realizace jednotlivých částí systému

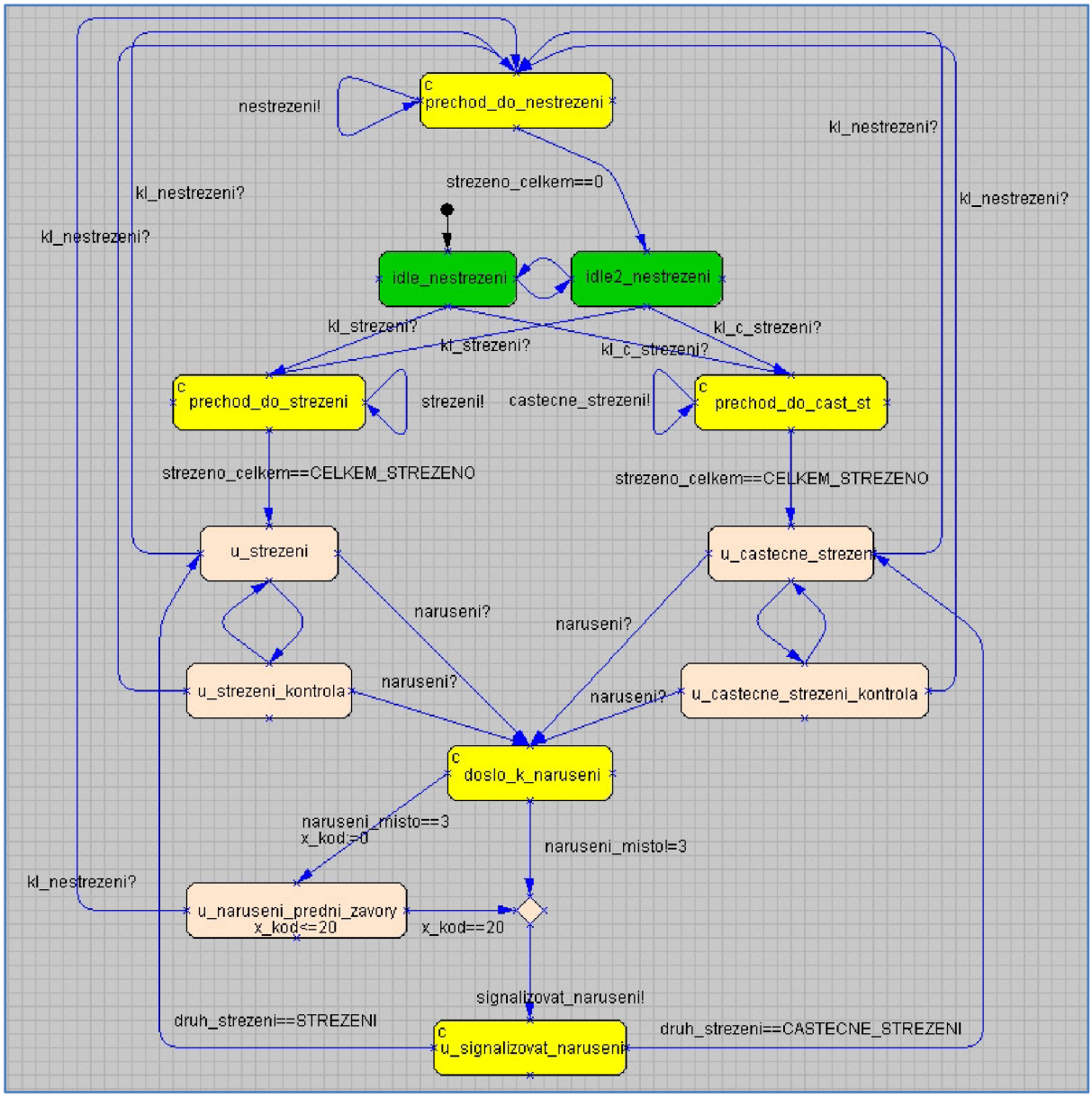
V této části bude podrobně rozebrán model, který byl vytvořen na základě slovní specifikace uvedené v části 7.1.

Na nejvyšší úrovni je model rozdělen do dvou částí, na vlastní EZS a na prostředí, pomocí kterého je modelováno příkladové chování vně EZS. Na následujícím obrázku je zobrazen celý projekt, tj. rozdělení na tyto dvě části a jaké procesy jsou v těchto částech zahrnuty.



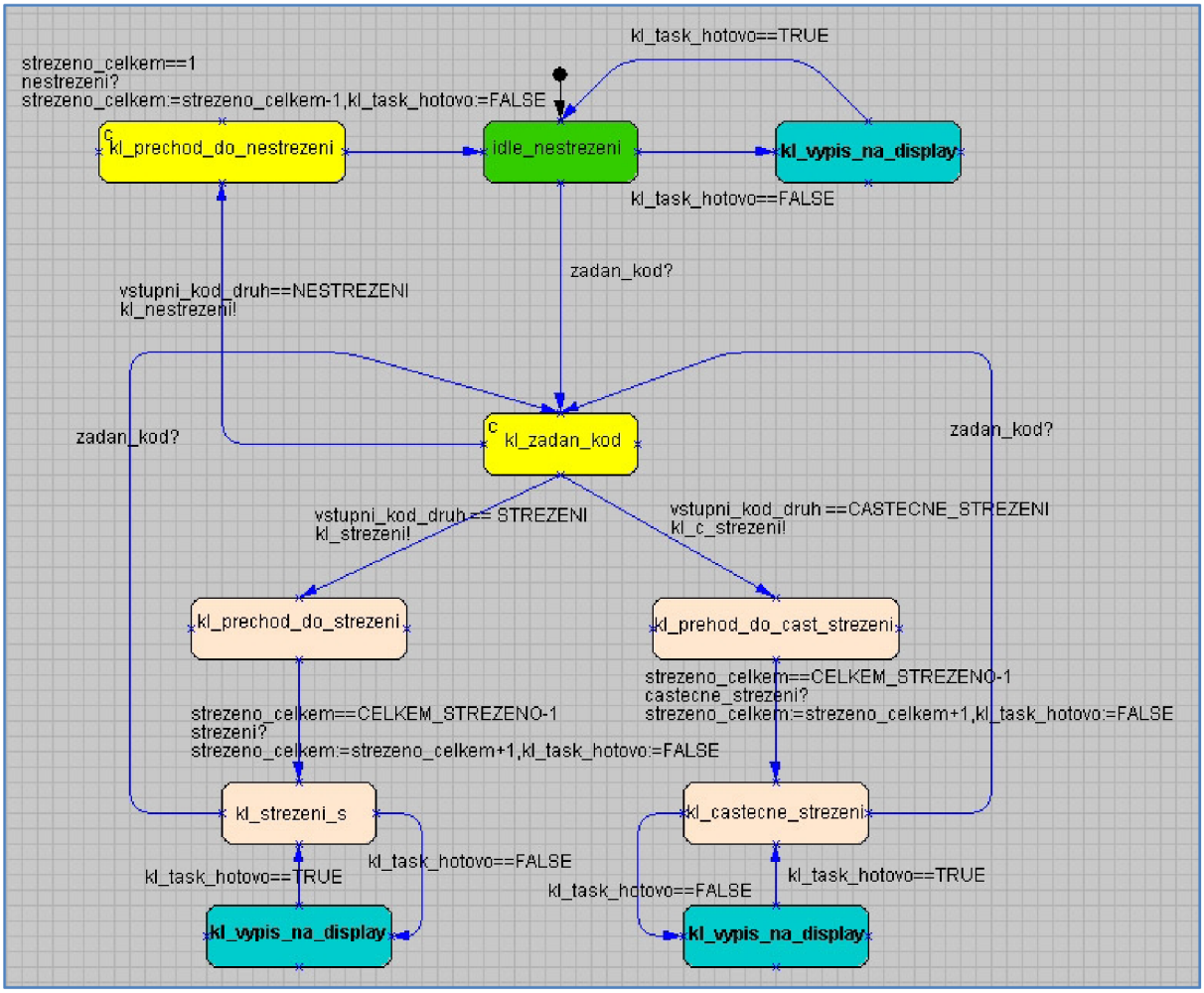
Obrázek 7.4: Rozvržení procesů v projektu.

