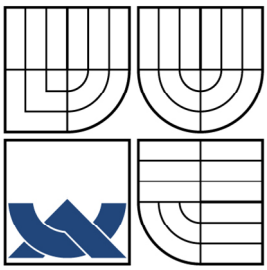
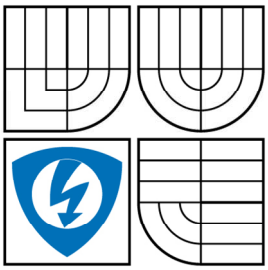


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV AUTOMATIZACE A MĚŘÍCÍ TECHNIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF CONTROL AND INSTRUMENTATION

PŘÍSTUPOVÉ A ZABEZPEČOVACÍ SYSTÉMY
ENTRANCE AND SECURITY SYSTEMS

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — Michal Kohut
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Fiedler, Ph.D.
SUPERVISOR

BRNO, 2010

VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav automatizace a měřicí techniky

Bakalářská práce

bakalářský studijní obor
Automatizační a měřicí technika

Student:	Michal Kohut	***ID:***	98141
Ročník:	3	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Přístupové a zabezpečovací systémy

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je rešerše v oblasti přístupových a zabezpečovacích systémů s ohledem na různé stupně zabezpečení.

1. Seznamte se s přístupovými systémy na bázi RFID, chipových karet atd.
2. Seznamte se s normami týkající se zabezpečovacích systémů, např. ČSN EN50131
3. Seznamte se s parametry, vlastnostmi a způsobem ovládání komerčně dostupných zabezpečovacích ústředen.
4. Seznamte se principem stavových automatů.
5. Navrhněte stavový automat menší zabezpečovací ústředny.

Pro odladění stavového automatu zvažte použití nástrojů nástrojů IAR VisualState nebo Matlab-Stateflow.

DOPORUČENÁ LITERATURA:

Manuály k nástrojům VisualState a StateFlow u vedoucího bakalářské práce.

Termín zadání:	8.2.2010	***Termín odevzdání:***	31.5.2010

Vedoucí práce: Ing. Petr Fiedler, Ph.D.

prof. Ing. Pavel Jura, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Abstrakt

Při psaní této bakalářské práce byla snaha popsat přístupové a zabezpečovací systémy a jejich součásti. Dále u těchto systému byla vysvětlena jejich funkce, využití a bylo uvedeno jejich rozdělení. Velká pozornost byla věnována také zabezpečovacím ústřednám, jejich vlastnostem a ovládání. V poslední řadě byl navržen stavový automat menší zabezpečovací ústředny. Ten byl rozdělen na 4 menší stavové automaty, které byly odladěny v programu IAR visualSTATE.

Abstract

During writing this bachelor labour I strived to describe some entrace and security systems and their parts. Also some functions and usage of these systems were consecrated and there was introduced their division. I concerned also with observing of preventive exchanges, their properties and operating. The last part describe state machine of security central. It is diveded to 4 smaller state macines which were all tested using IAR visualSTATE program.

Klíčová slova

Přístupový systém, Zabezpečovací systém, Detektor, Ústředna EZS, Stavový automat, Stavový diagram, RFID, Čipová karta, Komunikace.

Keywords

Entrace system, Security system, Detector, Central EZS, State automat, State diagram, RFID, CHip card, Communication.

B i b l i o g r a f i c k á c i t a c e

KOHUT, M. Přístupové a zabezpečovací systémy. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 59 s. Vedoucí semestrální práce Ing. Petr Fiedler, Ph.D.

Prohlášení

„Prohlašuji, že svou bakalářskou práci na téma Přístupové a zabezpečovací systémy jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne: ……

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Petru Fiedlerovi, Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

V Brně dne: ……

podpis autora

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

1. ÚVOD

Přístupové a zabezpečovací systémy se používaly už v dávné minulosti, kdy lidé přidělovali práva k přístupu k určitým důležitým věcem a zabezpečovali svůj majetek. Během let docházelo k vývoji těchto systémů, přes různé padací mosty, příkopy a další přístupové a zabezpečovací prostředky, až k dnešní době, kdy většina těchto systému je elektronická a můžeme se s nimi setkat denně, všude tam, kde se člověk podívá.

Cílem této bakalářské práce bylo seznámení se s přístupovými a zabezpečovacími systémy, normami týkajících se této problematiky, ústřednami, stavovými automaty a navržení stavového automatu menší zabezpečovací ústředny.

Zabezpečení objektu není lehká záležitost, musí se zvážit mnoho podstatných věcí, aby nedocházelo k jeho narušení. Musí se například vybrat druh ochrany nebo stupeň zabezpečení. Další důležitou věcí je volba ústředny, která může mít mnoho rozdílných vlastnosti a parametrů, mezi kterými uživatel volí podle velikosti a typu střeženého objektu.

Ústředny jsou řízeny stavovými automaty, které slouží k modelování dynamického chování systému.

2. PŘÍSTUPOVÉ SYSTÉMY [1][2][3][4][5]

Přístupové systémy umožňují provádět efektivní kontrolu a zabezpečení vstupu do určitých objektů. Provádět vstup je umožněno jen subjektu, který práva na přístup do těchto objektů vlastní. Dále tyto systémy zajišťují rychlý pohyb v těchto objektech a to je zajištěno tím, že odpadá nutnost nosit u sebe tolik klíčů a otevírání zámků je mnohem pohodlnější. Prostředek, kterým se subjekt identifikuje, může být plastová karta (kontaktní i bezkontaktní), čip nebo biometrický rys člověka.

Výhody přístupových systémů oproti klíčům:

1. Pokud dojde ke ztrátě karty nebo jsou odebrána přístupová práva, stačí kartu vymazat ze systémové databáze a je jedno, jestli byla karta vrácena nebo si jí vlastník nechal.
2. Přístupové systémy umožňují kontrolovat, kdo vstoupil nebo naopak opustil určitou oblast v určitém čase. Také umožňují sledovat neplatné pokusy o vstup.
3. Možnost přidělení vstupu jen do určitých oblastí a jen v určeném časovém úseku.
4. Nedochází k opotřebení čipu a karet jako u klíčů.

Obrázek 2.1: Bezkontaktní klíčenky[1]

Přístupové systémy neslouží pouze k otevírání elektrických dveřních zámků, ale také podle přístupových práv umožňují průchod jakoukoliv elektronickou zábranou. Pomocí těchto systémů lze ovládat i elektronické zabezpečovací systémy. Ve výsledku tyto systémy umožňují v mnoha případech zmenšit náklady na ostrahu či zámkový systém, a přesto podstatně zvýšit úroveň bezpečnosti.

2.1 DĚLENÍ PŘÍSTUPOVÝCH SYSTÉMŮ

Přístupové systémy se dělí podle správy na:

- centrálně řízené
- autonomní
- kombinované

Centrálně řízené zámky se používají ve velkých organizacích nebo při vysokém počtu nasazení. Tento systém se vyznačuje rychlou a efektivní reakcí na změny. Další výhodou je možnost zablokovat přístup při ztrátě autorizačního klíče. Zablokování se provede odstraněním autorizačního klíče z centrálně uložené evidence.

Autonomně řízené zámky se používají v prostředí bez velkého nasazení. Tyto zámky jsou závislé pouze na energetickém zdroji. Jelikož se jedná o elektrické zámky, není potřebná výměna zámku, pouze se vymaže záznam z paměti.

Kombinované zámky jsou kombinací předešlých variant a řeší jejich nedostatky. Tyto zámky se jeví jako centrálně řízené, ale při vyskytnutí se problému, dojde k přepnutí do nezávislého režimu.

Zámky lze také rozdělit podle toho, jestli je zapotřebí externího klíče nebo klíč je součástí nositele. Mezi externí klíče patří třeba kontaktní magnetické karty,

bezkontaktní čipové karty a rádiové nebo IR vysílače. Klíče, které jsou součástí nositele, mohou byt biometrické nebo číslicově kódové.

Mezi hlavní přístupové systémy patří přístupové systémy na bázi RFID a čipové karty.

2.1.1 Čipové karty

Čipová karta je integrovaný obvod, zalisovaný v nějakém nosiči, obsahující kryptografický koprocesor s dostatečně velkou pamětí a operačním systémem, který bývá umístěn v paměti ROM čipu. Pod pojmem čipová karta si můžeme představit miniaturní kryptografický počítač, jehož funkcí je komunikace s PC nebo terminálem pomoci kontaktního nebo radiového přenosu. Čipové karty mohou ve svém koprocesoru generovat šifrovací klíčové páry a následně s nimi dělat různé operace, díky tomu privátní klíč nikdy neopustí kartu.

Čipové karty zajišťují dvojí bezpečnost, jednou je samotná karta, kterou vlastníte a druhou heslo. Pro zjištění vašich informací je zapotřebí mít vaší kartu a současně znát vaše heslo. Čipové karty mohou obsahovat další bezpečnostní prvky, jako jsou magnetické proužky a natištěné informace.

Kontaktní čipová karty

Kontaktní čipové karty mají na sobě osm kontaktů, jejichž prostřednictvím dochází k propojení se čtečkou. Tyto karty jsou používány jako bezpečné medium a jsou napájeny ze čtečky.

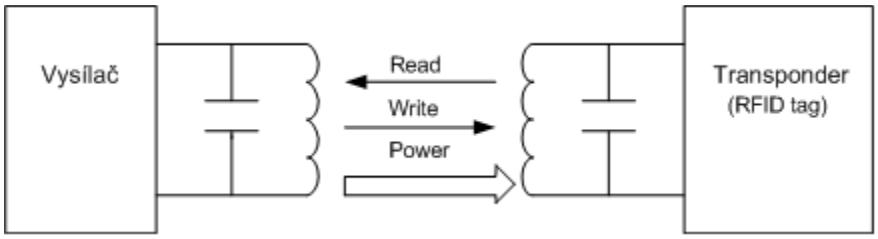
Bezkontaktní čipová karty

Součásti Bezkontaktní čipové karty je čip a anténa. Ke komunikaci se čtečkou používá elektromagnetické vlny, nemusí se zasouvat do čtečky. Díky tomu jsou používány pro identifikaci fyzického přístupu a jsou rovněž napájeny ze čtečky.

Využití čipových karet je velice rozsáhlé. Nejčastěji bývají využívány pro řízení fyzického přístupu v rámci přístupových systémů objektů. Většinou se používá bezkontaktní RF komunikace. Jedná se o jednoduchou identifikaci, pomocí identifikačního čísla. U přístupového systému s vyššími bezpečnostními podmínkami lze doplnit o verifikaci vlastníka karty, pomocí zadání kódu PIN.

2.1.2 Přístupové systémy na bázi RFID

RFID je bezkontaktní identifikace pomocí rádiového signálu bez nutnosti přímé viditelnosti, jedná se vlastně o rádiovou náhradu čárových kódů. O vývoj karty RFID se zasloužila firma Wal-mart, stejně jako u čárových kódů. K bezkontaktní identifikaci je využíváno paměťových čipů, které obsahují jedinečnou informaci určenou výrobním číslem čipu. Čipy se vyskytují v provedení pro čtení nebo pro čtení a zápis. Dále karty využívají převážně nosnou frekvenci 125 kHz, 134 kHz a 13,56 MHz. Dají se použít i jiné frekvence jako 868 MHz v Evropě a 915 MHz v Americe.



Obrázek 2.2: Základní princip komunikace RFID[4]

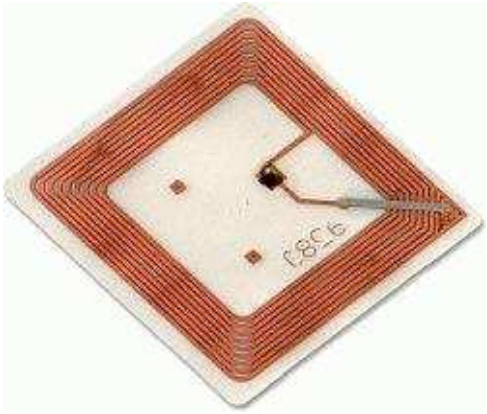
Každý RFID systém se skládá ze 3 částí a těmi jsou anténa, vysílač s dekodérem a transponder. Označení transponder pochází ze dvou slov TRANSmitter a resPONDER, tedy vysílač a odpovídač. V dnešní době se častěji používá označení RFID tag. Princip komunikace RFID vychází z toho, že je radiový signál vysílán vysílačem, tento signál aktivuje RFID tag, který odešle informace zpět a případně zapíše přijaté informace do své paměti.

