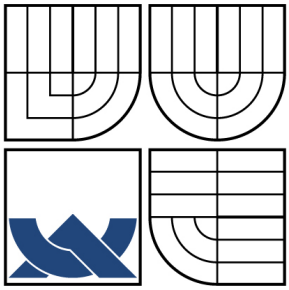
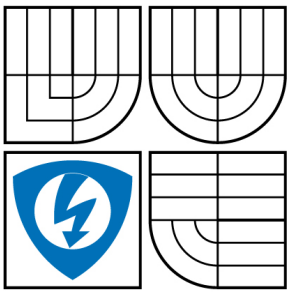


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF CONTROL AND INSTRUMENTATION

ZABEZPEČOVACÍ SYSTÉM S KOMUNIKACÍ PŘES MOBILNÍ TELEFON

SECURITY SYSTEM WITH MOBILE PHONE COMMUNICATION

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

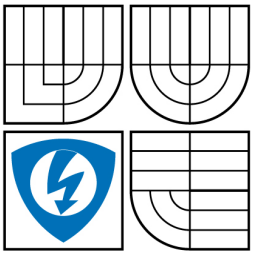
AUTOR PRÁCE — Bc. JAKUB ULBRICH

AUTHOR

VEDOUCÍ PRÁCE — Ing. TOMÁŠ MACHO, Ph.D.

SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav automatizace a měřicí techniky

Diplomová práce

magisterský navazující studijní obor
Kybernetika, automatizace a měření

Student:	Bc. Jakub Ulbrich	***ID:***	83177
Ročník:	2	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Zabezpečovací systém s komunikací přes mobilní telefon

POKYNY PRO VYPRACOVÁNÍ:

1. Seznamte se s problematikou komunikace mikroprocesorového systému a mobilního telefonu.
2. Seznamte se s mikrokontroléry řady ATMEGA 16.
3. Navrhněte a realizujte mikroprocesorový systém s mikrokontrolérem řady ATMEGA 16, který by sloužil jako základ zabezpečovacího systému a umožňoval propojení s mobilním telefonem.
4. Ověřte funkčnost mikroprocesorového systému včetně možnosti odesílání SMS zpráv přes mobilní telefon.
5. Rešte problematiku zálohovaného napájení mikroprocesorového systému a mobilního telefonu.

DOPORUČENÁ LITERATURA:

Dle vlastního literárního průzkumu a doporučení vedoucího práce.

Termín zadání:	9.2.2009	***Termín odevzdání:***	25.5.2009

Vedoucí práce: Ing. Tomáš Macho, Ph.D.

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

UPOZORNĚNÍ:

Vysoké učení technické v Brně
Fakulta elektrotechniky a komunikačních technologií
Ústav automatizace a měřící techniky

Zabezpečovací systém s komunikací přes mobilní telefon

Diplomová práce

Obor: Kybernetika, automatizace a měření
Student: Bc. Jakub Ulbrich
Vedoucí práce: Ing. Tomáš Macho, Ph.D.

Abstrakt:

Tato práce se zabývá problematikou elektronických zabezpečovacích systémů. V první části práce jsou popsány komponenty elektronických zabezpečovacích systémů, jako jsou klávesnice, detektory, poplachová zařízení apod. Dále jsou zde popsány různé možnosti zastřežení a odstřežení objektů, způsoby detekce neoprávněného vniknutí do objektu i jiných událostí a také způsoby vyvolání poplachu.

Druhá část diplomové práce je zaměřena na konstrukci jednoduchého zabezpečovacího systému, který je určen pro zabezpečení průměrně velkého bytu s jedním vchodem. Systém dokáže obsluhovat až čtyři detektory pohybu. Obsluha systému je prováděna prostřednictvím 16 tlačítkové klávesnice a pro snadnou orientaci v ovládání slouží LCD displej. Poplach je hlášen interiérovou sirénou, ovšem do systému lze připojit i jiné hlásiče poplachu, které mají vstup přizpůsobený pro příjem log. 0 nebo log. 1. Systém je vybaven komunikačním zařízením (mobilní telefon), které hlásí poplach na dálku až na 3 telefonní čísla. Uživatel může využít také dálkového ovládání prostřednictvím SMS zpráv k odstřežení systému nebo ke zjištění jeho stavu. Systém je řízen mikrokotrolérem AVR ATmega16 firmy Atmel. V této práci je uvedena stručná charakteristika všech součástí modelu elektronického zabezpečovacího systému.