Hlavním prvkem celého EZS je ústředna. Ta má za úkol řízení celého systému, přechody do stavů střežení, částečného střežení či nestřežení, vyhlášení poplachu jako reakci na narušení detekované čidly, atd. Komunikace mezi ústřednou, klávesnicí a čidly je provedena pomocí urgentních kanálů. Po zapnutí se ústředna a všechny součásti systému nacházejí ve stavu nestřežení. Pokud byl zadán kód vyjadřující, že se má přejít do stavu střežení, ústředna vyšle střežící signály ke všem čidlům a poté přejde do stavu střežení. Z tohoto stavu je možné vše odstřežit a přejít zpět do stavu nestřežení, nebo při narušení detekovat jestli došlo k narušení v přední části objektu (vstup) a má se umožnit zadání kódu, nebo rovnou začít signalizovat narušení. Na obrázku 7.5 je automat vyjadřující přesné chování ústředny.



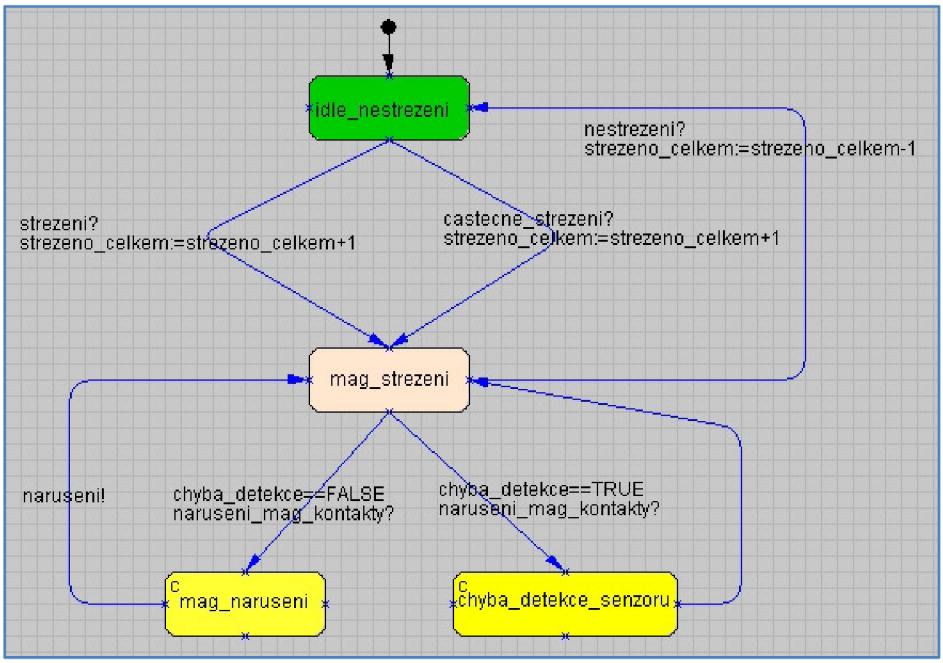
Obrázek 7.5: Automat vyjadřující chování ústředny.

Druhým velmi důležitým prvkem je ovládací klávesnice umístěná za vstupními vraty do objektu, a která umožňuje uživateli celý systém ovládat. Podle zadaného kódu umožňuje klávesnice přechody mezi stavy systému střežení, částečného střežení či nestřežení. Nestřežení je výchozí stav i této komponenty. Po zadání kódu a přechodu všech prvků do stavu střežení přejde i klávesnice do tohoto stavu a informuje uživatele o stavu systému na displeji.



Obrázek 7.6: Automat vyjadřující chování klávesnice.

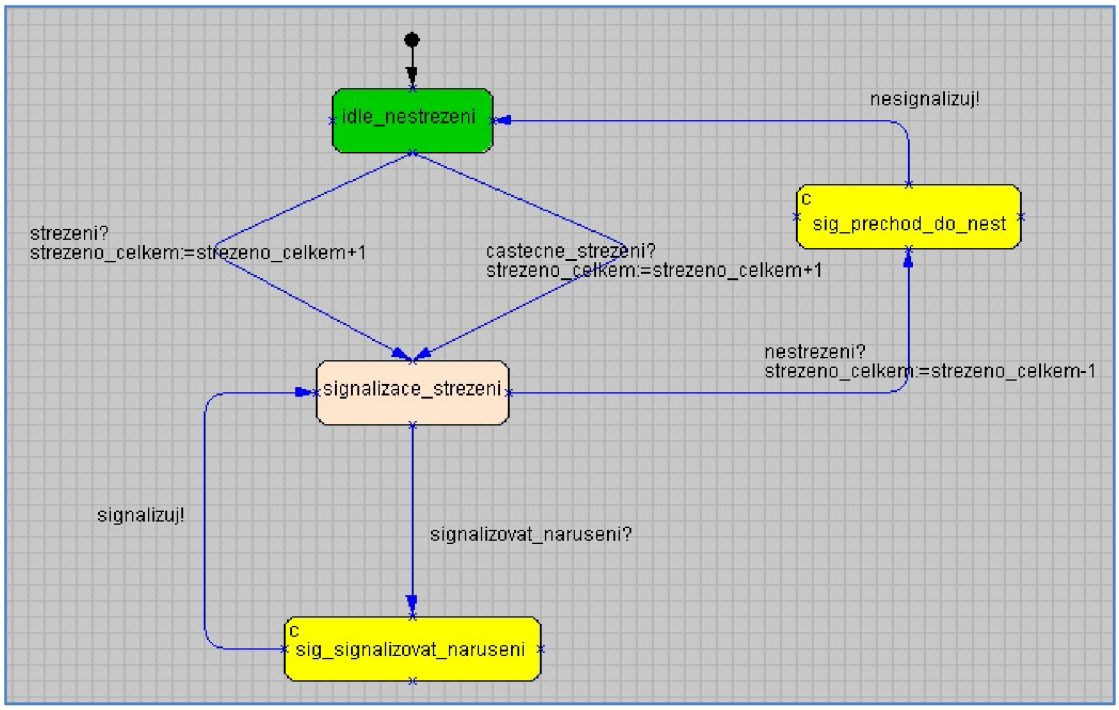
Na dalším obrázku je znázorněno chování magnetických senzorů otevření oken. Výchozí stav je nestřežení, ve kterém když obdrží signál od ústředny o střežení či částečném střežení přejde do stavu střežení a v něm setrvává, dokud nedojde k odstřežení, nebo k vnějšímu narušení. K vyhlášení narušení dojde, pokud byl dán signál z prostředí, tj. byl někým střežený prostor narušen. V případě použití jednodušších čidel je zde možnost eliminace zákmitů kontaktu.