Karty RFID dělíme podle typu na:

- pasivní
- aktivní

Pasivní RFID karty pracují jako vysílače periodických pulsu do okolí. Blízká RFID karta využije přijímaný signál k nabití svého napájecího kondenzátoru a odešle odpověď. Pasivní karty jsou nejrozšířenější, nemají vlastní zdroje energie a jsou napájeny polem snímače.

Aktivní RFID karty mají vlastní baterii a jsou schopny samy vyslat svoji identifikaci. Aktivní karty se používají méně než pasivní karty, protože jsou dražší, složitější a těžší.



Obrázek 2.3: Pasivní RFID čip[4]

Na obr. 2.3 vidíme, jak vypadá pasivní RFID čip. Čtverečky kolem jsou anténa a maličký černý flek uprostřed je čip. Aktivní čip navíc obsahuje nezávislý zdroj napájení.

Karty RFID můžeme také dělit podle možnosti zápisu:

- pouze ke čtení (programováno ve výrobě)
- zapisovatelné 1x nebo vícenásobně (programováno při použití)

- zapisovatelné vícenásobně (programováno kdykoliv, čtení 1000 tagů/s)
- zapisovatelné vícenásobně (programováno kdykoliv, čtení 1600 tagů/s)

Mezi hlavní výhody RFID systémů, oproti čárovým kódům, patří čtení bez přímé viditelnost. Čárové kódy jsou snímány, proto musí byt viditelné. Dále je to hromadné čtení nosičů RFID a také možnost přepisování RFID nosičů, přitom vytištěnou etiketu nejde měnit. Naproti tomu výhoda čárových kódů oproti RFID systému je cena.

3. ZABEZPEČOVACÍ SYSTÉMY[6][7][9]

Zabezpečovací systémy se využívají k zabezpečování majetku, informací a osobní bezpečnosti. Jejich úkolem je detekovat jakýkoliv pokus o vniknutí do střeženého objektu a následně na něj upozornit.

Zabezpečovací systémy se dělí na zabezpečení mechanické a elektrické. Mezi mechanické zabezpečení patří např. bezpečnostní dveře a mříže nebo fólie na oknech. Tento způsob zabezpečení má odradit či ztížit přístup do objektu, přesto pokud bude mít zloděj dostatek času, prolomí tyto překážky. Úkolem elektrického zabezpečení je upozornit na pokus o vniknutí do objektu.

Elektrické zabezpečení je možné rozdělit na 3 druhy zabezpečení:

- drátová varianta
- bezdrátová varianta
- hybridní systém

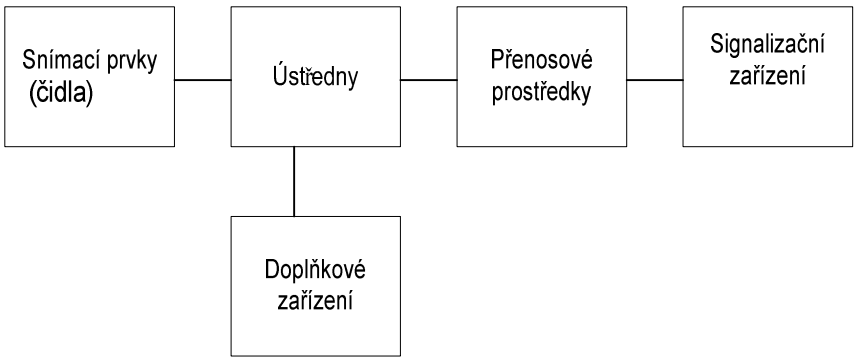
U drátové varianty jsou všechny součásti propojeny vedením, které zajišťuje komunikaci se zabezpečovací ústřednou. Tento způsob zabezpečení je náročný na instalaci, ale nenáročný na údržbu a pořizovací náklady.

U bezdrátové varianty dochází ke komunikaci radiovým signálem na frekvenci 433 MHz. Výhodou této varianty je, že není potřeba rozvodné sítě, dále je to možnost jednoduše měnit rozmístění prvků. Naopak nevýhodou je cenová náročnost a nutnost jednou ročně vyměnit baterie ve všech čidlech, na tuto potřebu výměny baterie upozorní každý prvek sám.

Hybridní systém je kombinace drátové a bezdrátové varianty. Využívá se např. k zabezpečení oddělené garáže nebo zabezpečení dvou, či více samostatně stojících objektů jedním systémem.

Systémů elektronické zabezpečovací signalizace (EZS) je celá řada, ale v podstatě se všechny skládají z několika základních stavebních jednotek, které dohromady tvoří zabezpečovací řetězec. Tento řetězec můžeme vidět na obr. 3.1. Mezi tyto základní stavební jednotky patří:

- snímací prvky (detektory)
- ústředny
- doplňkové zařízení
- zařízení pro odeslání poplachových informací
- signalizační prostředky



Obrázek 3.1: Blokové schéma zabezpečovacího řetězce[7]

3.1 SNÍMACÍ PRVKY

Funkcí snímacích prvků je vyslání signálu o narušení chráněného prostoru do elektronické zabezpečovací ústředny. Snímací prvky jsou voleny tak, aby co nejlépe vyhovovaly prostředí, do něhož mají být umístěny a také svému použití. Dalším požadavkem na konstrukci a instalaci snímacích prvků je zvětšit na maximum detekci skutečného vniknutí a zmenšit na minimum riziko planých poplachů.

Mezi nejpoužívanější snímací prvky, které se používají k zabezpečení bytů a rodinných domů, patří:

- PIR detektory
- magnetické kontakty
- požární detektory
- detektory zaplavení
- detektory rozbití skla

PIR detektory jsou infrapasivní snímače, sloužící pro ochranu vnitřních prostor před narušiteli. Jedná se o pohybové detektory, které zaznamenávají pohyb na základě analýzy teploty v určitém prostoru. Tyto detektory reagují na osvícení čelní strany čidla, zastínění čidla nábytkem, pohybující se záclony v blízkosti snímače, průvan před přední části čidla apod.

Magnetické kontakty se umísťují na okna a dveře, při jejich otevření vyšlou signál do ústředny o narušení. Pro jejich umístění se volí hlavní přístupová místa (vchodové dveře, brány apod.). Jejich nevýhodou je, že nereagují např. na rozbití nebo vyříznutí skla v okně.

Požární detektory slouží k detekci požárů. Existuji 3 druhy snímačů a to ionizační, optické a tepelné. Nejvíc používané jsou ionizační, které detekují zvýšený výskyt kouře v prostoru. Umístění těchto detektorů se realizuje podle objektu, který je třeba zabezpečit. U rodinných domů se musí nacházet v části vedoucí k východu z rodinného domu, u bytových domů se musí nacházet v každém bytě v části vedoucí směrem do únikové cesty.

Detektory zaplavení detekuji překročení povolené výšky vodní hladiny.

K detekci rozbití skla slouží akustické detektory. Kvalitní snímače ignorují jiné podobné zvuky. Detektor se umísťuje naproti skleněné výplni a to maximálně do vzdálenosti 9 metrů od skleněné výplně. Jeho výška instalace od podlahy by měla být přibližně 2 metry.

3.1.1 Dělení snímacích prvků

Snímací prvky se dělí podle toho, zda vyzařují nebo nevyzařují využitelnou energii do zabezpečovacího prostoru, na snímací prvky:

- aktivní
- pasivní

a) Aktivní snímací prvky při zjišťování rysů nebezpečí vytvářejí své pracovní prostředí aktivním zásahem do okolního prostoru.

b) Pasivní snímací prvky pouze pasivně registrují fyzikální změny v okolí.

Jak už aktivní snímací prvky, tak i neaktivní snímací prvky lze rozdělit podle následujících kriterií:

1) charakteru střežené oblasti na snímací prvky:

- prostorové
- směrové
- bariérové
- polohové

Snímací prvky prostorové reagují na jevy, které se týkají narušení střeženého prostoru. Snímací prvky směrové reagují jen na jevy v definovaném směru. Bariérové snímací prvky vytvářejí bariéru, tvořenou vyřazovací či snímací charakteristikou čidla a reagují na narušení této bariery. Snímací prvky polohové reagují na změnu polohy chráněného předmětu.

2) dosahu – pro vnitřní (vnější) na snímací prvky:

- s krátkým dosahem do 15 m (do 50 m)
- se středním dosahem do 50 m (do 150 m)
- s dlouhým dosahem nad 50 m (nad 150 m)

3) tvaru vyzařovací nebo snímací charakteristiky na snímací prvky:

- se standardním dosahem
- se širokoúhlým dosahem
- s kruhovým dosahem
- se svislou barierou
- s vodorovnou barierou
- s dlouhým dosahem

3.1.2 Druhy ochrany na základě umístění snímacích prvků

Podle toho, ve které části zabezpečeného prostoru může být pomoci čidel detekováno nebezpečí, nabízejí se tyto ochrany:

Plášťová ochrana

Plášťová ochrana se skládá zpravidla z magnetických kontaktů umístěných na oknech a dveřích, dále pak z detektorů tříštění skla u skleněných ploch. Úkolem této ochrany je zabezpečit objekt proti vniknutí narušitele a bývá v činnosti v mimopracovní době.

Prostorová ochrana

U této ochrany se používají infrapasivní prostorové nebo mikrovlnné čidla, které mají zajistit ochranu cenných předmětů. Tato ochrana přichází na řadu, pokud

dojde k překonání plášťově ochrany nebo narušitel se schová v objektu v době nestřežení.

Předmětová ochrana

Předmětová ochrana má na starosti ochranu předmětů vysoké hodnoty. Tato ochrana se skládá ze speciálních kontaktů umístěných buď na střežených předmětech, nebo u nich.

Osobní ochrana

Ochrana se provádí pomocí tísňových hlásičů a jejich úkolem je ochrana obyvatel, zaměstnanců apod. ve střeženém objektu. Všechny tísňové hlásiče jsou opatřeny zpětnou signalizací.

3.2 PŘENOSOVÉ PROSTŘEDKY

Zařízení vybavena pouze lokální signalizací jsou využívána pouze v případě nízkých rizik, a to nejčastěji v privátním sektoru. Pokud je zapotřebí chránit místa s velkým rizikem narušení nebo chránit větší majetek, ať už materiální hodnoty či data, je nezbytné, aby byly informace o poplachu přenášeny ze střeženého objektu do místa, odkud lze zajistit zásah. Výběr způsobu přenosu dat probíhá na základě technické proveditelnosti, vhodnosti z hlediska bezpečnosti a také podle cenových možností.

Nejčastější způsoby přenosu dat:

- Připojení radiovým vysílačem
- Připojení po telefonní lince
- Připojení GPRS komunikátorem

Obrázek 3.2: GPRS komunikátor[19]

Připojení radiovým vysílačem

Komunikace mezi rádiovým vysílačem a pultem centralizované ochrany je velice spolehlivá a každých 15 minut je automaticky prováděna kontrola funkčnosti spojení mezi zabezpečovacím systémem a PCO. Elektronický zabezpečovací systém v objektu je doplněn o radiový vysílač. Před instalací rádiového vysílače je zapotřebí zkontrolovat sílu radiového signálu ve střeženém objektu.

Připojení GPRS komunikátorem

Připojení komunikátorem slouží k přenosu dat v síti mobilních operátorů GSM. Komunikátor posílá na PCO malé datové pakety, které jsou v případě výpadku GPRS nahrazeny SMS zprávami. Každých 15 minut je prováděna kontrola funkčnosti spojení mezi zabezpečovacím systémem ve střeženém objektu a pultem centrální ochrany.

Připojení po telefonní lince

Většina ústředen zabezpečovacího systému je vybavena telefonním komunikátorem, ale je potřebná přítomnost pevné telefonní linky. Musí byt zajištěno, že připojení k této telefonní lince je uděláno tím způsobem, že ústředna EZS je

prvním zařízením v objektu, které je připojeno k této lince. Díky tomu je zajištěno, že ústředna je prvním zařízením v objektu, připojeným k této telefonní lince. Nevýhodou je kontrola spojení s PCO pouze 1x za 24 hod.