Klíčová slova:

Elektronický zabezpečovací systém, EZS, ATmega16, pasivní infračervený detektor pohybu, PIR detektor, GSM pager, AT příkaz, PDU formát SMS

Brno University of Technology
Faculty of Electrical Engineering and Communication
Department of Control, Measurement and Instrumentation

Security system with mobile phone communication

Master's thesis

Specialization of study: Cybernetics, control and measurement
Student: Bc. Jakub Ulbrich
Supervisor: Ing. Tomáš Macho, Ph.D.

Abstract:

This thesis deals with the question of electronic security systems. In the forepart are described electronic security system components such as keyboards, detectors, alarm devices etc. Various methods of security or de-security of properties, trespassing and other events detection methods, and ways of alarm calling are described there too.

The next part of the master's thesis focuses on the construction of an alarm system which is designed for security of a common-size flat with one entry. The system manages to control up to four movement detectors. The operation of the system is handled by a 16-button keyboard, and easy orientation is provided thanks to a liquid crystal display. The alarm is signaled by an indoor alert siren, however, other alarm announcing devices with an input matched for the log. 0 or log. 1 reception can be connected too. The system contains communication equipment (mobile phone) which signals alarm at a distance to the three telephone numbers. User can use a distance control by text message to unlock system or to determine its status. The system is controlled by the microcontroller AVR ATmega16, the product of Atmel company. A brief description of all components of the electronic alarm system is included in this work.

Keywords:

Electronic security system, ESS, ATmega16, passive infrared movement detector, PIR detector, GSM pager, AT command, PDU format SMS

Bibliografická citace této práce

ULBRICH, J. *Zabezpečovací systém s komunikací přes mobilní telefon*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 104 s. Vedoucí diplomové práce Ing. Tomáš Macho, Ph.D.

P r o h l á š e n í

„Prohlašuji, že svou diplomovou práci na téma "Zabezpečovací systém s komunikací přes mobilní telefon" jsem vypracoval samostatně pod vedením vedoucího diplomové 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 diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové 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:……

P o d ě k o v á n í

Děkuji vedoucímu diplomové práce Ing. Tomáši Machovi, Ph.D. za cenné rady a ochotu při řešení diplomové práce.

Dále bych chtěl poděkovat kolegovi Miroslavu Václavkovi za poskytnutí souboru pro ovládání LCD displeje.

Děkuji také rodičům za vytvoření stabilního zázemí při studiu.

V Brně dne:…….. Podpis:……

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

1. ÚVOD

Zabezpečovací systémy jsou určeny k ochraně osob, majetku a informací. Jejich úkolem je zaregistrovat a oznámit pokus o neoprávněném vniknutí do objektu a zamezit nebo ztížit pachateli vstup, případně jej odradit. Objekt lze zabezpečit např. mechanicky, základem takovéhoto zabezpečení jsou bezpečnostní dveře, okenní mříže či fólie na sklo, trezory atd. Mechanické zabezpečení pouze znesnadňuje nepovolané osobě vstup do objektu. Podaří-li se pachateli mechanické zabezpečení překonat, má zcela volné pole působnosti, dále mu tedy nic nebrání k provedení jeho záměru. Kvalitnější a dnes i nejrozšířenější jsou elektronické zabezpečovací systémy (dále jen EZS), které chrání objekty na zcela jiném principu než systémy mechanické. EZS se nesnaží pachateli znesnadnit vstup do objektu, jeho úkolem je prostřednictvím poplachového systému informovat o neoprávněném vstupu, případně poskytovat aktuální informace např. o pohybu pachatele. Právě poplachový systém je jedna z nejdůležitějších součástí EZS. Ekonomicky nejvýhodnější variantou je použití poplachových sirén, které spoléhají na duchapřítomnost lidí v okolí. Ovšem díky moderní době se lidé stávají imunními vůči houkavému zvuku sirén nebo je ohrožení cizího majetku nechává chladnými. Pokud se tedy nelze spolehnout na známou osobu nacházející se v blízkosti střeženého objektu, která by v případě poplachu zasáhla, stává se použití sirén jako poplachového systému neefektivním řešením a je třeba hledat jinou variantu hlášení poplachu. Velmi účinné jsou hlásiče poplachu na dálku, které prostřednictvím komunikačního zařízení informují majitele objektu či přímo orgány bezpečnosti o neoprávněném vniknutí. Zásahová akce pak bývá rozjeta téměř okamžitě. Takovýmto komunikačním zařízením může být například mobilní telefon. Ten však nemusí být využit pouze jako hlásič poplachu, lze jím také celý zabezpečovací systém ovládat, může plnit i funkci odposlechu. Právě elektronickým zabezpečovacím systémem s komunikací přes mobilní telefon se zabývá tato práce. V práci je shrnuta problematika elektronických zabezpečovacích systému a ovládání mobilního telefonu externím zařízením. Součástí práce je také návrh elektronického zabezpečovacího systému s mobilním telefonem, který je řízen mikrokontrolérem řady ATmega.

2. ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY (EZS)

Elektronické zabezpečovací systémy patří k nejrozšířenějším a nejdostupnějším zabezpečovacím prostředkům objektů, jak soukromých, tak i firemních či státních. Jejich úkolem je chránit osoby, majetek, informace a upozornit tak, jsou-li v ohrožení. Dokáží zachytit nepovolené či nebezpečné aktivity v objektu a podat o tom zprávu tam, kam si majitel přeje.

Komponenty EZS lze s vyhodnocovacím zařízením propojit pomocí kabelů, kterými je přenášeno napájecí napětí a veškeré informace, nebo lze komunikaci mezi komponenty zprostředkovat bezdrátově. Systémy s kabelovým vedením je vhodné instalovat do rozestavěných objektů nebo do objektů v rekonstrukci, kde je možné bez problému instalovat veškerou kabeláž do zdi. Odpadají tak drastické zásahy do hotových zdí. Výhodou těchto systémů oproti bezdrátovým je vyšší spolehlivost, nižší cena komponentů a odpadá nutnost výměny baterií v zabezpečovacích prvcích. Bezdrátové systémy je vhodné instalovat do hotových objektů, není totiž nutné vysekávat do zdi díry a vkládat do nich kabelové rozvody. Montáž je tak bezprašná, čistá a velmi rychlá. Výhodou je velká variabilita systému, je možno přidávat další prvky nebo je jednoduše přemisťovat dle potřeby. Nevýhodou je napájení zabezpečovacích komponentů bateriemi, nutnost kontroly stavu baterií a jejich občasná výměna. Doporučuje se baterie preventivně jednou ročně vyměnit. Jsou ovšem také komponenty, které na potřebu výměny baterie upozorňují, zde potom odpadá občasná kontrola stavu baterií.

Při zabezpečování objektu proti vloupání se doporučuje volit kombinaci elektronického a mechanického zabezpečení. Důležitou roli hraje mechanické zabezpečení (kvalitní dveře, zámky, okenní mříže, bezpečnostní fólie na sklech apod.), které slouží pro ztížení neoprávněného vstupu do objektu. Elektronický zabezpečovací systém pak dokáže sledovat pokus o překonání těchto zábran a je schopen vyhlásit včasný poplach, který přivolá pomoc, zatímco je pachatel stále ještě mimo objekt.

EZS má 4 základní části

- Přístupový systém
- Detektory
- Ústředna
- Výstupní zařízení (hlášení poplachu)

EZS může být také vybaveno komunikačním zařízením, které může sloužit jako přístupový systém, výstupní zařízení, může být také využito k ovládání systému.

2.1 PŘÍSTUPOVÝ SYSTÉM

Přístupovým systémem se myslí prostředek pro odstřežení EZS použitím tzv. indikačního prvku, který slouží povolaným osobám pro bezpečný vstup. Indikačním prvkem může být několika místný kód, kterým lze prostřednictvím kódovací klávesnice deaktivovat EZS. Jako další indikační prvek se používají čipové karty, které EZS deaktivují po vložení do snímače karet nebo po přiložení na bezdotykovou čtečku. Pro odstřežení lze také použít dálkový ovladač mající v sobě tzv. plovoucí přenosový kód, který dokáže EZS deaktivovat na vzdálenost několika metrů. Lze také použít mobilní telefony, deaktivaci EZS je možné provést zasláním SMS zprávy na přijímač napojený na EZS nebo také tzv. prozvoněním přijímače. Moderními indikačními prvky jsou biometrické snímače, které využívají jedinečné znaky lidského těla. Dokáží uživatele identifikovat na základě otisku prstu, geometrie ruky, sítnice oka apod.

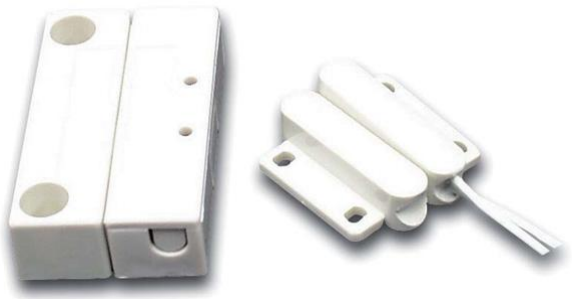
Vzhledem k tomu, že při použití identifikačního prvku přístupový systém identifikuje každého uživatele, lze např. ve velkých podnicích monitorovat docházku, kontrolovat a evidovat využívání kopírovacích strojů, zprostředkovat bezhotovostní úhradu za stravování apod.