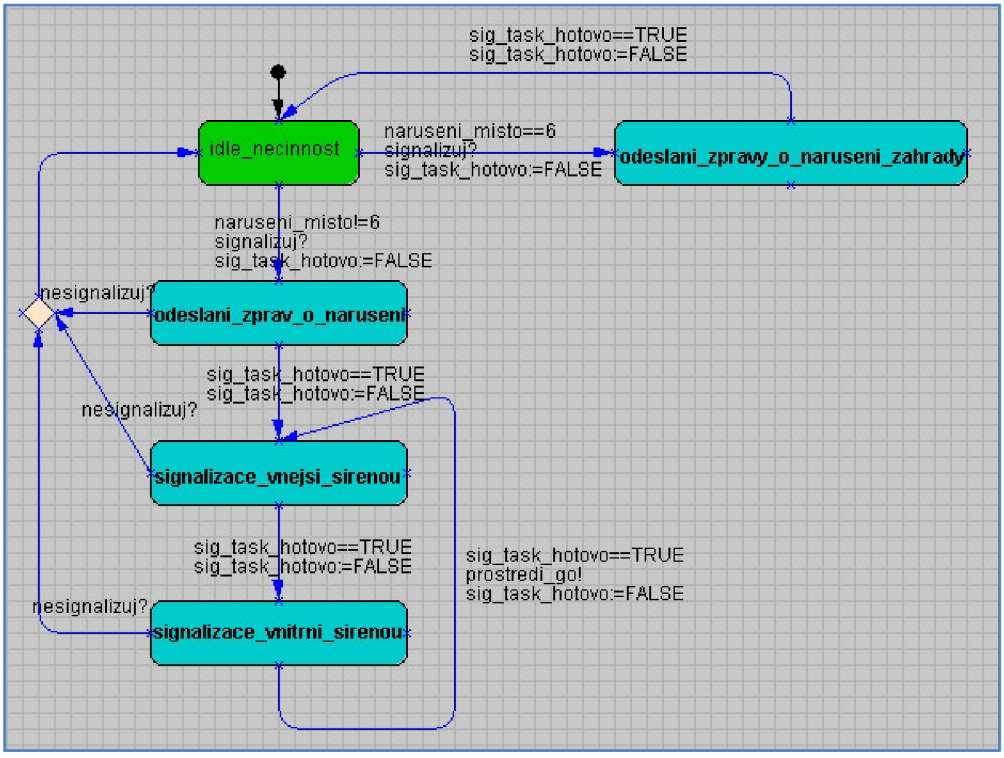
Obrázek 7.7: Automat vyjadřující chování magnetických kontaktů.

Chování ostatních čidel je velice podobné s tím rozdílem, že se reaguje na jiné signály, všechna čidla nejsou aktivní (ve stavu střežení) při částečném střežení a není detekce zákmitů. Z důvodu pouze těchto malých rozdílů zde nebude rozebíráno konkrétní chování ostatních detektorů.

Dalším důležitým prvkem systému je signalizace. Ta je implementována pomocí dvou automatů. Jeden, který se obstarává řízení signalizace, a druhý, který vlastní signalizaci provádí. Signalizace je aktivována ústřednou při vyhodnocení narušení, které bylo zaznamenáno pomocí čidel, a dá podnět k započetí signalizace. Také kdykoli v průběhu signalizace může dostat podnět od ústředny, že má signalizace skončit a ukončí ji. Při vlastní signalizaci se rozlišují dva případy. V prvním došlo k narušení jen v oblasti zahrady, tudíž není nutné informovat bezpečnostní agenturu a je pouze zaslána zpráva majiteli o narušení hranic pozemku například pomocí SMS či krátkého hovoru. V druhém případě jde o narušení indikované čidly na všech ostatních místech a je nutné upozornit bezpečnostní agenturu zasláním informací na pult centralizované ochrany (PCO), a dále signalizovat narušení pomocí vnitřní akustické a vnější vizuální i akustické sirény do doby vypnutí, nebo příjezdu povolaných osob.