3.3 SIGNALIZAČNÍ PROSTŘEDKY

Pro akustickou signalizaci poplachu slouží sirény. Sirény mají upozornit na narušení střeženého objektu a zároveň znepříjemnit pobyt narušitele ve vnitřních prostorách. Základní dělení sirén je na vnitřní a venkovní.

Vnitřní sirény

Převážně se jedná o piezoměniče, které po přivedení napětí vydávají akustický signál. Vnitřní sirény mohou byt vybaveny také optickou signalizací. Tyto zařízení by neměly byt instalovány v blízkosti ústředny ani ovládací klávesnice. Jejich umístění by mělo být v místnosti, kde by měl být akustický signál nejsilnější a nejčastěji pod strop, aby byly co nejméně přístupné.

Venkovní sirény

Součásti venkovní sirény jsou většinou piezo- nebo magnetodynamický měnič, blikač, záložní akumulátor a elektronika. Tyto zařízení jsou napájeny trvale z ústředny nebo pomocného zdroje a elektronika udržuje záložní akumulátor v nabitém stavu. Vnější sirény jsou opatřeny často bezpečnostním kontaktem nazývaným tamper, který chrání proti otevření krytu sirény. Tyto zařízení by neměly byt instalovány na viditelném místě, ale zároveň tak, aby byly v nesnadno přístupném místě.

Dalším řešením signalizace poplachu, které zvýší bezpečnost objektu, je připojit elektronické zabezpečovací zařízení k pultu centralizované ochrany.

Pult centralizované ochrany

Pult centralizované ochrany je dispečerské pracoviště, na které jsou posílány důležité informace, které je systém elektrické zabezpečovací signalizace schopen poskytnout. V případě příjmu hlášení poplachu v objektu je vyslána do objektu zásahová jednotka nebo kontaktovaná osoba určena majitelem objektu.

Obrázek 3.3: Pult centralizované ochrany (PCO)[8]

4. SYSTÉMOVÉ POŽADAVKY EZS [9][10][11]

EZS musí obsahovat funkce v souladu s normou ČSN EN 50131-1 pro detekci vniknutí, aktivaci tísňových prostředků, zpracování informací, vyhlášení poplachů a prostředky k ovládání EZS. Při návrhu EZS je dále potřebné určit, v jakém prostředí bude tento systém instalován a jaký má být stupeň zabezpečení.

Základní věcí, co je třeba posoudit před určením způsobu zabezpečení a zvolením stupně zabezpečení je zranitelnost daného objektu, tedy míru možnosti vloupaní a zájem pachatelů. Prvním faktorem zranitelnosti je frekventovanost místa možného napadení, to znamená jaká, je třeba viditelnost z ulic či domovních chodeb na hlavní vchod do objektu nebo jak je rušné okolí domu či bytu. Čím je frekventovanost menší, třeba jako u domků s vysokými neprůhlednými ploty nebo odlehlých míst, tím větší je pravděpodobnost možnosti pokusu o vniknutí. Dalšími faktory zranitelnosti jsou hlučnost okolí a možnosti proniknout méně častými cestami do objektu.

4.1 STUPEŇ ZABEZPEČENÍ

Každý EZS je proveden na základě přiřazeného stupně zabezpečení, který určuje oprávnění, přístupové úrovně, provozování, vyhodnocování, detekce, hlášení, napájení, zabezpečení proti sabotáži, monitorování propojení a záznam událostí. Zabezpečení dělíme na 4 stupně, kde stupeň 1 je základní a stupeň 4 je nejvyšší. Pokud je EZS důkladně rozdělen do subsystému, pak je možné, aby komponenty v každém subsystému měly různý stupeň zabezpečení.

Stupeň	Název
1	Nízké riziko
2	Nízké až střední riziko
3	Střední až vysoké riziko
4	Vysoké riziko

Tabulka 4.1: Stupně zabezpečení[10]

Velikost rizika je dána předpokládanou znalostí a vybaveností narušitele.

1. Vniknutí do zabezpečeného prostoru provádí osoba s malými znalostmi EZS a s jednoduchými nástroji.
2. Vniknutí do zabezpečeného prostoru provádí osoba s omezenými znalostmi EZS, s běžným nářadím a přenosnými přístroji.
3. Vniknutí do zabezpečeného prostoru provádí osoba obeznámena s EZS, s rozsáhlým sortimentem nástrojů a přenosnými přístroji.
4. Vniknutí do zabezpečeného prostoru provádí osoba s možnosti zpracovat podrobný plán vniknutí a s kompletním sortimentem zařízení.

Orientačně můžeme stupně zabezpečení rozdělit podle objektů nebo věcí, na které se mají vztahovat. U nízkého rizika se jedná o garáže, chaty, byty a rodinné domy. U nízkého až středního rizika může jít o komerční objekty. U středního až vysokého rizika se jedná o střežení zbraní, cenin, informací a narkotik. U vysokého rizika jde zejména o objekty národního a vyššího významu.

4.2 TŘÍDY PROSTŘEDÍ

Dále je zapotřebí před výběrem vhodných komponentu zvážit v jakém prostředí se budou dané komponenty nacházet. Prostředí dělíme do 4 tříd. Třída komponentů je udávána v dokumentaci výrobce.

Třída	Název
I	Vnitřní
II	Vnitřní – všeobecné
III	Venkovní – chráněné nebo extremní vnitřní podmínky
IV	Venkovní – všeobecné

Tabulka 4.2: Třídy prostředí[10]

I. Jedná se o podmínky působící obvykle ve vnitřních prostorách při stálé teplotě, jako jsou obytné a obchodní objekty.
Předpokládají se změny teplot v rozmezí +5 °C až +40 °C při střední relativní vlhkosti okolo 75 % bez kondenzace.

II. Jedná se o podmínky působící obvykle ve vnitřních prostorách při nestálé teplotě, jako jsou chodby, haly nebo schodiště.
Předpokládají se změny teplot v rozmezí – 10 °C až +40 °C při střední relativní vlhkosti okolo 75 % bez kondenzace.

III. Jedná se o podmínky působící obvykle vně budov, kde součásti EZS nemůžou byt ovlivněna povětrnostními vlivy.
Předpokládají se změny teplot v rozmezí – 25 °C až +50 °C při střední relativní vlhkosti okolo 75 % bez kondenzace.

IV. Jedná se o podmínky působící obvykle vně budov, kde součásti EZS můžou byt ovlivněna povětrnostními vlivy.
Předpokládají se změny teplot v rozmezí – 25 °C až +60 °C při střední relativní vlhkosti okolo 75 % bez kondenzace.

4.3 PŘÍSTUPOVÉ ÚROVNĚ

Norma udává 4 přístupové úrovně:

- úroveň 1 – přístup pro kohokoli
- úroveň 2 – přístup pro uživatele, například osoba obsluhující systém
- úroveň 3 – přístup pro uživatele, například pro servisní techniky
- úroveň 4 – přístup pro uživatele, například výrobce zařízení

Přístup k jednotlivým ovládacím prvkům, které jsou přístupné na různých přístupových úrovních nebo k indikačním prvkům, které jsou viditelné v jednotlivých přístupových úrovních, musí byt rozlišen pomocí zámku, klíčového nebo kódového přepínače.

Pro rozlišení přístupu se používají prostředky jako biometrie. Biometrie je to souhrn výpočetních technik, které dokážou rozpoznat kteroukoliv osobu na základě jejich anatomických vlastností. Mezi anatomické vlastnosti patří například otisk prstu, oční duhovka, oční sítnice, tvář, písmo, chůze, apod. Tato technologie člověka identifikuje rychle a spolehlivě.

4.4 OPRÁVNĚNÍ

Počet kombinací logických a mechanických klíčů k přístupu k funkcím EZS je udán v tabulce 4.3.

Úrovně přístupu 2,3 a 4	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Logický klíč	1000	10 000	100 000	1 000 000
Mechanický klíč	300	3 000	15 000	50 000

Tabulka 4.3: Požadavky na kódy oprávnění[10]

K zabezpečení přístupu k funkcím EZS může být použito i biometrických prostředků.

4.5 NAPÁJENÍ

Napájecí zdroj musí napájet EZS ve všech jeho stavech a také zálohovaných paměťových medií po požadovanou dobu. Tento zdroj je uložený v samostatném krytu nebo v jednom nebo více komponentech EZS.

Napájení dělíme na tři typy:

- typ A: základní napájecí zdroj a náhradní napájecí zdroj dobíjení EZS
- typ B: základní napájecí zdroj a náhradní napájecí zdroj nedobíjení EZS
- typ C: základní zdroj s omezenou kapacitou

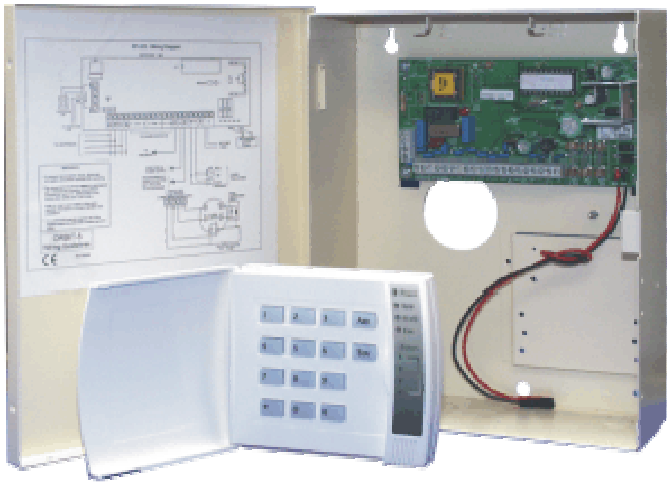
Přepnutí mezi základním napájecím zdrojem a náhradním napájecím zdrojem nesmí způsobit poplachový stav nebo jinak ovlivnit EZS. U napájecího zdroje typu C musí být doba, po kterou je tento zdroj schopen napájet EZS, jeden rok.

5. ÚSTŘEDNY EZS[13][14][15][16]

Ústředna je základní řídící jednotka systému elektronické zabezpečovací signalizace. Její funkce jsou:

- provádění shromáždění a vyhodnocení informací od senzorů
- signalizace a vysílaní informace o svých stavech
- ovládání poplachových, signalizačních a doplňkových prostředků
- napájení prvků EZS elektrickou energií
- umožňuje diagnostiku EZS

Na dnešní ústředny se můžeme dívat jako na mikropočítače s potřebnými rozhraními. Díky těmto rozhraním dochází k připojení senzoru, zobrazovacích zařízení, ovládací jednotky a také dalších ústředen. Jeden systém (EZS) může obsahovat více ústředen hierarchicky uspořádaných. U některých ústředen je možné rozdělit střežený prostor na zóny, to umožňuje pohyb v druhém patře a první střežit ve dvoupodlažním domě.



Obrázek 5.1: Zabezpečovací ústředna[12]

Ústředny rozlišujeme podle kabelového vedení na drátové a bezdrátové. Výhodou drátové ústředny je bezporuchový a stabilní provoz, také možnost zapojení velkého počtu detektorů. Naopak nevýhodou je náročnost údržby a vedení kabelových rozvodů v objektu. U bezdrátové ústředny je výhodou skoro bezúdržbový provoz a nezávislost na napájení. Jejich nevýhodou je vysoká cena ústředny a detektorů.

Ústředny jsou zálohovaný akumulátorem, kvůli nebezpečí výpadku elektrického proudu. Umístění ústředny by se mělo nacházet na místě, které není běžně přístupné a také odděleně od ovládající klávesnice. Často se umisťuje do různých komor nebo na toaletě.