2.2 DETEKTORY

Detektory jsou nejcitlivějším článkem celého EZS, jejich úkolem je monitorovat střežený prostor a zachytit neoprávněnou akci v tomto prostoru. Detektory dokáží rozpoznat celou řadu jevů. Lze monitorovat nejen pohyb a odhalit nepovolanou osobu v objektu, ale je také možné zabezpečit objekt například proti požáru, úniku hořlavých plynů, vody, lze také zachytit zvuk tříštícího se skla, otevření dveří, dokonce i řezání či vrtání trezoru.

2.2.1 Magnetické kontakty

Magnetické kontakty jsou nejjednodušší detektory, používají se pro kontrolu uzavření oken nebo dveří. Skládají se ze dvou částí. První část tvoří permanentní magnet, druhou část pak jazýčkové relé. Obě části jsou zataveny zpravidla do plastových výlisků. Permanentní magnet se umisťuje na okraj okna nebo dveří, relé je nutné umístit vedle magnetu na rám okna nebo dveří. Rozdělí-li se tyto dvě části na větší vzdálenost, což prakticky nastane při otevření okna či dveří, relé rozepne kontakt, čímž detektor podává znamení k vyvolání poplachu. Kvalitnější magnetické kontakty využívají polarizace magnetického pole k tomu, aby je nebylo možné zablokovat přiložením cizího magnetu. Lze je použít nejen pro monitorování nepovoleného otevření oken či dveří, poslouží také při počítání doby, během které je nutné opustit právě zabezpečený prostor, kdy se po uzavření dveří EZS hned nebo po několika sekundách aktivuje.



Obrázek 1: Magnetický kontakt [10]

2.2.2 Pasivní infračervené detektory (PIR)

PIR detektory jsou nejpoužívanějšími detektory pohybu. Jsou určené k prostorové ochraně objektu, pracují na principu detekce pohybu osob v zorném poli. Využívají skutečnosti, že každé těleso s určitou teplotou vyzařuje vlnění v infračerveném pásmu, které odpovídá teplotě těles. Snímací prvek zaznamenává změny záření, které na něj dopadá, a elektronika detektoru tyto změny vyhodnotí. Pak podle daných kritérií dá povel pro vyvolání poplachu. Detektory se umisťují tak, aby co nejlépe pokryly hlídaný prostor, nesmějí být ovšem namířeny na zrcadla, skla, okna a další lesklé a odrazné plochy, které by odrážely sluneční paprsky do detektoru. Dále by detektor neměl být umístěn v místech s proudícím vzduchem a v blízkosti zdrojů vodních či olejových par. PIR detektory by měly být standardně vybaveny rozpínacím kontaktem, který dokáže odhalit sejmutí krytu detektoru. Ve střeženém objektu nesmí dojít k narušení nebo sejmutí krytu, pachatel by tak mohl poškodit citlivou elektroniku detektoru a tím jej zneškodnit.

Obrázek 2: Pasivní infračervený detektor [12]

2.2.3 Ultrazvukové detektory

Tyto detektory pracují na principu radaru, tedy vysílají signál o určité frekvenci a přijímají jeho odraz od stěn sledovaného prostoru. Dojde-li na přijímač signál o jiné frekvenci, než byl vyslán, detektor získává informaci o pohybu v prostoru a je připraven vyslat žádost o poplach. Detektory pracují s frekvencemi nad pásmem slyšitelnosti pro člověka (větší než 20kHz). Detektory nejsou vhodné pro prostory, kde se pohybují zvířata, která dokáží vnímat vyšší frekvence než

člověk, protože jim může být signál z detektoru velmi nepříjemný. Není vhodné umisťovat tyto detektory v blízkosti zdrojů zvuku se širokým kmitočtovým spektrem (např. telefony).

Obrázek 3: Ultrazvukový detektor [16]

2.2.4 Mikrovlnné detektory

Pracují na podobném principu jako ultrazvukové detektory s tím rozdílem, že mikrovlnné detektory pracují v pásmu 1GHz až 10GHz a vysílají do prostoru mikrovlny. Opět sledují změnu frekvence vyslaného a přijatého signálu. Mikrovlny pronikají sklem, tenkými stěnami apod., vzniká tedy riziko, že při nevhodné montáži dojde k detekci pohybu mimo střežený prostor. Mikrovlnné detektory se často používají v komplikovaných prostorech s vysokými rušivými vlivy v kombinaci s pasivními infračervenými detektory (PIR). Požadavek na poplach je vyhodnocen po porovnání informací z obou detektorů.