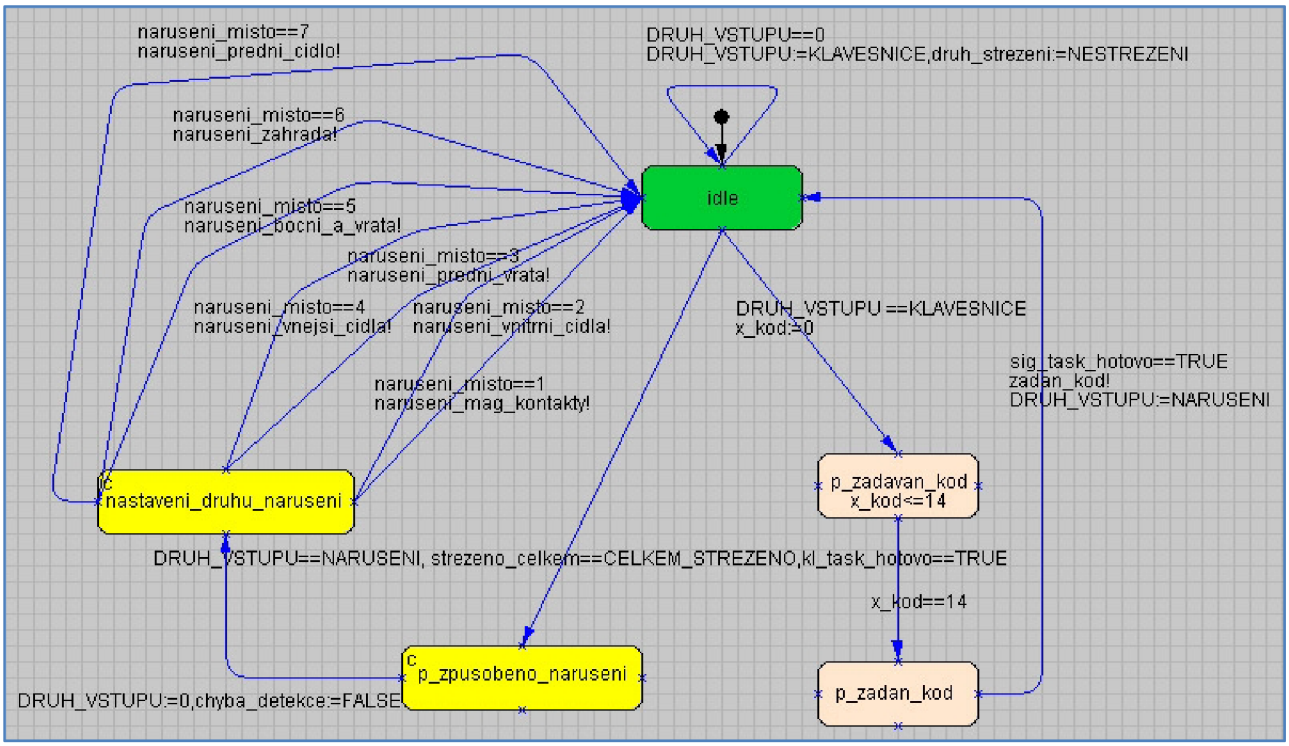
Obrázek 7.8: Automat vyjadřující chování řídícího modulu signalizace.



Obrázek 7.9: Automat zachycující vykonávání signalizace.

Prostředí je prvek vně systému, díky kterému je možné simulovat systém samotný. Níže je uveden obrázek, ze kterého je zřejmé chování. Nejprve dojde k zadání kódu pro střežení na klávesnici, na to reaguje ústředna příslušnými kroky pro uvedení celého systému do stavu střežení,

poté dojde k narušení objektu podle příslušných parametrů a o reakci se postarají čidla, která dají podnět ústředně. Ta vyhodnotí, zda bude signalizováno narušení či nikoli. Posléze dojde opět k zadání kódu, ale tentokráte jde o kód, který vyjadřuje, že se má přejít do stavu nestřežení, a ústředna vykoná potřebné kroky.



Obrázek 7.10: Automat simulující chování prostředí.

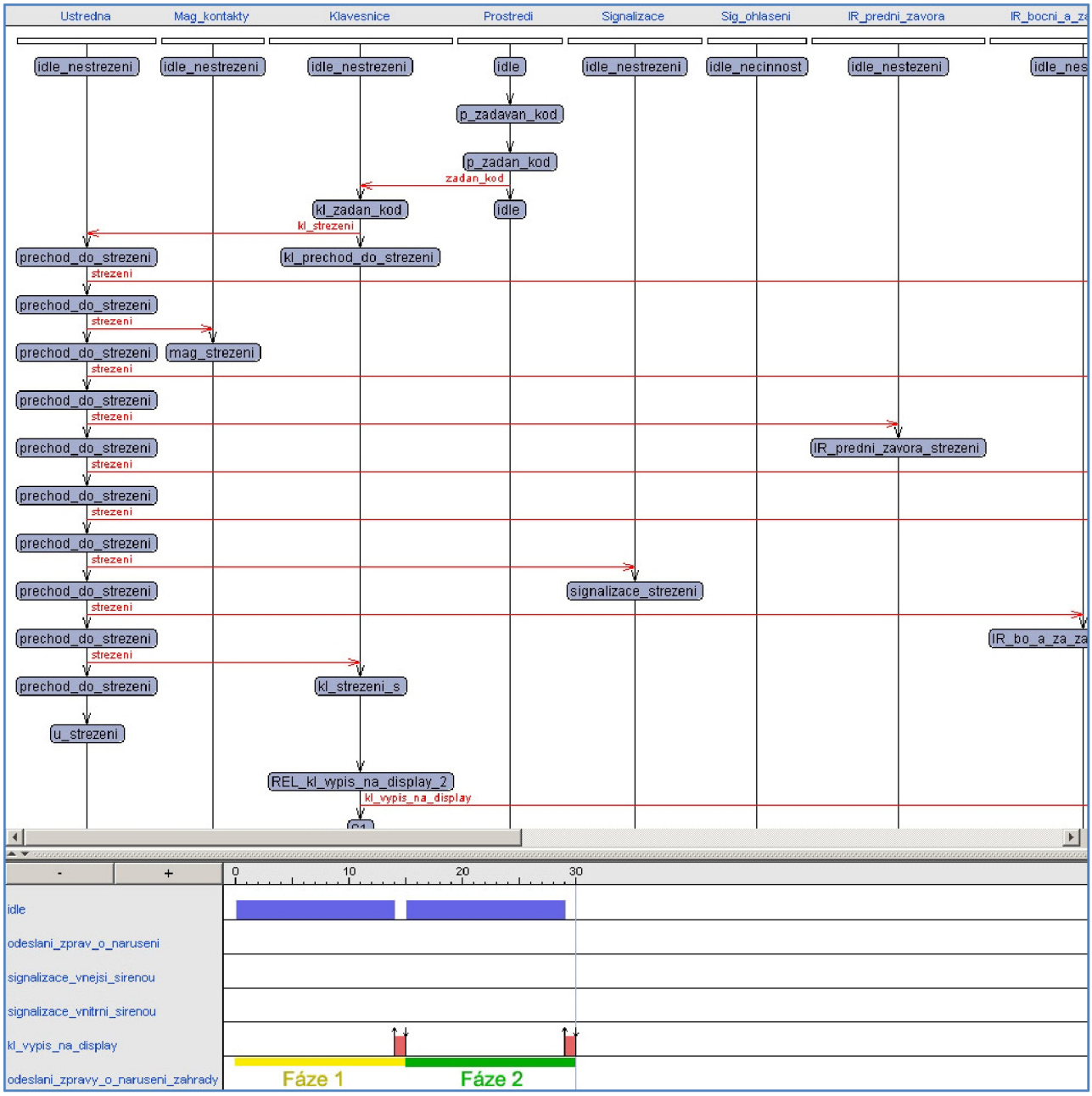
Úkoly byly voleny tak, aby popisovaly chování systému viditelné pro uživatele a také kvůli přehlednosti při simulaci. Jsou znázorněny na diagramech uvedených výše a jsou zvýrazněny poli s modrozelenou barvou.

7.3.2 Simulace modelu

V této části bude popsána simulace několika modelových situací, které by ve skutečnosti byly systémem řešeny. Ve všech případech je systém ve výchozím stavu nestřežení.