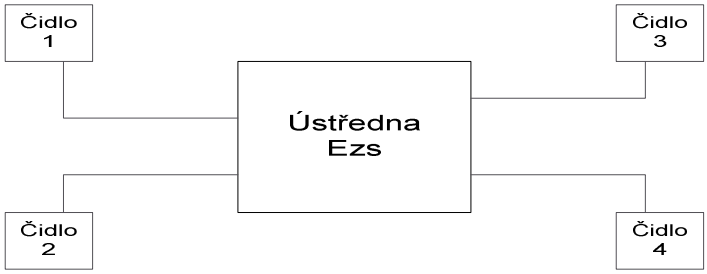
5.1 DĚLENÍ ÚSTŘEDEN

V zásadě lze ústředny EZS rozdělit podle možného způsobu připojování zabezpečovacích smyček k ústředně do čtyř hlavních skupin:

- smyčkové ústředny
- ústředny s přímou adresací senzorů
- ústředny smíšeného typu
- ústředny s bezdrátovým přenosem informací od senzorů

Smyčkové ústředny

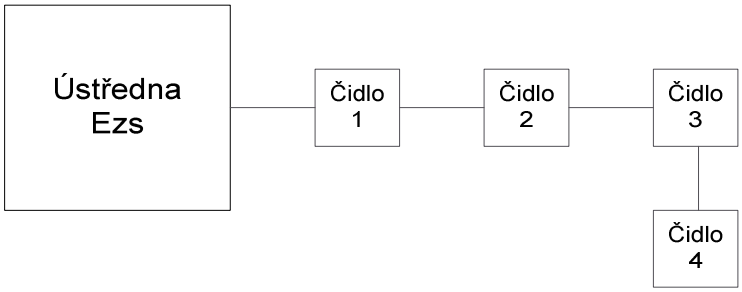
Charakteristické pro tyto ústředny je, že každá poplachová smyčka je napojena na samostatný vyhodnocovací obvod ústředny. Proudové smyčky mají danou hodnotu a toleranci. Tyto smyčky jsou zakončeny zakončovacím odporem tak, aby vykazovaly předepsanou hodnotu pro příslušný typ ústředny. Změnou této hodnoty, která může nastat aktivaci některého z čidel smyčky, dojde k vyhlášení poplachu. Systémy EZS obsahující smyčkovou ústřednu, jsou náročné na kabelovou síť, neboť ke každému čidlu je veden kabel příslušné smyčky.



Obrázek 5.2: Příklad zapojení systému EZS se smyčkovou ústřednou[13]

Ústředny s přímou adresací senzorů

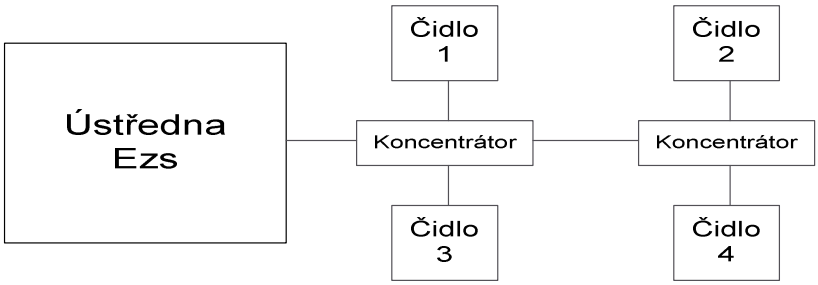
Komunikace mezi ústřednou a senzorem probíhá po datové sběrnici. Ústředna periodicky generuje adresy jednotlivých čidel a přijímá příslušné odezvy. Senzory jsou napojeny v libovolném pořadí a každý obsahuje komunikační modul.



Obrázek 5.3: Příklad zapojení systému EZS s ústřednou s přímou adresací senzorů[13]

Ústředny smíšeného typu

Komunikace mezi ústřednou a koncentrátorem (sběrnicový modul smyček) probíhá po datové nebo analogové sběrnici. Na koncentrátor jsou čidla připojeny pomoci smyček jako u smyčkových ústředen.



Obrázek 5.4: Příklad zapojení systému EZS s ústřednou smíšeného typu[13]

Ústředny s bezdrátovým přenosem informací od senzorů

- systém s jednosměrnou komunikací (simplex)
- systém s obousměrnou komunikací (duplex)

U simplexu má senzor vysílač a v ústředně je přijímač. U duplexu má senzor i ústředna jak vysílač, tak i přijímač.

5.2 VLASTNOSTI ÚSTŘEDNY EZS

Volba ústředny a jejího následného provedení je velice důležitá. Základními prvky při volbě ústředny jsou její vlastnosti.

Jednou z hlavních vlastností ústředny je maximální počet zón. Bezpečnostní zóna je prostor chráněny detektorem připojeným vedením nebo bezdrátově k ústředně. Takže počet zón udává rozsah zabezpečovacího systému. Rozlišujeme maximální počet zón připojených na základní desku ústředny a maximální počet zón v systému, protože u některých ústředen je možné připojit speciální modul, který rozšíří možný počet zón v systému. Zápis možného zapojení zón může vypadat např. takhle 2x5+2/4. Zápis vyjadřuje, že je možné připojit 10 zón na desku ústředny, plus 2 zóny do klávesnice a plus 4 zóny na expandér.

Mezi důležitou vlastnost patří také počet podsystémů. Díky podsystémům je možné rozdělit hlídaný prostor na samostatné části, které mají možnost mít svůj individuální režim zabezpečení, tím lze jednou ústřednou zabezpečit 2 až více objektů. Z toho plyne, že k ovládání podsystémů stačí jen jedna ústředna.

Další vlastností je přítomnost sběrnicové technologie. Digitální sběrnicový systém zajišťuje obousměrnou komunikaci mezi detektorem a ústřednou. Na sběrnici je možné připojit expandéry, bezdrátovou nástavbu a další moduly. Možnost připojení bezdrátové nástavby je také zajímavou vlastností, jedná se o připojení bezdrátového přijímače, se kterým jsou spojeny bezdrátové detektory a tím vzniká možnost vytvořit novou bezdrátovou zónu bez zásahu do zdiva.

Ústředny mohou být doplněny o komerční vlastnosti, mezi které patří FM rádio, hlasitý telefon, budík, přístupová práva přes telefon a vysoká kvalita hudby a hlasu.

5.3 TYPY ZÓN A REŽIMU

Podle typu zóny a režimu v jakém se ústředna vyskytuje je spuštěná odpovídající reakce ústředny. Mezi hlavní režimy zabezpečovací ústředny patří:

- vypnuto
- zapnuto
- zapnuta plášťová ochrana
- podsystémů

Při vypnutém režimu je ústředna neaktivní, je možný pohyb po objektu a na narušení detektorů ústředna nereaguje. Naopak při zapnutém režimu je ústředna

aktivní, po objektu se nikdo nepohybuje a narušení detektorů není ignorováno, ale dochází k reakci ústředny dle programu. Režim zapnuta plášťová ochrana je kombinaci režimů vypnuto a zapnuto, detektory tvoří dvě rozdílné skupiny. Jednou skupinou jsou detektory, které jsou aktivní a tvoří plášťovou ochranu a druhou jsou detektory, které jsou neaktivní. V tomto režimu je možný pohyb v domě, zatímco je dům chráněn před narušením z vnější strany. U režimu podsystémů dochází k rozdělení ústředny do podsystémů. Základní varianta je rozdělení na dva podsystémy. Hlídaný objekt je rozdělen na dvě samostatné části, které lze zapínat a vypínat samostatně. Jednotlivým uživatelům je přístup do těchto podsystémů buď povolen, nebo zakázán.

Detektory se dělí do zón. Dochází k volbě vlastností zón a druhu reakce systému na narušení detektorů. Mezi nejčastěji používané zóny patří:

- okamžitá zóna
- zpožděná zóna
- podmínečně zpožděná zóna
- 24 hodinová zóna
- plášťová (Stay)

Při okamžité zóně, pokud je ústředna v režimu vypnuto, je ignorováno narušení detektorů a pokud je v režimu zapnuto, dojde k okamžitému poplachu při narušení detektorů. Při zpožděné zóně, pokud je ústředna v režimu vypnuto, je ignorováno narušení detektorů a pokud je v režimu zapnuto, spustí se čas pro příchod při narušení detektorů. Během tohoto času musí dojít k zadání správného kódů, pokud k tomu nedojde do určené doby, dojde k aktivaci poplachu. Při podmínečně zpožděné zóně, pokud je ústředna v režimu vypnuto, je ignorováno narušení detektorů a pokud je v režimu zapnuto a dojde k narušení během času zpoždění pro

příchod je poplach aktivován až po uplynutí tohoto času, nedojde-li k vypnutí do stanoveného limitu pro příchod. Při 24 hodinové zóně, dojde k okamžitému poplachu při narušení detektorů, pokud je ústředna v režimu zapnuto i vypnuto. Při plášťové zóně, pokud je ústředna v režimu vypnuto, je ignorováno narušení detektorů, pokud je v režimu zapnuto, dojde k okamžitému poplachu při narušení detektorů a pokud je v režimu zapnuto Stay, tak narušení zóny definováno jako STAY je ignorováno.

5.4 OVLÁDANÍ ÚSTŘEDEN

Ovládání ústředen může být manuální a to klávesnicemi, nebo dálkové a to pomocí mobilu a klíčenek.

Klávesnice

Ústředna je ovládána klávesnicí, se kterou je přímo propojena. Díky klávesnici lze zjistit informace o poruchách a stavu detektorů. Klávesnice slouží také k naprogramování ústředny a k informování o stavu EZS. Pro programování je potřeba se instalačním kódem dostat do režimu programování, zadat adresu a zadat data. Klávesnice jsou dodávány ve dvou základních provedeních a to buď LED klávesnice, nebo LCD klávesnice.

Obrázek 5.5: Led klávesnice[17]

Pro představu o funkci LED klávesnice uvedené na obrázku slouží následující popis klávesnice. Popis slouží pouze pro systém na obrázku, každá firma má svůj způsob signalizování stavu, ale princip je v podstatě stejný. LED AC signalizuje svitem napájení ze sítě AC a naopak při zhasnutí signalizuje vadné napájení. LED READY signalizuje svitem zelené barvy, že všechny detektory jsou v klidu a možnost zapnutí systému. LED ARM signalizuje svitem, že systém je v chodu a blikáním signalizuje poplach v systému. Klávesy 1 až 10 znázorňují zóny shodného čísla a jejich svit vyjadřuje stav, ve kterém se nachází. Pokud klávesa svítí, zóna je narušena, a pokud klávesa nesvítí, zóna je v klidu. U klávesy TBL je svitem signalizovaná porucha v systému a následným stiskem klávesy přejde klávesnice do režimu zobrazení poruch. U klávesy MEM je svitem signalizováno upozornění na stav, kdy během posledního zapnutí byl v systému poplach.

Klávesnice LCD jsou schopné stejně dobře podávat informace o stavech systému jako klávesnice LED, jen je rozdíl v zobrazení. Místo svitu kláves se údaje přímo vypisují na displeji. Mezi výhody klávesnic LCD patří možnost listovat v historii ústředny, a tím mít přehled, co se stalo v systému v určitý čas.

Přístupová bezdotyková karta

K aktivaci a deaktivaci alarmu stačí přiložit kartu ke čtečce. U systémů s vyšším zabezpečovacím stupněm je potřeba kombinace s kódem vloženým na klávesnici.

Bezdrátový kódovaný ovladač

K aktivaci a deaktivaci alarmu stačí stisknout tlačítko na dálkovém ovladači.

Mobilní telefon

Tato možnost připadá v úvahu, pokud je systém osazen GSM komunikátor, pak lze ovládat a zjišťovat stav ústředny odkudkoliv mobilním telefonem.

6. FUNKCE ÚSTŘEDNY [18]

Vstupy slouží k příjmu a identifikaci poplachových, sabotážních, poruchových signálů a zpráv. Jsou schopné taky přijímat a identifikovat jiné signály a zprávy. Díky provozním funkcím je ústředna schopna reagovat automaticky nebo na manuální příkazy uživatele. Zpracování umožňuje ústředně zpracování signálů a zpráv od detektorů a tísňových hlásičů, vyhodnocení sabotáže a monitorování funkcí a odezvu na uživatelské instrukce. Výstupy zajišťují předání informací uživateli o vyhlášení nebo signalizaci poplachu, poruchy nebo sabotáže. Pomoci sabotážní ochrany dochází k detekci sabotáže pomoci elektrických, elektronických nebo jiných prostředků a pomáhá odolávat sabotáži použitím fyzických prostředků. Další funkcí je monitorování, které slouží ke sledování správné funkce ústředny a propojení. Je závislá na stupni zabezpečení.

Vstupy

Vstupy přijímají a zpracovávají v závislosti na stupni zabezpečení signály a zprávy z různých zařízení, tak jak je dáno v následujících šesti bodech.

Detekce narušení **–** příjem a zpracování signálů a zpráv z detektorů.

Tísňové zařízení **–** příjem a zpracování signálů a zpráv z tísňových zařízení.