Obrázek 4: Mikrovlnný detektor [17]

2.2.5 Prostorové zvukové detektory

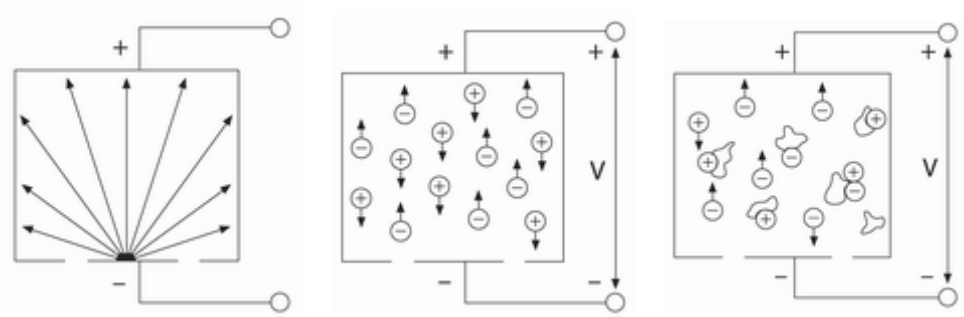
Neboli detektory rozbití skla. Vyhodnocují signály z vestavěného mikrofonu a posuzují vysokofrekvenční vlny vzniklé rozbitím skla, nízkofrekvenční vlny

způsobené nárazem na sklo apod. Na trhu je mnoho variant těchto detektorů. Před pořízením je např. nutné vědět, zda budou na střežených sklech instalovány bezpečnostní nebo sluneční fólie.

Obrázek 5: Prostorový zvukový detektor (detektor rozbití skla) [10]

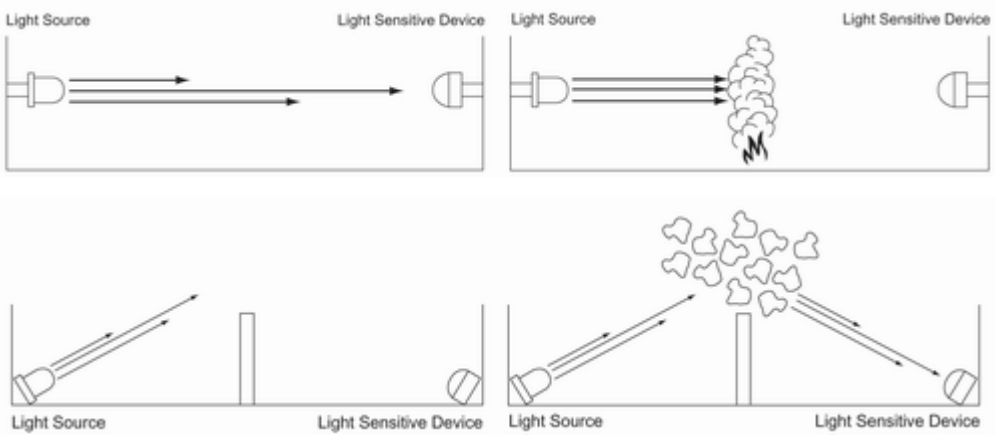
2.2.6 Detektory kouře

Fungují na principu ionizace nebo přerušení paprsku světla. Ionizační senzory využívají ionizační komoru, kde dochází k ionizaci plynu, resp. detekovaného kouře. Tyto detektory jsou nejpoužívanější z důvodů nízké ceny a dobré detekci již malých částeček kouře. Uvnitř ionizačního detektoru se nachází malé množství prvku americium-241, který je dobrým zdrojem potřebných alfa částic. Konstrukce detektoru se skládá ze dvou elektrod – kladné a záporné. Alfa částice generované prvkem americium uvolňují elektrony do atomů kyslíku a dusíku ve vzduchu, které se nacházejí v komoře uvnitř detektoru. Volný elektron reprezentuje záporný náboj, zatímco atom s chybějícím elektronem naopak kladný náboj. Elektron je přitahován ke kladné elektrodě a kladně nabitý atom k záporné elektrodě. Senzor se tak v klidovém stavu chová jako slabý zdroj proudu. Dostane-li se do komory kouř, jeho částice pak na sebe naváží elektrony i kladné ionty a neutralizují je. Tím se sníží hodnota proudu, čímž detektor dostává informaci o přítomnosti kouře. Hodnota sníženého proudu je přímo úměrná koncentraci kouře. Prvek americium je radioaktivní, ovšem množství radiace je velmi malé, alfa částice nemohou projít např. skrz papír nebo několika centimetrovou vrstvou vzduchu. Nedoporučuje se však přímá manipulace s detektorem, opravy či revize je vhodné přenechat odborníkům.