V první situaci uživatel odchází z objektu a zadáním kódu objekt zabezpečí, při návratu do střeženého objektu zadá kód pro ostřežení a systém přejde do stavu nestřežení.

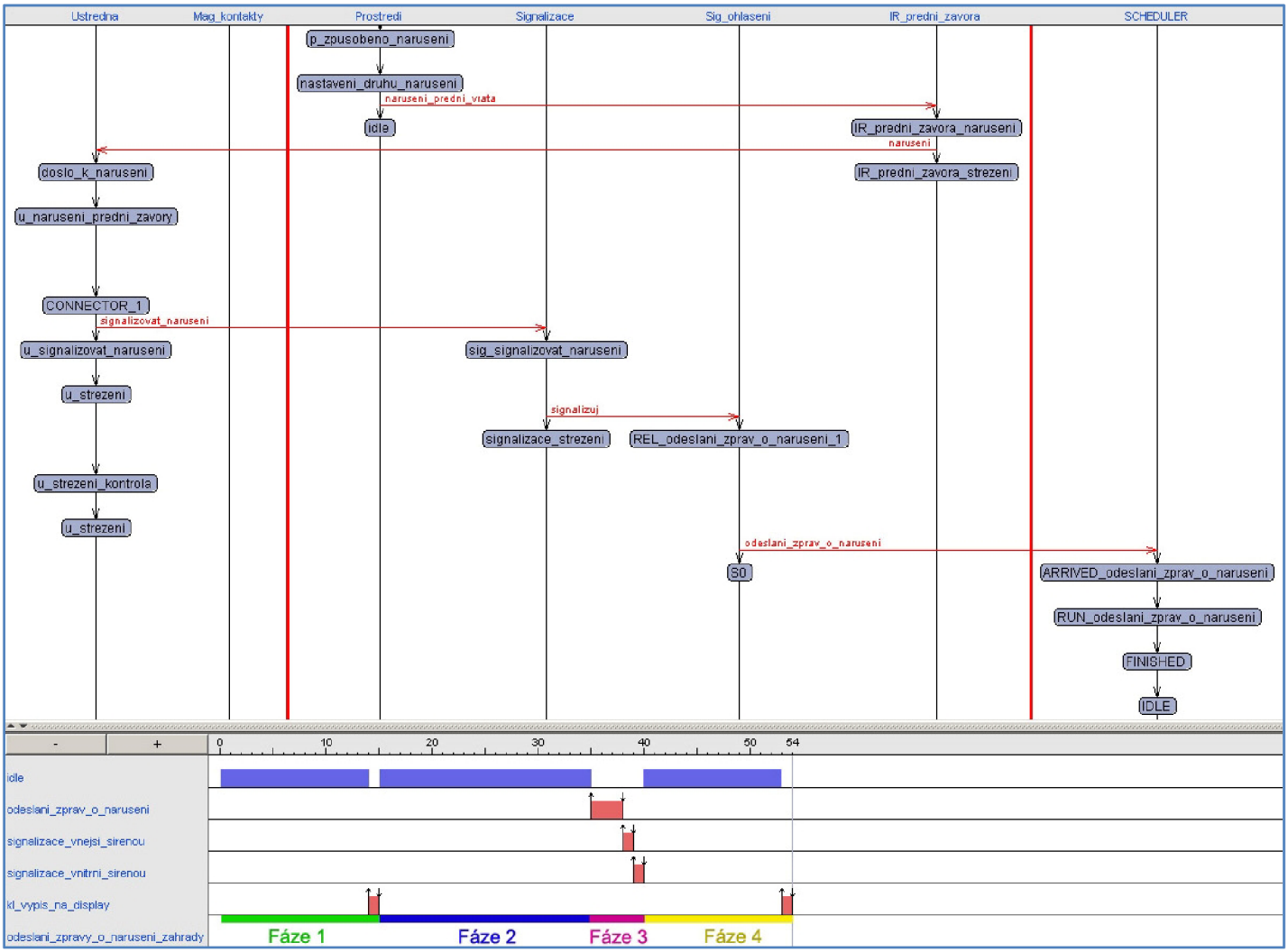
Na obrázku níže je zobrazeno simulační okno s danou simulací. V horní části je vidět komunikace z prostředí na klávesnici a dále do ústředny, která následně zajistí přechod ostatních prvků do střežení. Ve spodní části je znázorněna celá simulace. Zvýrazněná část jako fáze 1 znázorňuje zadání kódu, přechod do střežení a končí výpisem stavu systému na klávesnici. Fáze 2 značí čas rezervovaný pro zadání kódu a o ukončení střežení a výpis informací na displej.



Obrázek 7.11: Simulační příklad 1.

V následujícím případě, je obdobná situace, s tím rozdílem, že buď nebyl zadán kód pro odstřežení, nebo jde opravdu o útok narušitele vedený přes přední vstupní dveře. Následuje signalizace narušení a po příjezdu povolaných osob a zadání kódu ukončení střežení.