Sabotáž **–** příjem a zpracování sabotážních signálů a zpráv.

Porucha **–** příjem a zpracování poruchových signálů a zpráv.

Monitorování – ověření, že ústředna a propojení pracují správně.

Uživatelský vstup – příjem a zpracování informací ze zařízení uživatelských vstupů

Provoz

Ústředna musí obsahovat prostředky umožňující oprávněný přístup uživatele k jejím funkcím. Přístupové úrovně a oprávnění jsou popsány v kapitole č. 6.4 a 6.5.

K nastavování do stavu střežení je zapotřebí, aby ústředna nabízela uživateli prostředky s příslušnými úrovněmi přístupu. Ústředna může umožňovat automatické nastavení stavu střežení v předem daný čas, pokud ano, musí generovat minimálně jednu signalizaci, než dojde k uvedení do stavu střežení. Ústředna je povinná mít prostředky pro uživatele s příslušnou přístupovou úrovní k nastavení do stavu klidu. Ústředna může umožňovat nastavení do stavu klidu v předem daný čas. Vybavení příchodovou trasou je volitelné. Pokud se jedná o řešení pomocí příchodové trasy, ústředna musí obsahovat prostředky ke stanovení poplachových bodů na ní. Dobu umožňující ukončit uvádění do stavu klidu musí byt ústředna schopna omezit maximálně na 45 s. Pokud je tato doba překročena, musí byt vyhlášen poplach. Pokud dojde k poplachu během uvádění do stavu klidu, je poplach signalizován nebo vyhlášen jenom vnitřním výstražným zařízením. Správnost nastavení do stavu klidu musí bytí signalizována a signalizace nesmí být delší než 30 s.

Zpracování

Ústředna musí být schopna zpracovávat vstupní signály nebo zprávy a generovat výstupní signály či zprávy a signalizace. Zpracování narušení, tísňových, sabotážích a poruchových signálů nebo zpráv musí proběhnout samostatně tak, aby generovaly jeden nebo více poplachových stavů. Pokud při zpracování uživatelských vstupů ústředna umožňuje uživateli prostředky k signálům nebo zprávám vstupů nebo příkazům na ústředně nebo ovládacím zařízení, musí přístup k zvoleným funkcím odpovídat:

- stupni zabezpečení
- přístupové úrovni
- každé podskupině přístupové úrovně podle dokumentace výrobce

Monitorování provozu

Ústředna, která je programově řízena zpracováním sériových dat musí obsahovat prostředky k monitorování provozu podle stupně zabezpečení, při stupni zabezpečení 1 a 2 volitelně a při stupni zabezpečení 3 a 4 povinně.
Musí byt splněny následující podmínky:

- detekce poruchy generátoru časové základny musí proběhnout během 10 s.
- ústředna musí obsahovat pro stupeň zabezpečení 4 výstup, který je povinný změnit stav, pokud je zapnuto monitorování provozu.
- činnost monitorování provozu pro stupeň zabezpečení 3 a 4 musí uskutečnit pokus restartovat procesor a generovat na ústředně poruchový signál nebo zprávu.
- pokud dojde k restartování ústředny podle předešlého bodu, musí navázat na činnost v předešlém provozním stavu.

Signalizace

Signalizace musí být k dispozici, i přestože jsou signalizace sdruženy do společných prostředků hlášení. Může docházet k signalizaci na přístupové úrovni 1, že informace je dostupná na dalších přístupových úrovních. Signalizace poplachu, sabotáže a poruchy si musí vynutit potvrzení uživatele, pokud k tomu dojde, musí signalizace probíhat aspoň do vynulování těchto stavu. Signalizace stavu střežení musí být omezena na maximálně 180 s po ukončení uvádění do tohoto stavu.

Signalizace stavu klidu je omezena na maximálně 30 s po ukončení uvedení do tohoto stavu.

Zabezpečení proti sabotáži

Úkolem zabezpečení proti sabotáži je zmenšit riziko sabotáže na minimum, k tomu slouží kryty komponentů, které musí mít prostředky k zamezení přístupu k jejich vnitřním prvkům podle stupně zabezpečení ústředny a všechny připojení vedoucí k ústředně musí být uvnitř krytu ústředny. Ústředna musí být zabezpečena tak, aby vniknutí do ústředny bylo možné pouze v případě použití příslušného nářadí.

Propojení

Ústředna může využívat přímá nebo datová sběrnicová propojení. Pro správnou funkčnost musí ústředna mít prostředky k potvrzení funkčnosti propojení. Na potvrzení o správné funkčnosti propojení musí byt ústředna připravena v časech a to při stupni zabezpečení 1 do 240 minut, při stupni zabezpečení 2 do 120minut, při stupni zabezpečení 3 do 100 sekund a při stupni zabezpečení 4 do 10 sekund. Pokud nelze zjistit potvrzení propojení z důvodu poruchového stavu musí byt zajištěno generování poruchových zpráv nebo signálů pro všechny stupně zabezpečení.

Záznam události

Záznam povinné události musí proběhnout během 10 s od vzniku události a nesmí být přepsán nebo ovlivněn nepovinnou události. V ústředně není možné mazat nebo měnit obsah paměti události, pouze v případě, že je kapacita paměti ústředny plná, pak jsou mazány nejstarší události. Dále musí každá uložena událost ve stupních zabezpečení 2, 3 a 4 obsahovat čas a datum vzniklé události.

7. STAVOVÝ AUTOMAT[20][21][22]

Stavové automaty slouží k modelování dynamického chování systému. Díky nim, lze vyjádřit stavy modelovaného elementu a přechody mezi jednotlivými stavy. Při průchodu mezi jednotlivými stavy mohou probíhat různé akce. Takže stavový automat je v podstatě model skládající ze tří základních stavebních prvků: stavů systému, přechodu mezi stavy a akcemi.

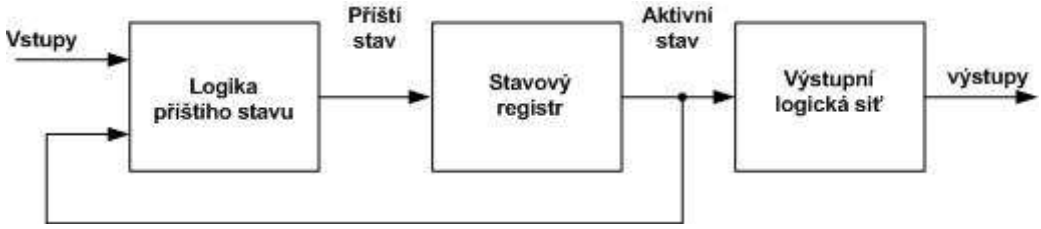
7.1 DĚLENÍ STAVOVÝCH AUTOMATŮ

Obecně dělíme stavové automaty na dva základní typy. Prvním typem je stavový automat poznávací, u kterého je výstupem binární informace. Tato informace určuje, jestli daný automat přijme danou posloupnost vstupu a je na ni adekvátní odpověď. Druhým typem je stavový automat převodový, u kterého je výstup závislý na přijatém vstupu a aktuálním stavu systému. Dalším dělením stavových automatů je na deterministický a nedeterministický. Deterministický má vždy pro jednu dvojici stav-vstup pouze jeden přechod, nedeterministický má možnost mít více přechodů z daného stavu, ale podmínkou je jeden konkrétní vstup.

Dále rozlišujeme dva druhy stavových automatů: Moorův a Mealyho. Rozdíly mezi těmito dvěma automaty spočívají v:

Moorův automat

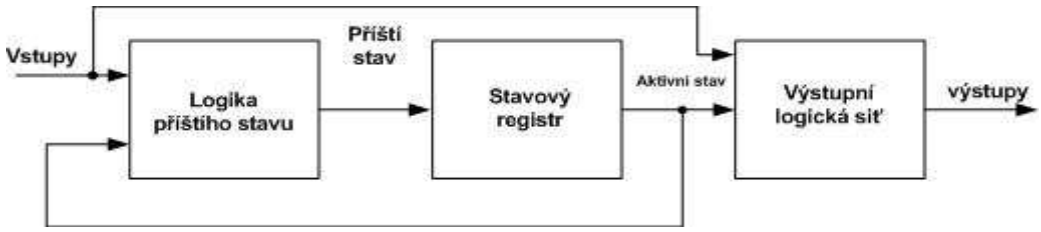
- závislost výstupní signály jen na stavu automatu
- změna výstupu jen v okamžiku aktivní hrany hodinového signálu



Obrázek 7.1: Blokové schéma Moorova automatu[20]

Mealyho automat

- závislost výstupní signály i na vstupních signálech
- kombinační výstupy reagují okamžitě na změny signálů, na nichž jsou závislé
- výstupní signály mohou být dány kombinační logikou nebo kombinační logikou s registrovaným výstupem



Obrázek 7.2: Blokové schéma Mealyho automatu[20]

7.2 POPIS STAVOVÝCH AUTOMATŮ

Popis stavových automatů můžeme rozdělit do dvou rovin, a to popis struktury a popis funkce (chování). Popis struktury bývá vyjádřen blokovým schématem, z něhož vyplývají obecné vlastnosti automatu a možnosti jeho použití. Chování automatu vychází i z elektrického schématu, ale nejpřehlednější je pro popis

chovaní stavový diagram. Převod mezi stavovým diagramem a elektrickým schématem je proveditelný automaticky pomoci návrhových systému.

Stavový diagram je v informatice způsob grafického zápisu vývoje systému, který má konečný počet stavů. Popisuje všechny stavy daného objektu a přípustné přechody mezi nimi.

Stavový diagram definuje pojmy:

- stav systému
- přechod mezi stavy
- událost
- aktivita/akce
- podmínka
- počáteční/koncový stav

Stav systému

Pod pojmem stav si můžeme představit trvání konfigurace neměnných podmínek v systému. Během stavu objekt čeká, buď na událost, nebo než se nějakým způsobem objekt zachová. Stavy jsou znázorněny pomocí obdélníku se zaoblenými rohy a názvem umístěným v horní části, kromě počátečního a koncového stavu. Stav je určen:

- hodnotami daného objektu,
- relacemi s dalšími objekty
- aktuálně vykonávanou aktivitou
- může obsahovat libovolný počet akcí a aktivit.

Přechod mezi stavy

Přechod slouží k propojení jednotlivých stavů, které směřuje od počátečního stavu k cílovému. K přechodu dojde, pokud nastane specifikovaná událost, musí být splněny specifikované podmínky a provede se specifikovaná akce.

Akce/ Aktivita

Akce je činnost, která probíhá během přechodu mezi stavy nebo také při vstupu nebo výstupu z určitého stavu. Akce proběhne rychle a je nepřerušitelná. Aktivita je delší proces než akce a naopak od akce je to možné aktivitu přerušit.

Událost

Příkladem události může být signál, volání, ukončení ohraničeného časového úseku nebo okamžiky ukončení vykonání určitých činností. Jméno události identifikuje každý přechod na diagramu stavu.

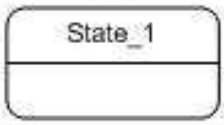
Podmínka

Podmínka musí být splněna, aby došlo k přechodu ze stavu do stavu.

Počáteční/koncový stav

Počáteční stav je stav bez vnitřní činnosti. V tomto stavu je objekt automaticky v počáteční chvíli a znázorňuje grafickou oblast, ve které začíná proces změny stavu. Koncový stav je stav, ve kterém se objekt nachází automaticky po ukončení práce. Koncový stav znázorňuje oblast, ve které končí proces změny stavu objektu.