Obrázek 6: Ionizační princip detektoru (vlevo - alfa částice generované prvkem americium; uprostřed - elektrony vytvářejí elektrický proud; vpravo - přítomnost kouře na sebe váže elektrony i kladné ionty) [14]

Fotoelektrické senzory mohou pracovat na dvou různých principech. Prvním principem je blokování průchodu světla. Zdroj světla míří přímo na světlo citlivý přijímač. Dostane-li se kouř mezi zdroj a přijímač, kouř pohltí část intenzity světla, důsledkem čehož dopadne na přijímač světlo o menší intenzitě. Detektor tak dostává informaci o přítomnosti kouře. Druhým principem je odklánění paprsku světla. Zdroj světla nemíří přímo na světlo citlivý snímač, ovšem dostane-li se do komory detektoru určitá koncentrace kouře, pak dochází k lomu paprsku světla. Ten pak dopadá na přijímač, čímž je detektor informován o přítomnost kouře a připraven podat žádost o spuštění alarmu, popřípadě dát povel k uvedení hasicího zařízení do provozu.



Obrázek 7: Fotoelektrický princip detektoru kouře (nahoře - odklonění paprsku světla; dole - blokování průchodu paprsku světla) [14]

Obrázek 8: Detektor kouře [10]

2.3 ÚSTŘEDNA

Ústředna je mozkem celého zabezpečovacího systému, jejím úkolem je vyhodnotit signál z detektorů a rozhodnout, zda se jedná o neoprávněnou akci. Na základě tohoto rozhodnutí dává pokyn k poplachu, tedy aktivuje výstupní zařízení. Většinou se jedná o mikroprocesorový systém, který je naprogramován tak, aby byl schopen ovládat všechny komponenty EZS. Možnosti vyhodnocování signálů z komponentů jsou vcelku neomezené, ústředny např. dokáží hlídat pouze část objektu, což lze využít v rodinných domech, když obyvatelé spí. Ústředna by měla být umístěna na takovém místě, aby nebylo možné ji úmyslně zničit, čímž by pachatel dosáhl odstavení systému. Doporučuje se umístění do uzamykatelných skříní, na těžko přístupná místa apod. Je také možné prostor pro ústřednu zabezpečit detektory. Naopak nedoporučuje se umístění do trvale nepřístupných prostor z hlediska údržby zařízení. Některá poplachová zařízení mohou být vybavena logikou, která kontroluje stav ústředny. Pokud logika nedostává z ústředny pravidelné signály, považuje ústřednu za odstavenou či zničenou a spouští poplach.

2.4 VÝSTUPNÍ ZAŘÍZENÍ

Výstupní zařízení podávají informaci o poplachu. Tuto informaci lze podávat akusticky, opticky či dálkově prostřednictvím komunikačního zařízení. Výstupním zařízením mohou být také aktivní prvky, které zamezí neoprávněné akci, např. stropní hasiče požáru nebo systém pro odvětrávání unikajícího plynu.

2.4.1 Vnitřní sirény

Vnitřní sirény se umisťují dovnitř střeženého objektu, jejich úkolem je za pomoci pronikavého zvuku, který vydávají, znepříjemnit pachateli pobyt v objektu a přispět k jeho útěku. Vnitřní sirény jsou napájeny přímo z ústředny, některé sirény mohou být ovšem vybaveny vestavěnou baterií pro případ, že by se pachatel pokusil ústřednu zlikvidovat.

Obrázek 9: Vnitřní siréna [10]

2.4.2 Venkovní sirény

Venkovní sirény upozorňují okolí na skutečnost, že ve střeženém objektu došlo k nedovoleným akcím. Spoléhají tedy na rychlé jednání osob nacházejících se v blízkosti napadeného objektu. Sirény jsou většinou opatřeny světlem, pomocí něhož lze snadno identifikovat napadený objekt. Není totiž vždy snadné určit, který z objektů je napaden, je-li v blízkém okolí několik dalších zabezpečených objektů. Většina sirén je vybavena záložní baterií, která se v klidovém stavu dobíjí z ústředny, při poplachu sirénu napájí. Sirény se umisťují vně střeženého objektu, je vhodné je instalovat co nejvýše na zeď ovšem tak, aby nebylo problematické provádět občasnou údržbu zařízení.