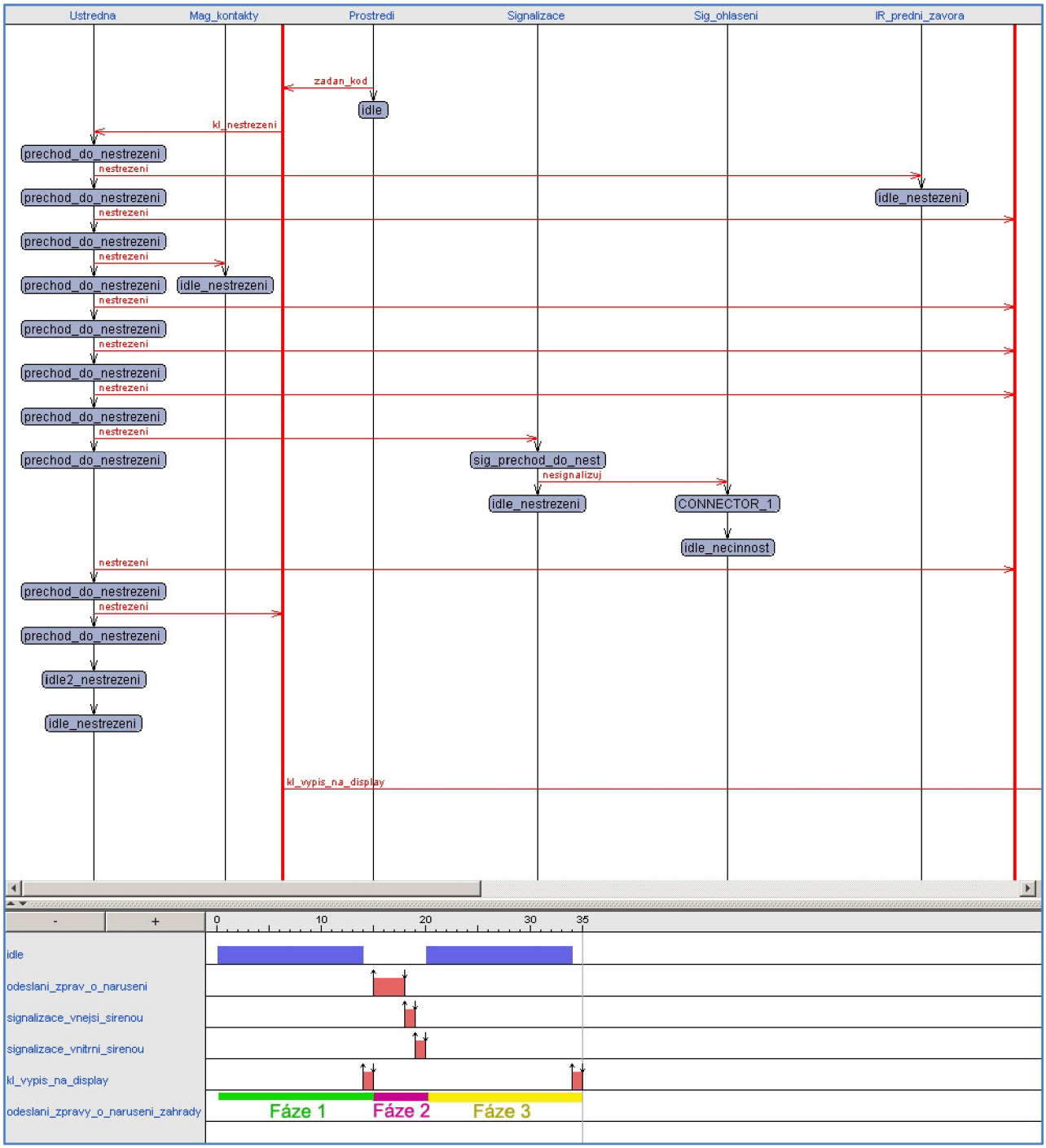
V horní části obrázku je znázorněn postup systému od narušení po začátek signalizace tj. zaslání informací na PCO. Ve spodní části zvýrazněné pomocí barev: fáze 1 odpovídá přechodu do stavu střežení a výpis na displeji klávesnice, fáze 2 je čas poskytnutý na zadání kódu pro odstřežení, jelikož došlo k porušení v místě normálního vstupu, fáze 3 vdaném intervalu nebyl zadán kód, dojde tudíž k signalizaci narušení, skládající se ze zaslání informací o narušení na PCO a signalizaci pomocí sirén, a fáze 4 přechod do nestřežení s výpisem informací na displeji u klávesnice.



Obrázek 7.12: Simulační příklad 2.

V dalším příkladu je modelována situace narušení objektu v době střežení na všech místech krom vstupních dveří a prostoru zahrady. Z počátečního stavu dojde k zadání kódu a zastřežení celého objektu a výpisu na displeji klávesnice. Následně dojde ke vstupu například přes okno v přední části objektu a tím se vyvolá oznámení od magnetického kontaktu, který hlídá otevření okna. Ústředna signál vyhodnotí a dá podnět k započetí signalizace o narušení. Ta probíhá do okamžiku, kdy je zadán kód vyjadřující přechod systému do stavu nestřežení, ústředna ukončí střežení i signalizaci narušení a uživatel je o tom informován na displeji klávesnice.

Na obrázku níže je zobrazeno simulační okno s danou simulací. V horní části je vidět komunikace od uživatele na klávesnici a dále do ústředny, která zajistí přechod do nestřežení a ukončí signalizaci. Ve spodní části je znázorněna celá simulace. Zvýrazněná část jako fáze 1 znázorňuje čas zadání kódu pro přechod do střežení a končí výpisem stavu na klávesnici. Fáze 2 je již vlastní signalizace narušení. V tomto případě, skládající se ze zaslání informací o narušení na PCO a signalizaci pomocí sirén. Fáze 3 značí zadání kódu o ukončení střežení a výpis informací na displej klávesnice.



Obrázek 7.13: Simulační příklad 3.

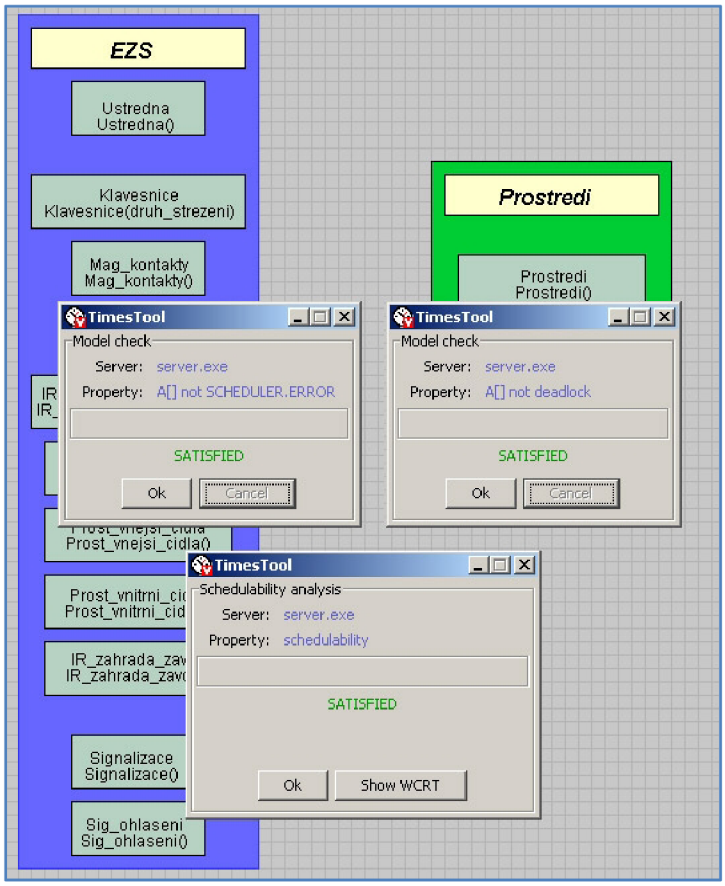
7.3.3 Verifikace modelu

Verifikace neboli ověření správnosti modelu je důležité hlavně kvůli tomu, že i když provedeme velký počet simulací, není možné vždy postihnout všechny případy, které mohou nastat.

Následující dotazy jsou součástí modelu, konkrétně jsou uloženy v souboru xkucha15.q.

Nejdříve jsou zde ověřeny vlastnosti celého systému. Ty jsou v zásadě tři, první ověřuje, zda v modelu není možné uváznout, dle syntaxe verifikátoru je zapsán jako `A[] not deadlock`, druhá, zda se někdy nevyskytne chyba v plánovači, psáno jako `A[] not SCHEDULER.ERROR`, a třetí, zda

jsou všechny úlohy naplánovatelné a jestli je garantováno jejich včasné dokončení, velice blízce souvisí s předchozí vlastností, tzv. analýza plánovatelnosti, ta má vlastní položku v menu editoru. Výsledek těchto dotazů je na následujícím obrázku.