Grafické znázornění těchto pojmu je uvedeno v následující tabulce:

Počáteční stav	
Koncový stav	
Stav	
Přechod	
Událost	event /
Akce	/ action
Podmínka	[Condition]

Tabulka 7.1: Grafické znázornění pojmů[22]

8. NÁVRH STAVOVÉHO AUTOMATU MALÉ ZABEZPEČOVACÍ ÚSTŘEDNY

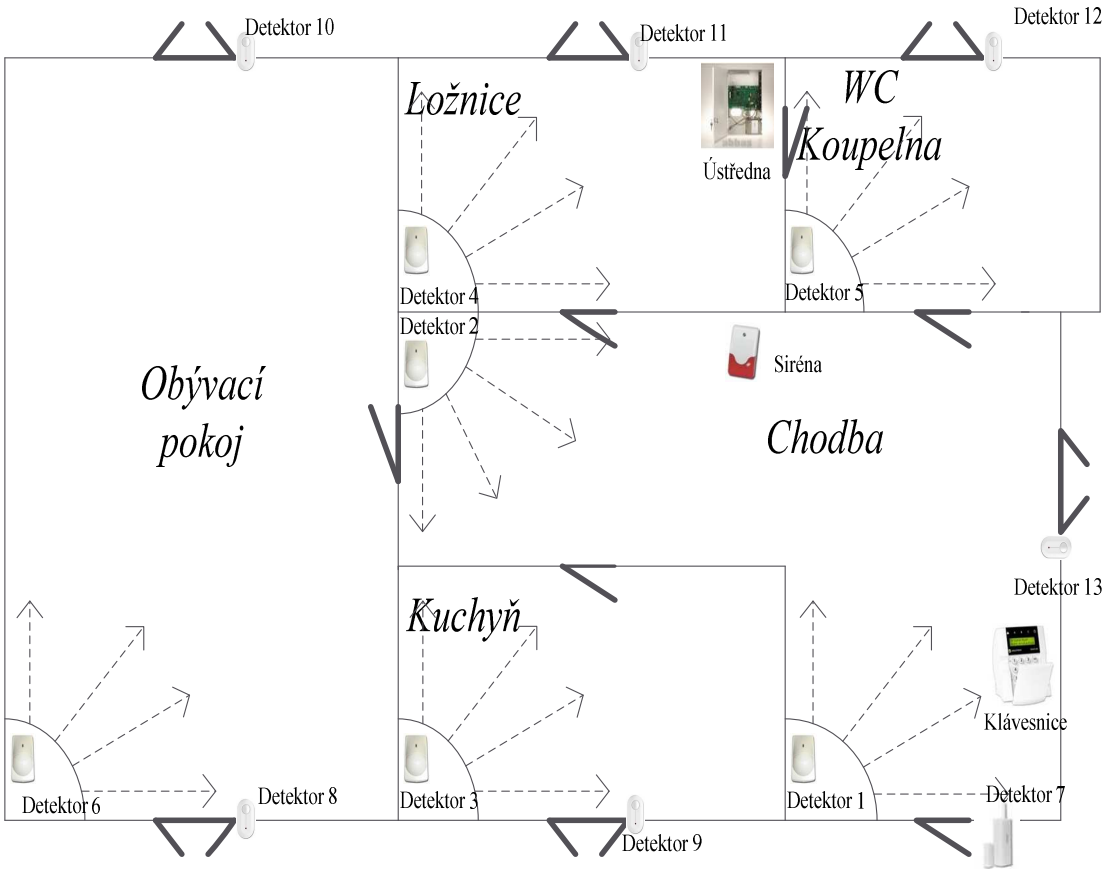
Tento návrh stavového automatu menší zabezpečovací ústředny, bude schopen řídit zabezpečovací systém malého přízemního rodinného domku. Pro názorné vysvětlení funkcionality stavového automatu menší zabezpečovací ústředny byl navržen zabezpečovací systém malého přízemního rodinného domku, který bude tímto stavovým automatem řízen.

8.1 ZABEZPEČOVACÍ SYSTÉM MALÉHO PŘÍZEMNÍHO RODINNÉHO DOMKU

Zabezpečovací systém se skládá ze zabezpečovací ústředny, klávesnice, detektorů, vnitřní sirény a kabeláže, kterou jsou tyto prvky propojeny. Jelikož se jedná o přízemní rodinný dům je použita jak prostorová, tak i plášťová ochrana. Systém obsahuje pouze jeden podsystém, jelikož dům je jednopatrový bez garáže a pro zabezpečení jednoho patra postačí jeden podsystém, v kterém bude možno použít 3 režimy zabezpečení.

8.1.1 Použité prvky EZS

Jednotlivé prvky jsou rozmístěny po domě tak, aby byl zabezpečen každý jednotlivý pokoj v domě a aby prvky co nejlépe plnily svou funkci. Rozmístění je zobrazeno na obr. 8.1.



Obrázek 8.1: Umístění prvku EZS v domě

Zabezpečovací ústředna je jádrem zabezpečovacího systému. Její hlavní úlohou je přijímání a vyhodnocování výstupních signálů od detektorů, také napájí další prvky EZS elektrickou energii. Ústředna je umístěna v ložnici, kde je mimo dohled a dosah neoprávněných osob.

Klávesnice ovládá zabezpečovací systém, ukazuje stav systému a jeho jednotlivých bezpečnostních smyček. Klávesnice je umístěna u vstupních dveří, aby byla rychle přístupna po příchodu do domu, k zadání kódu pro vypnutí zabezpečovacího systému.

Siréna je piezoměnič, který po přivedení napětí vydává akustický signál. Siréna slouží k akustickému upozornění na narušení domu a je nainstalovaná v chodbě, aby se poplach rozléhal po celém domě.

Pohybový detektor je tvořen optickou částí, která zajišťuje správné nasměrování infrapaprsků do ohniska, ve kterém se nachází PIR senzor. Ten vytváří elektrický proud odpovídající danému pohybu. Signál je potom zpracován speciálními obvody, které provedou následné rozhodnutí o aktivaci detektoru nebo ponechání v klidu. Pohybovým detektorem je vybavena každá místnost v domě, dokonce v chodbě jsou tyto detektory dva, aby byla pokryta celá plocha místnosti.

Detektor tříštění skla vyhodnocuje slyšitelnou část zvuku, která vzniká tříštěním skla a tlakovou vlnu, která vzniká v okamžiku rozbíjení skla. Tlaková vlna a slyšitelná část zvuku jsou monitorovány mikrofonem, pokud dojde ke splnění časového průběhu a intenzity obou složek, dojde k vyhlášení narušení. Tímto detektorem je vybaveno každé okno v domě.

Magnetický kontakt je tvořen jazýčkovým relé s drátovým vývodem, které je připevněno na pevnou část rámu a na pohyblivou část dveří je připevněn magnet. Při zavření dveří se relé sepne a naopak při otevření rozepne a tím se spustí příchodový čas, během kterého musí být zadán kód pro vypnutí zabezpečovacího systému. Tedy se jedná o rozpínací kontakt, kterým jsou vybaveny vstupní dveře domu.

8.1.2 Použité typy ochrany

Pro zabezpečení tohoto objektu byly použity dva druhy ochrany a to:

- plášťová ochrana
- prostorová ochrana

Plášťová ochrana signalizuje narušení pláště zabezpečeného domu, při němž je detekováno narušení oken a dveří. K detekci jsou použity detektory tříštění skla a detektor dveří. Pokud tato ochrana selže nebo je obelstěná útočníkem, je v záloze ochrana prostorová.

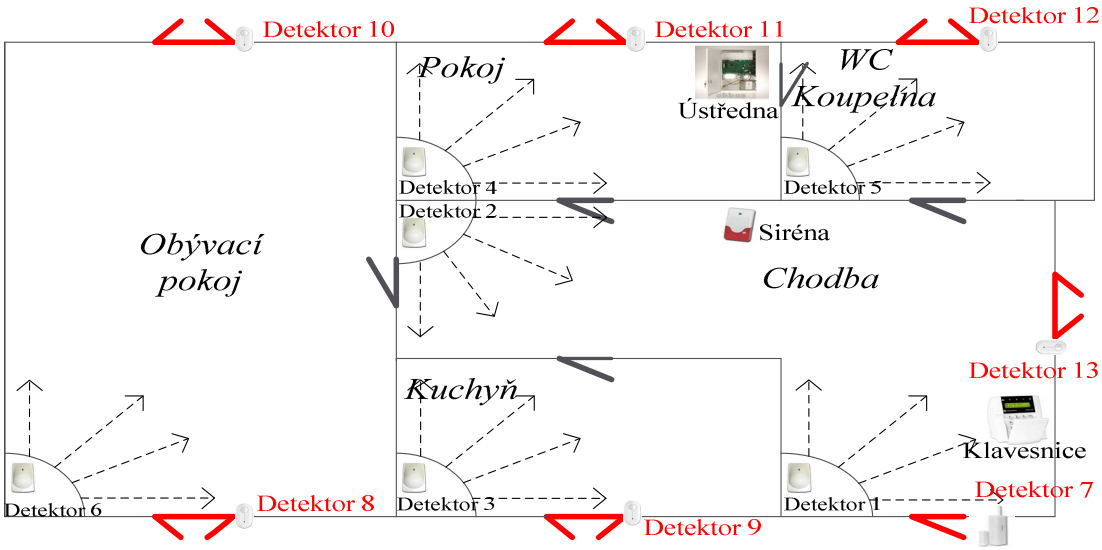
Prostorová ochrana signalizuje narušení vnitřku zabezpečeného domu, k tomuto účelu slouží pohybové detektory, které pokud jsou aktivní, zaregistrují pohyb ve střeženém prostoru.

8.1.3 Použité typy režimu

Zabezpečovací systém nabízí 3 typy režimů, v kterých může být systém zabezpečen:

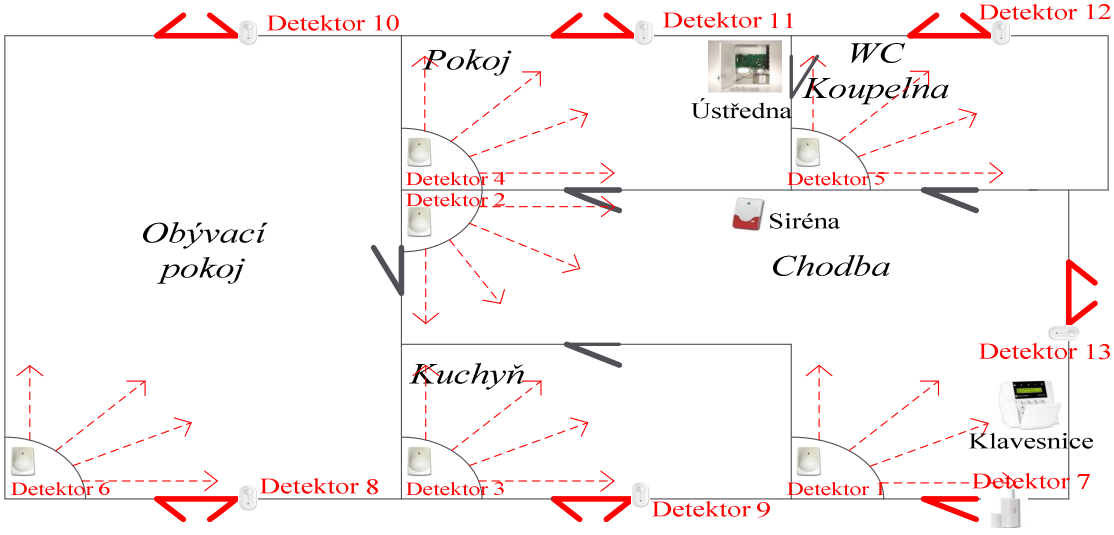
- režim Den
- režim Odchod
- režim Noc

Režim Den hlídá pouze obvod domu, tedy se jedná o plášťovou ochranu, ochrana vnitřku zůstává vypnuta, uživatel se tedy může pohybovat po domě beze strachu, že by někdo nepozorovaně vnikl do domu. Z toho je zřejmé, že pohybové detektory budou neaktivní a naopak detektory dveří a oken budou zapnuty, jak je zobrazeno na obr. 8.2, aktivní detektory jsou označeny červeně.