Obrázek 10: Venkovní siréna [10]

2.4.1 Hlášení poplachu na dálku

Vzdálená komunikace byla do zabezpečovacích systémů implementována z důvodu málo efektivního hlášení poplachu sirénami. Pokud totiž okolí napadeného objektu na zvuk sirény nereaguje a pachatel je vůči pronikavému zvuku dostatečně imunní, nic mu nebrání pokračovat v jeho záměru. Vzdálená komunikace řeší hlášení poplachu na dálku příslušným útvarům či osobám (často majitel objektu), které se postarají o zabezpečení napadeného objektu. Nejznámějším takovýmto útvarem je pult centralizované ochrany PCO. PCO je dispečerské pracoviště, které registruje informaci o poplachu, případně zpracovává další informace, které je elektronický zabezpečovací systém schopen poskytnout (stav čidel, informace o pohybu pachatele atd.). Dle druhu vyhlášeného poplachu vysílá operátor PCO zásahovou jednotku, aby objekt zabezpečila, popřípadě podává informaci Policii. Majiteli pak odpadá starost se zajišťováním napadeného objektu. Existuje několik možností, jak může zabezpečovací systém vzdálenou komunikaci navázat. Rozlišují je jejich výhody a nevýhody. Některé zabezpečovací systémy dokonce nabízejí kromě dálkového hlášení poplachu i další možnosti využití vzdálené komunikace.

2.4.1.1 Komunikace přes pevnou telefonní linku

Spojení s oprávněnou osobou nebo útvarem a předávání informace se děje přes pevnou telefonní linku. Komunikace tohoto typu se využívá hlavně pro hlášení poplachu ve spojení s PCO. Lze také zajistit, aby zabezpečovací systém komunikoval s mobilním telefonem majitele objektu, ale vzhledem k tomu, že provozovatel sítě pevné telefonní linky účtuje při spojení s mobilními sítěmi vysoké poplatky za hovorné, je toto řešení neefektivní a nepoužívá se. K provozu nepotřebuje zabezpečovací systém zvláštní pevnou linku, lze využít již zavedenou telefonní linku v objektu. Dojde-li k poplachu, komunikátor odpojí ostatní telefonní zařízení na lince, vytočí číslo PCO a po vyřízení potřebných informací komunikaci ukončí. Poté připojí zpět ostatní telefonní zařízení. Tato varianta připojení není dnes nejlepším řešením, neboť majiteli značně narůstají poplatky za telefon. Komunikátor totiž zpravidla jednou denně navazuje kontrolní spojení s PCO, které je započítáno jako

běžný hovor, dle toho také zpoplatněno. Připojení pomocí pevné telefonní linky je navíc méně spolehlivé a také velice snadno napadnutelné (např. přerušení přívodního kabelu telefonní linky).

2.4.1.2 Komunikace přes bezdrátovou síť

Tento typ komunikace je využíván výhradně pro hlášení poplachu na PCO. Vysílá-li PCO signál bezdrátové sítě a je-li střežený objekt v dosahu tohoto signálu, pak lze tuto síť k hlášení poplachu využít. Je nutné pořídit vysílač, který v případě poplachu vyšle informace v podobě dat po bezdrátové síti do PCO. Toto spojení nelze jednoduše sabotovat. Výhodou je také nezávislost na cizích přenosových sítích (pevné telefonní linky, mobilní sítě apod.). Pomocí bezdrátové sítě je možné trvale kontrolovat spojení mezi EZS a PCO. Provozní náklady bývají většinou nízké.

2.4.1.3 Komunikace přes mobilní síť GSM

Komunikace s oprávněnou osobou nebo příslušnými útvary probíhá pomocí některé z mobilních sítí (přes tzv. GSM bránu). Je-li území, na kterém se střežený objekt nachází, pokryto signálem některého z mobilních operátorů, pak lze tento typ komunikace využít. Spojení lze navázat jak s majitelem střeženého objektu, tak i s PCO. Existuje několik typů zařízení, které komunikaci přes mobilní síť zprostředkovávají.

Mobilní telefon

Mobilní telefon je přístroj, který využívá možnost komunikace přes mobilní sítě GSM. Přístroj je určen pro veřejnost k vzájemné komunikaci. Zprostředkovává jak hlasovou (telefonní hovory), tak i datovou (krátké textové zprávy aj.) komunikaci. Mobilní telefon může také plnit funkci komunikátoru zabezpečovacího systému. Přes systémový konektor jej lze napojit na ústřednu systému, která pak využívá jeho komunikačních dovedností např. k hlášení poplachu. Mobilní telefon ovšem neslouží pouze jako vysílač, dokáže data i přijímat. Tím se zabezpečovací

systém rozšiřuje o možnost dálkového ovládání např. pomocí krátkých textových zpráv odeslaných na mobilní telefon systému, které dokáže ústředna zabezpečovacího systému dekódovat a aplikovat. Pro tyto účely postačí starší mobilní telefon se základními funkcemi. Jeho cena se pohybuje velmi nízko a stále klesá, což je velkou výhodou.