Obrázek 7.14: Verifikace na uváznutí a chyby plánovače, analýza plánovatelnosti.

Následují další dotazy dokazující požadované chování systému. Ty budou uváděny jen v textové podobě bez odpovídajících obrázků.

Zda je dosažitelný stav v automatu ústředny, který vyjadřuje střežení.

```
E<> (Ustredna.u_strezeni)
```

Jestli vždy, když je požadováno nestřežení, systém opravdu ve stavu nestřežení.

```
A[] (druh_strezeni==NESTREZENI imply Ustredna.idle_nestrezeni)
```

Zda existuje cesta, kdy přejde klávesnice do stavu částečného střežení a bude následovat výpis na displeji.

```
E<> (Klavesnice.kl_castecne_strezeni and kl_task_hotovo==FALSE)
```

Pokud existuje cesta, že se má střežit bude opravdu ústředna ve stavu střežení.

```
E<> (druh_strezeni==STREZENI imply Ustredna.u_strezeni)
```

Když je ústředna ve stavu střežení, jsou ve stavu střežení všechna příslušná čidla (uvedeno je jen jedno) včetně klávesnice.

```
E<> (Ustredna.u_strezeni imply (Mag_kontakty.mag_strezeni and
Klavesnice.kl_strezeni_s))
```

Nikdy nebude dosažitelný stav ústředny, že došlo k narušení, tak aby v něm bylo možné setrvat.

```
A[] not (Ustredna.doslo_k_naruseni)
```

Neexistuje možnost, že by došlo k prodlevě či vykonávání něčeho jiného v případě, že se má začít signalizovat narušení.

```
A[] not(Signalizace.sig_signalizovat_naruseni)
```

Zda plánovač někdy naplánuje provedení úlohy odeslání zpráv o narušení. Zde je vidět nesouhlasné tvrzení verifikátoru, že k tomuto nedojde, ale jak je vidět výše ze simulací, tato úloha je běžně prováděna. I při pokusu umístění úlohy tak, že musí být vykonána, verifikátor nazná, že nikoli.

```
E<> (SCHEDULER.RUN_odeslani_zprav_o_naruseni)
```

7.3.4 Implementace modelu v jazyce C

Součástí nástroje Times Tool je i generátor kódu, který je schopen z vytvořeného modelu generovat zdrojový kód v jazyce C. Tento způsob je využitelný při vytváření systému na univerzální platformě, ale jak již bylo nastíněno v části návrhu, produkty určené přímo jako zabezpečovací systémy mají od výrobce dané grafické konfigurační nástroje. Zdrojové kódy jsou vygenerovány i se systémem BirckOS, který lze využít. Systém, rozhraní a jejich definice jsou v souborech: brickos_kernel.c, brickos_hooks.h, brickos_interface.h, brickos_system.h. Vlastní model, definice konstant, proměnných a funkcí jsou v souborech: xkucha15.c, xkucha15.h, xkucha15_global.h, xkucha15_init.c, xkucha15_init.h. Poslední jmenovaný a k němu příslušný hlavičkový soubor jsou určené k dopsání inicializační části, která má být provedena před spuštěním vlastního systému. Byl také automaticky vygenerován soubor Makefile pro překlad zdrojových kódů. V dalším textu jsou vybrané úryvky vygenerovaného kódu.

V následujícím části je definice offsetů jednotlivých úloh, funkce na jejich vydávání a kompletaci.

```
/**
 * @name Task identifiers (tid).
 */
#define tid_offset 200
#define tid_odeslani_zprav_o_naruseni tid_offset+0
#define tid_signalizace_vnejsi_sirenou tid_offset+1
#define tid_signalizace_vnitrni_sirenou tid_offset+2
#define tid_kl_vypis_na_display tid_offset+3
#define tid_odeslani_zpravy_o_naruseni_zahrady tid_offset+4
#define tid_NOP tid_offset+5

char release_list[NB_TASK]={ 0,0,0,0,0};

wakeup_t task_release(wakeup_t data) {
  if(release_list[data]) {
    switch (data) {
    default: return true;
  }
```

```
  } else
  return false;
}
wakeup_t task_complete(wakeup_t tid) {
  switch(tid) {
  case 0:case 1:case 2:case 3:case 4:}
  return true;
}
```

V této části automaticky vygenerovaného kódu je zřejmá definice používaných konstant, časových proměnných a celočíselných proměnných.

```
/**
 * Constant values
 */
#define CELKEM_STREZENO 9
#define TRUE 1
#define FALSE 0
#define NESTREZENI 0
#define STREZENI 1
#define CASTECNE_STREZENI 2
#define Prostredi_KLAVESNICE 1
#define Prostredi_NARUSENI 2

/**
 * Clock variables
 * Ordered: global first, then local clocks for each process.
 */
time_t clock_Ustredna_x_kod;
time_t clock_Prostredi_x_kod;

/**
 * Integer variables
 */
int naruseni_misto=1;
int strezeno_celkem=0;
int druh_strezeni=1;
int chyba_detekce=0;
int sig_task_hotovo=1;
int kl_task_hotovo=1;
int Prostredi_DRUH_VSTUPU=1;
int* IVARS[NB_VAR]
={&naruseni_misto,&strezeno_celkem,&druh_strezeni,&chyba_detekce
,&sig_task_hotovo,&kl_task_hotovo,&Prostredi_DRUH_VSTUPU};
```