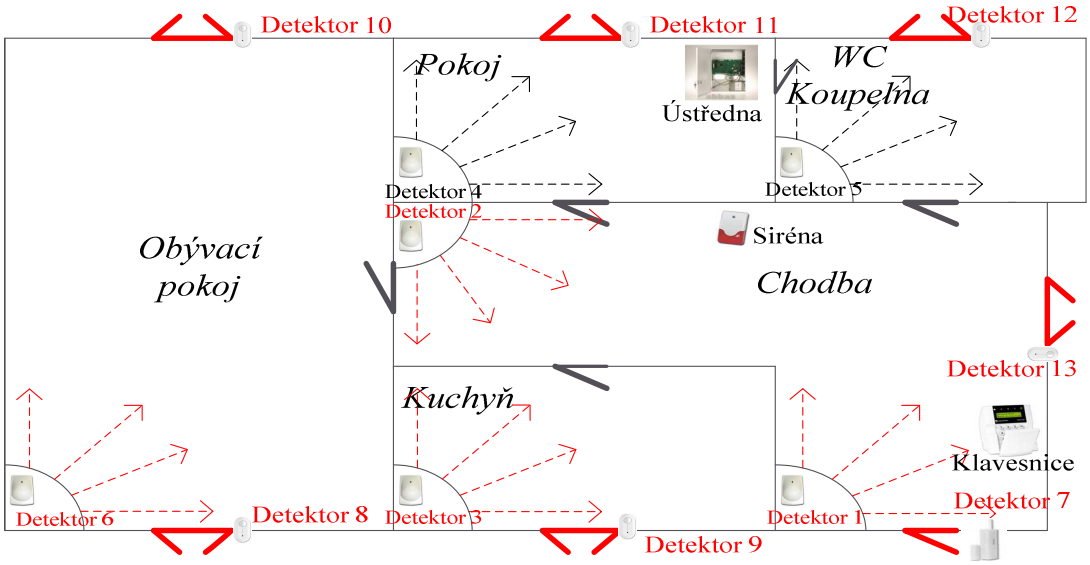
Obrázek 8.2: Funkční detektory při režimu Den

Režim Odchod se používá pro ochranu domu při nepřítomnosti uživatele v domě. Tento režimu hlídá jak obvod domu, tak i vnitřek domu, tedy jsou aktivní obě ochrany plášťová i prostorová. Jestliže je aktivován tento režim, detekují pohybové detektory i detektory dveří a oken, jak je zobrazeno na obr. 8.3. Aktivní detektory jsou označeny červenou barvou.



Obrázek 8.3: Funkční detektory při režimu Odchod

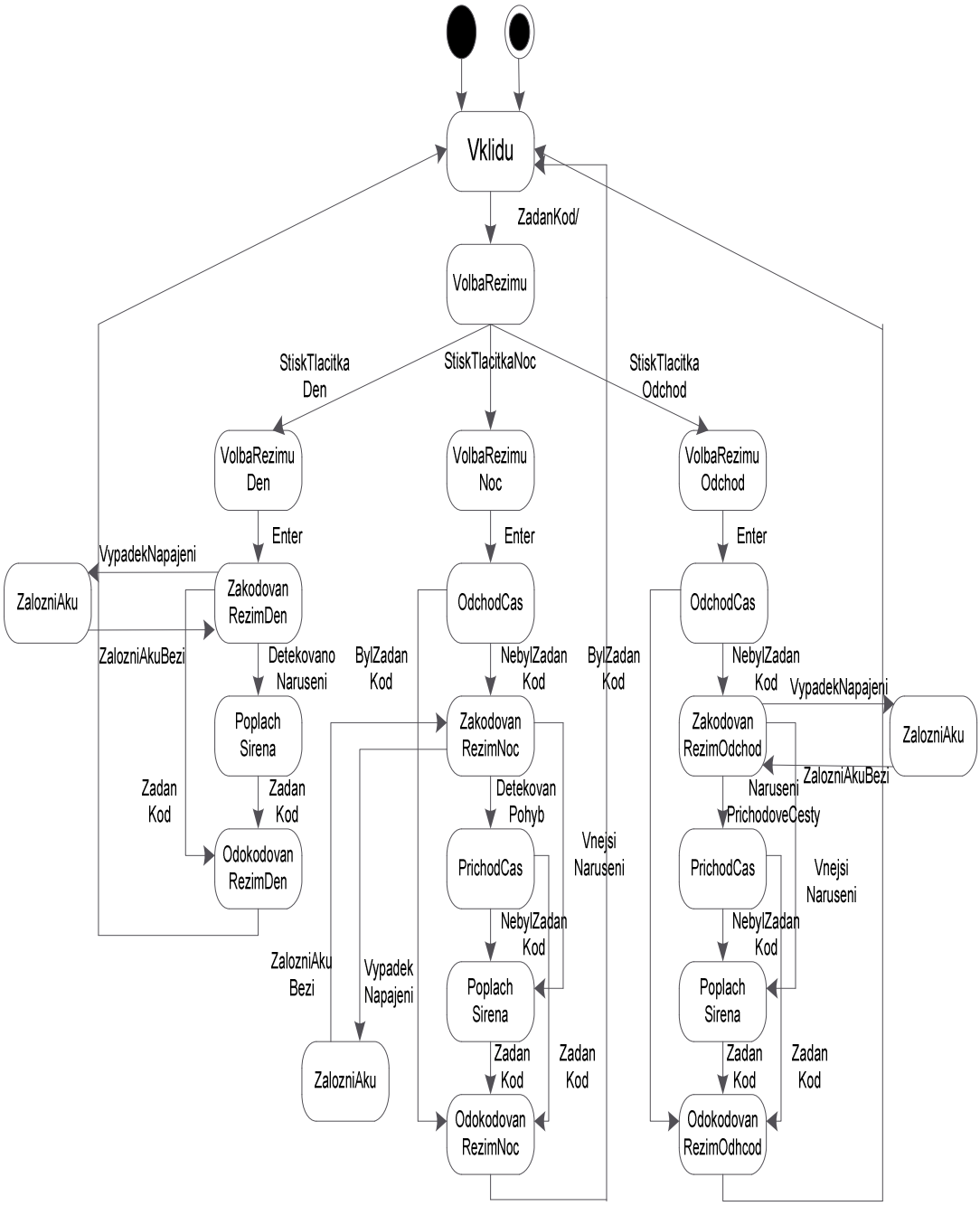
Režim Noc se používá hlavně pro ochranu domu v nočních hodinách. Uživateli umožní pohybovat se v místnostech určené na spánek, a zároveň si dojít na toaletu, ostatní místnosti jsou zabezpečeny pohybovými detektory. Aktivní jsou také všechny detektory plášťové ochrany, jak si můžeme prohlednout na obr. 8.4. Aktivní detektory jsou označeny červenou barvou.



Obrázek 8.4: Funkční detektory při režimu Noc

8.2 STAVOVÝ AUTOMAT

Navržený stavový automat menší zabezpečovací ústředny, který má řídit navržený zabezpečovací systém malého rodinného domku, je zobrazen na obr. 8.5.



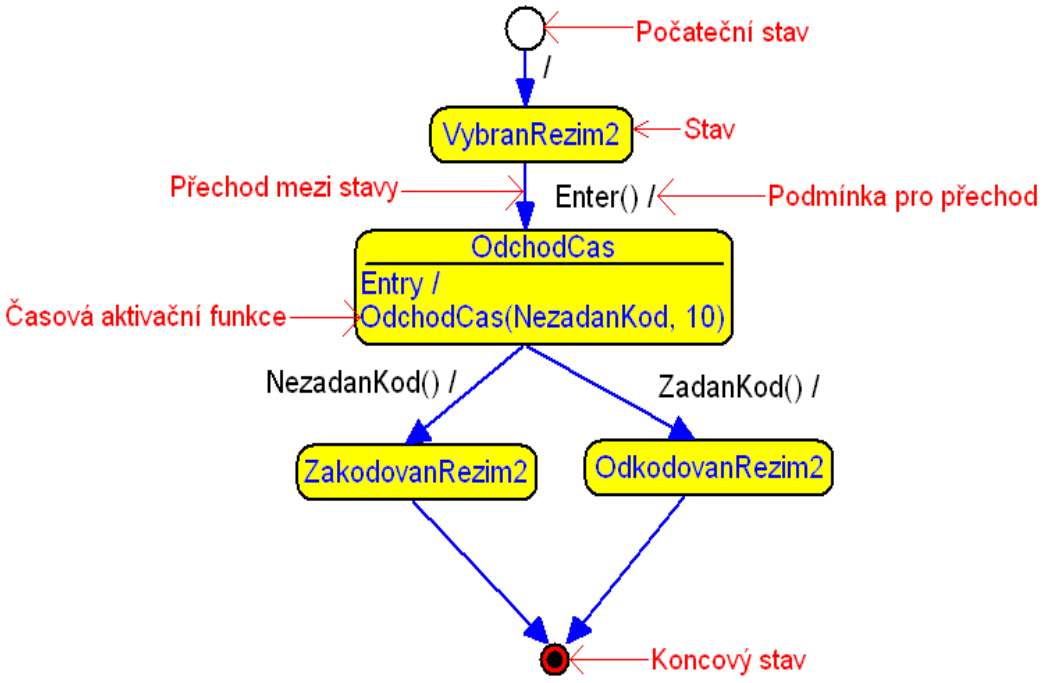
Obrázek 8.5: Navržený stavový automat menší zabezpečovací ústředny

Stavový automat se skládá ze stavů, mezi kterými se může systém pohybovat splněním určitých podmínek, tyto podmínky mohou byt splněny pomocí uživatele a to pomocí klávesnice nebo vyhodnocováním stavu detektoru.

Stavový automat byl pro přehlednost rozdělen na 4 stavové automaty:

- stavový automat Výběr režimu
- stavový automat Režim Den
- stavový automat Režim Odchod
- stavový automat Režim Noc

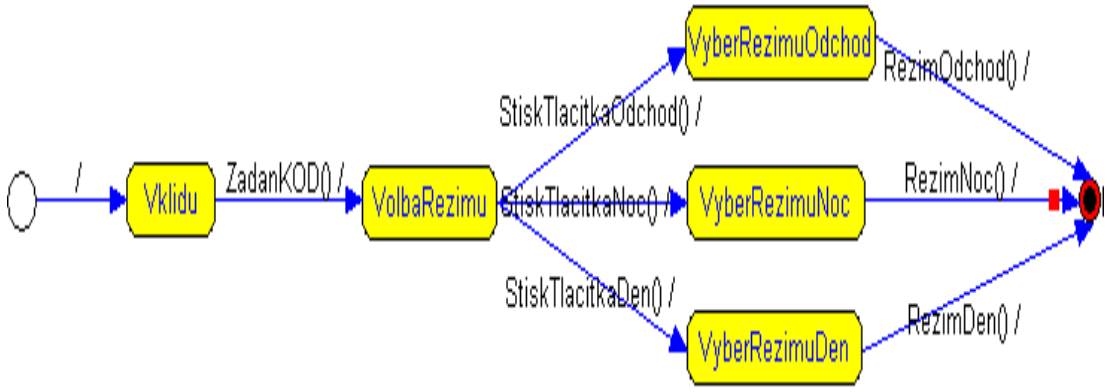
Každý z těchto 4 stavových automatu byl odladěn v programu Visualstate. Pro vysvětlení syntaxe zápisu stavového automatu v prostředí Visualstate, byl na obr. 8.6 popsán jednoduchý stavový automat.



Obrázek 8.6: Syntaxe zápisu stavového automatu v prostředí VisualState

8.2.1 Stavový automat Výběr Režimu

První stavový automat uživateli nabízí výběr režimu, v kterém má byt objekt zabezpečen.

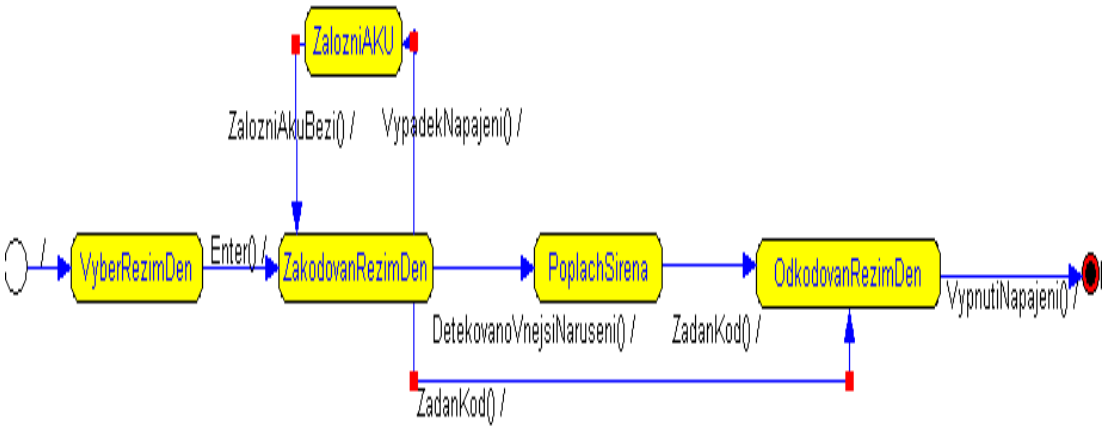


Obrázek 8.7: Stavový automat Výběr Režimu

Pokud se systém nachází ve stavu vklidu, jsou všechny detektory v klidu a není zapnut žádny z režimu. Jestli chce uživatel nějaký režim vybrat, musí na klávesnici zadat svůj uživatelský kód, následně systém přejde do stavu VolbaRezimu a uživateli se naskytne možnost vybrat si z 3 režimů, jak je vidět na obr. 8.7, a to podle toho jestli chce uživatel opustit dům, pak musí stisknout tlačítko Odchod, nebo chce jít spát, pak musí stisknout tlačítko Noc anebo chce jen dům zabezpečit před vnějším narušením, pak musí zvolit tlačítko Den.