Následuje zdrojový kód odpovídající činnosti, které provádějí jednotlivé úkoly. Do původního textu byly přidány a zvýrazněny obsahy souborů, které jsou uvedeny za klíčovým slovem #include.

```
/**
 * Task bodies
 */
// odeslání zpráv o narušení
int odeslani_zprav_o_naruseni() {
  TASK_BEGIN(odeslani_zprav_o_naruseni)
#include "./tasks/zprava_o_naruseni.h"
odeslat_zpravu( &zprava_na_pco );
```

```
sig_task_hotovo=TRUE;
  TASK_END(odeslani_zprav_o_naruseni)
}


//výpisy na klávesnici
int kl_vypis_na_display() {
  TASK_BEGIN(kl_vypis_na_display)
#include "./tasks/kl_vypis.h"
switch (druh_strezeni) {
       case NESTREZENI:
            vypis(&nestrezeni);
            sound_system(NESTREZENI);
            break;
       case STREZENI:
            vypis(&strezeni);
            sound_system(STREZENI);
            break;
       case CASTECNE_STREZENI:
            vypis(&castecne_strezeni);
            sound_system(CASTECNE_STREZENI);
            break ;
}
kl_task_hotovo=TRUE;
  TASK_END(kl_vypis_na_display)
}

// signalizace pomocí vnější sirény
int signalizace_vnejsi_sirenou() {
  TASK_BEGIN(signalizace_vnejsi_sirenou)
#include "./tasks/sig_vnejsi_sirena.h"
#define DELKA 5
sig_opticka( DELKA );
sig_akusticka ( DELKA );
sig_task_hotovo = TRUE;
  TASK_END(signalizace_vnejsi_sirenou)
}

// signalizace pomocí vnitřní sirény
int signalizace_vnitrni_sirenou() {
  TASK_BEGIN(signalizace_vnitrni_sirenou)
#include "./tasks/sig_vnitrni_sirena.h"
#define DELKA 5
sig_akusticka ( DELKA );
sig_task_hotovo = TRUE;
  TASK_END(signalizace_vnitrni_sirenou)
}

// odeslání zprávy o narušení zahrady
int odeslani_zpravy_o_naruseni_zahrady() {
  TASK_BEGIN(odeslani_zpravy_o_naruseni_zahrady)
#include "./tasks/zprava_o_naruseni_zahrady.h"
odeslat_zpravu( &zprava_o_naruseni_zahrady );
sig_task_hotovo=TRUE;
  TASK_END(odeslani_zpravy_o_naruseni_zahrady)
}
```

Poslední část je věnována vlastnímu programu. Zde je viditelné spuštění inicializační funkce xkucha15_init(), ve které je možné vykonat vše, co má být vykonáno před spuštěním vlastního procesu. Následuje vytvoření úkolů s danými parametry, vynulování časových proměnných a spuštění řídícího procesu v kontroléru.

```
int main(int argc, char **argv) {

  xkucha15_init();

  execi( &odeslani_zprav_o_naruseni, 0, NULL, 5,
SMALL_STACK_SIZE);
  execi( &signalizace_vnejsi_sirenou, 0, NULL, 4,
SMALL_STACK_SIZE);
  execi( &signalizace_vnitrni_sirenou, 0, NULL, 3,
SMALL_STACK_SIZE);
  execi( &kl_vypis_na_display, 0, NULL, 2, SMALL_STACK_SIZE);
  execi( &odeslani_zpravy_o_naruseni_zahrady, 0, NULL, 1,
SMALL_STACK_SIZE);
/*
 * Reset clock variables
 */
  setClock(Ustredna_x_kod,0);
  setClock(Prostredi_x_kod,0);

  execi( &controller, 0, NULL, PRIO_HIGHEST, SMALL_STACK_SIZE);

  cputw(MAKESIG);
  return 0;
}
```

8 Závěr

V tomto projektu jsem se seznámil s velice zajímavou a mně dosud převážně neznámou oblastí, která se dotýká a bude stále více dotýkat každého z nás. Bylo velice náročné proniknout a zorientovat se v produktech a možnostech, které se neustále prohlubují a zdokonalují. A dále pak navrhnout dva rozdílné systémy pro zabezpečení a ochranu objektu.

Všechny prvky, které byly uvedeny v části návrhu EZS, byly následně zohledněny při vytváření modelu a bylo by je možné při případné realizaci použít.

V případě, že by bylo žádoucí nedělat stavební zásahy do objektu, bylo by možné celý tento navržený systém realizovat pomocí bezdrátových variant těchto prvků, případně využít obecné bezdrátové moduly, ke kterým lze připojit libovolný drátový prvek. Ale je nutné při tomto řešení uvážit, že není možné napájet prvky z ústředny a při požadavku na zálohování musí mít každý bezdrátový prvek vlastním záložní zdroj.

Také rozšíření stávajícího systému lze realizovat buď klasickými prvky připojenými pomocí kabeláže, nebo velice jednoduše využít bezdrátový modul připojitelný k stávající ústředně a k němu připojit bezdrátové prvky.

Jako praktické ověření funkčnosti návrhu bylo, po dohodě s vedoucím práce, zvoleno právě vytvoření formálního modelu a následná simulace a verifikace tohoto modelu.

Ve zvoleném nástroji Times Tool verze 1.3 beta jsem narazil na nesrovnalosti ohledně výsledků simulace a výsledků z verifikace, které spolu nekorespondovaly. Zřejmě ještě není tento nástroj dostatečně vyladěn.

Na projektu by bylo možné dále pracovat a vylepšit jeho funkcionalitu dalšími rozšířeními. Příkladem rozšíření by molo být přidání detekce požáru, možnosti vniknutí přes střechu či sklepní prostory, sloučení systému EZS s výše zmíněným kamerovým systémem. Případně pracovat na ovládacím systému ústředny a přidat například nemožnost přechodu do stavu střežení, když bude detekováno otevřené okno, apod. Další možnou návazností na projekt by mohla být implementace přímo pro daný typ ústředny, například tak jak bylo nastíněno v návrhu.

Vzhledem ke stále více se blížící neodkladné rekonstrukci popisovaného objektu a neustále zvyšující se hrozbě napadení soukromí a osobního majetku bude při rekonstrukci přihlédnuto k této částečné analýze možností zabezpečení a ochrany daného objektu.

Literatura

[1] Křeček S., *Příručka zabezpečovací techniky*. Blatná, CQC 2002.

[2] ACCES: Elektronická zabezpečovací signalizace (EZS). Dodávky a instalace EZS. URL http://www.acces.cz

[3] Optex- Home. Výrobce zabezpečovací techniky. URL http://www.optexeurope.com

[4] JABLOTRON - elektronické zabezpečovací systémy. Výrobce zabezpečovací techniky. URL http://www.jablotron.cz

[5] Zabezpečovačky.cz. Internetový obchod. URL http://www.zabezpecovacky.cz

[6] ELNIKA | CCTV velkoobchod | Kamerové systémy. Dovozce a distributor CCTV a akumulátorů. URL http://www.elnika.cz

[7] Abbas. Specializovaný distributor bezpečnostních a slaboproudých systémů. URL http://www.abbas.cz

[8] Levné kamerové systémy Brno - Návrhy, dodávky, montáž a servis kamerových systémů. Realizátor kamerových systémů. http://www.levnekamerovesystemy.cz

[9] UPPAAL. Oficiální stránky simulačního nástroje Uppaal. http://www.uppaal.com/

[10] TimesTool. Oficiální stránky simulačního nástroje Times Tool. http://www.timestool.com/

[11] Code Synthesis for Timed Automata. DOCIS Documents in Computing and Information Science. URL http://wotan.liu.edu/docis/dbl/nojoco/2002_9_4_269_CSFTA.html

[12] Modelling tips for Times. Uppsala universitet, Modelling in Times. URL www.it.uu.se/edu/course/homepage/realtid/H03/ass2/modellingtips.pdf

[13] Spelza, s.r.r. Vývoj, výroba a komplexní podpora systémů Dominus-Millennium a Dominus. URL http://www.spelza.cz/