8.2.2 Stavový automat Režim Den

Pokud byl vybrán ve stavovém automatu Výběr režimu režim Den, následuje stavový automat Režim Den.

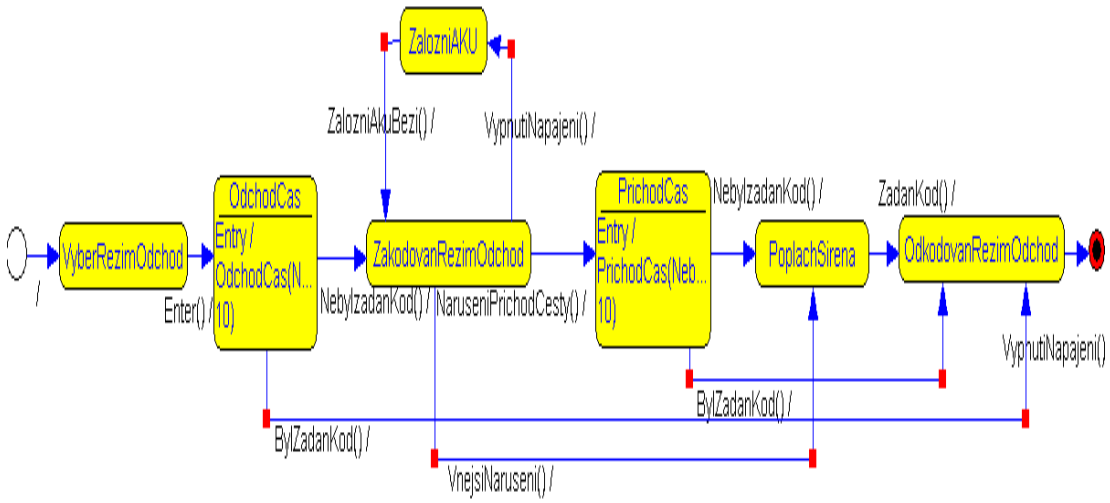


Obrázek 8.8: Stavový automat Režim Den

Zde systém čeká na potvrzení výběru režimu, a to uživatel provede stisknutím tlačítka Enter na klávesnici, pokud k tomu dojde systém, je okamžitě zakódován a detektory detekují. V tomto stavu systém čeká, jestli nebude zadán uživatelský kód, potom by byl, systém ihned odkódován a systém by se vrátil do stavu vklidu nebo jestli nebude detekováno vnější narušení, pokud k tomu dojde, je spuštěn poplach, který bude trvat, dokud uživatel nezadá uživatelský kód, poté systém je odkódován a vrací se do stavu vklidu.

8.2.3 Stavový automat Režim Odchod

Pokud byl vybrán ve stavovém automatu Výběr režimu režim Odchod, následuje stavový automat Režim Odchod.

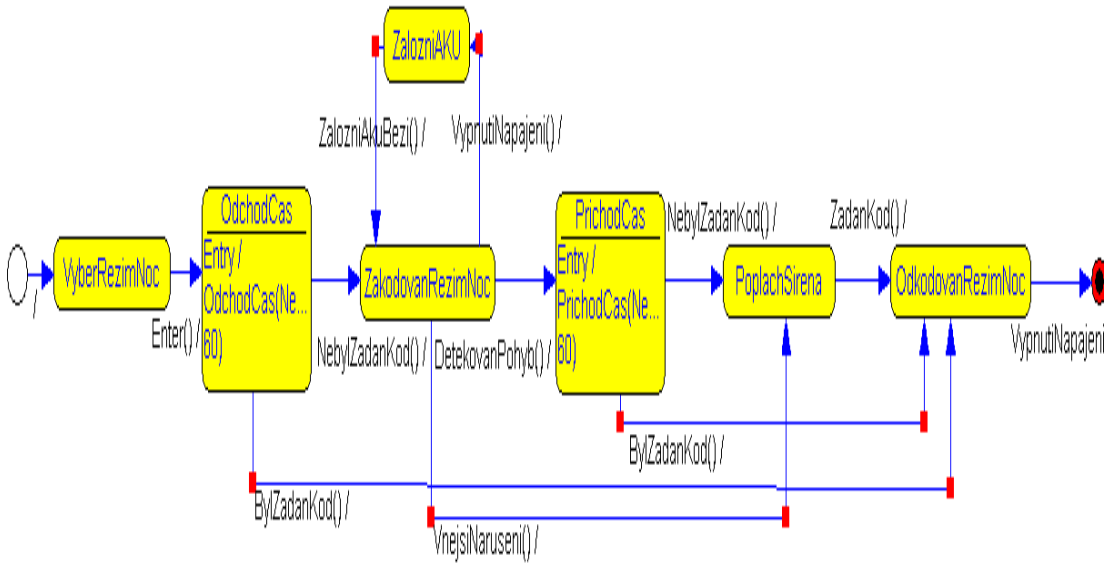


Obrázek 8.9: Stavový automat Režim Odchod

Zde systém čeká na potvrzení výběru režimu a to uživatel provede stisknutím tlačítka Enter na klávesnici, po potvrzení systém spustí odchodový čas, během kterého má uživatel opustit byt, pokud tak učiní a nezadá uživatelský kód, dojde k zakódování režimu, pokud si odchod rozmyslí, může zadat uživatelský kód a systém přechází do stavu, kdy je režim Arm odkódován, tedy systém je vklidu. Pokud je systém zakódován a dojde k narušení vnějšího obvodu je ihned spuštěn poplach, ale jestliže dojde k narušení přístupové cesty, spustí se příchodový čas, během kterého má uživatel čas zadat uživatelský kód. Pokud bude kód zadán, systém přejde do stavu kdy je režim Arm odkódován, v případě nezadání kódu bude spuštěn poplach.

8.2.4 Stavový automat Režim Noc

Pokud byl vybrán ve stavovém automatu Výběr režimu režim Noc, následuje stavový automat Režim Noc.



Obrázek 8.10: Stavový automat Režim Noc

Princip tohoto stavového automatu je téměř stejný jako u stavového automatu režim Noc, až na to, že při zakódování tohoto režimu je poplach spuštěn při narušení vnějšího obvodu nebo přístupové cesty a při detekci pohybu v chodbě se spustí příchodový čas na zadání uživatelského kódu.

9. ZÁVĚR

Během psaní této bakalářské práce jsem se obeznámil s funkcemi přístupových systému a s výhodami, které přinášejí do běžného i profesního života. Dále jsem se seznámil se zabezpečovacími systémy, jaké existují způsoby zabezpečení a druhy ochrany a které druhy detektorů k tomu slouží. Vypracoval jsem pohled na základní věci, které je třeba zvážit před výběrem zabezpečení objektu. Poté jsem se zaměřil na zabezpečovací ústředny, na jejich rozdělení, na způsob jejich komunikace s PCO, na jejich vlastnosti a na jejich funkce. Další problematikou, kterou jsem se zaobíral, byly stavové automaty, jejich dělení a popis.

Na základě informací dosažených psaním této bakalářské práce jsem navrhl stavový automat pro menší zabezpečovací ústřednu, který jsem pro přehlednost rozdělil na 4 samostatné stavové automaty a následně je odladil v programu IAR visualSTATE. Pro názorné vysvětlení funkcionality stavového automatu menší zabezpečovací ústředny jsem navrhl zabezpečovací systém malého přízemního rodinného domku, který bude tímto stavovým automatem řízen.

10. SEZNAM LITERATURY

[1] *Přístupové systémy* [online]. 2006 [cit. 2009-02-20]. Dostupný z WWW: http://www.z-ware.cz/?-6-aktuality

[2] VELEK, Martin. *Přístupový systém založený na MIFARE technologii*. [s. l.], 2008. 3-4 s. Vedoucí bakalářské práce Ing. Jiří Havlík.

[3] SEKERA, Jaroslav. *BEZDRÁTOVÝ PŘÍSTUPOVÝ SYSTÉM*. [s. l.], 2008. 16-17 s. Vedoucí diplomové práce Ing. Petr Fiedler, PhD

[4] *RFID - technologie pro internet věcí* [online]. 2000 [cit. 2009-03-13]. Dostupný z WWW: http://pandatron.sk/?733&rfid_-_technologie_pro_internet_veci

[5] *Čipové karty* [online]. 2003 [cit. 2009-03-20]. Dostupný z WWW: http://www.tsoft.cz/index.php?q=cz/index

[6] JELÍNEK, Josef. *Jak zabezpečit byt, dům, chatu, automobil*. [s.l.] : [s.n.], 2000. 84 s.

[7] *EZS zabezpečovací systémy* [online]. 2009 [cit. 2009-04-01]. Dostupný z WWW: http://www.zabezpeceni-domu.cz/index.php?nid=3643&lid=CZ&oid=453040

[8] *Elektronické zabezpečovací systémy (EZS)* [online]. 2008 [cit. 2009-04-01]. Dostupný z WWW: http://www.flexcom.cz/index.php/Elektronicke-zabezpecovaci-systemy-EZS.htm

[9] http://www.jablotron.cz/upload/File/pnj131-2007.pdf

[10] http://www.jablotron.cz/upload/File/pn50131-1.pdf

[11] *EZS - elektronické zabezpečovací systémy* [online]. 2005 [cit. 2009-04-05]. Dostupný z WWW: <http://www.acontrol.cz/stranka/el_zabezpecovaci-systemy>.

[12] *Ukázky zabezpečení rodinných domů* [online]. 2005 [cit. 2009-04-10]. Dostupný z WWW: http://alarmy.hyperlink.cz/vzory.htm

[13] http://www.micro.feld.cvut.cz/home/X34EZS/prednasky/04%20Ustredny%20EZS.pdf

[14] *Zařízení pro přenos dat* [online]. 2004 [cit. 2009-04-20]. Dostupný z WWW: http://www.svagency.cz/sluzby/zarizeni-pro-prenos-dat.aspx

[15] *Z čeho se skládá zabezpečovací systém EZS* [online]. 2001 [cit. 2009-05-21]. Dostupný z WWW: http://www.acesys.cz/zabezpecovaci-system-ezs.html

[16] http://www.alarmtec.cz/download/2/9/Prospekt-pro-uzivatele.pdf

[17] *Komunikace* [online]. 2008 [cit. 2009-04-25]. Dostupný z WWW: http://www.variant.cz/sekce13-komunikace.html

[18] ČSN EN50131-3

[19] *Bezpečnostní technika* [online]. 2007 [cit. 2009-05-01]. Dostupný z WWW: http://www.delmes.sk/search.php?rsvelikost=sab&rstext=all-phpRS-all&rstema=25

[20] http://homel.vsb.cz/~mor196/fsmkov.pdf

[21] *Stavové diagramy* [online]. 2006 [cit. 2009-05-10]. Dostupný z WWW: http://fpf.slu.cz/~vav10ui/obsahy/dipl/uml/Stavove/State4.htm

[22] *Stavový diagram* [online]. 2005 [cit. 2009-05-20]. Dostupný z WWW: http://web.sks.cz/users/ku/PRI/stavovy.htm

11. SEZNAM ZKRATEK

EZS	Elektronická zabezpečovací signalizace
RFID	Identifikace na rádiové frekvenci
PCO	Pult centralizované ochrany
RF	Radiová frekvence
IR	Infračervené záření
PC	Počítač
FM	Frekvenční modulace
LED	Elektroluminiscenční dioda
LCD	Displej z tekutých krystalů
GSM	Globální Systém pro Mobilní komunikaci
GPRS	General Packet Radio Service