Obrázek 11: Mobilní telefon Siemens C35 jako komunikátor EZS [18]

GSM modul

GSM moduly obsluhují stejné funkce jako starší mobilní telefony, některé ovšem nedokáží navázat telefonní hovor. Nejsou určeny pro veřejnost, uplatňují se v automatizační technice pro dálkové přenášení dat (vysílání a příjem). Tomu je také přizpůsobena konstrukce, kterou tvoří pouze plošný spoj se součástkami. GSM moduly nejsou zapouzdřeny, předpokládá se totiž jejich umístění přímo k řídícímu centru, čímž vznikne kompaktní komunikační celek. Ústředna komunikuje s modulem po sériové lince podobně jako s mobilním telefonem připojeným přes systémový konektor. Výhodou jsou velmi malé rozměry modulu, naopak nevýhodou je vysoká cena, která několikanásobně převyšuje cenu staršího mobilního telefonu.

Obrázek 12: GSM modul [19]

GPRS modem

GPRS modemy nevyužívají ke komunikaci telefonní hovory nebo krátké textové zprávy, informace jsou posílány jako data přes tzv. datovou mobilní službu GPRS. Provozovatel GSM sítě pak nepožaduje poplatky za hovorné, ale za přenesená data, což je výrazně levnější. GPRS modemy se používají ke komunikaci s PCO, který je vybaven příslušným přijímačem dat.

Obrázek 13: GPRS modem [20]

3. MOŽNOSTI EZS SE VZDÁLENOU KOMUNIKACÍ

Rozšířením EZS o mobilní telefon lze získat nadstavbu, která systému umožní komunikovat s majitelem střeženého objektu na dálku. Mobilní telefon umožňuje zprostředkovat jak ovládání systému, tak i hlášení poplachu. Lze jím také před příchodem do objektu zabezpečení deaktivovat nebo naopak po odchodu aktivovat. Možností využití mobilního telefonu je velmi mnoho. Velkou výhodou zabezpečovacích systémů s mobilní komunikací je velice široký dosah. Díky rozsáhlému pokrytí našeho území mobilními operátory se informace o objektu dostanou k majiteli téměř kamkoli na světě. Podstatnou výhodou je také bezdrátová komunikace s majitelem, spojení tedy nelze sabotovat přestřihnutím kabelu. Naopak zásadní nevýhodou použití mobilní komunikace je zpoplatnění všech úkonů, které mobilní operátor mezi majitelem a zabezpečovacím systémem zprostředkovává. Vyžaduje-li tedy zabezpečovací systém časté nastavování a ovládání, nebo posílá-li denně několik kontrolních oznámení, poplatky za hovorné rychle narůstají. Ovšem zabezpečovací systémy s mobilní komunikací bývají většinou konstruovány tak, aby jejich provoz nebyl značně nákladný. Při výrobě se většinou volí kompromis mezi provozními náklady a komfortem ovládání.

3.1 MOBILNÍ TELEFON JAKO PŘÍSTUPOVÝ SYSTÉM

K odstřežení prostoru může sloužit také mobilní telefon, který je napojen na ústřednu zabezpečovacího systému. Díky němu je majitel objektu schopen prostřednictvím osobního mobilního telefonu provést deaktivaci EZS odkudkoli a kdykoli, tedy i těsně před příchodem do objektu. Nabízejí se dva způsoby, jak lze pomocí mobilního telefonu zabezpečovací systém deaktivovat. První možností je deaktivace zasláním SMS s žádostí o odstřežení objektu. Výhodou je rychlost a komfort vyřízení odstřežení (v rámci možností odstřežení mobilním telefonem). Mnoho osob dnes vlastní smartphone, ve kterém lze předdefinovat různé SMS zprávy i jejich příjemce. Takové odeslání SMS zprávy včetně uzamčení a odložení

telefonu je pak otázkou několika vteřin. Nevýhodou je zpoplatnění každého odstřežení (cena SMS). Druhá možnost je oproti té první finančně přívětivější, lze ji totiž provozovat zdarma. Jedná se o odstřežení objektu prozvoněním, kdy majitel zavolá na mobilní telefon zabezpečovacího systému a po zaznění vyzváněcího tónu zavěsí. Ústředna registruje aktivitu na mobilním telefonu a dává pokyn k deaktivaci zabezpečení. Nevýhodou je ovšem delší čas, který musí uživatel k vyřízení žádosti investovat. Je nutné vyčkat na spojení hovoru, po krátkém zazvonění hovor ukončit nebo počkat na ukončení hovoru ústřednou, poté je teprve možné telefon uzamknout a odložit. Aby nebylo možné odstřežit objekt kýmkoli, kdo bude znát telefonní číslo mobilního telefonu zabezpečovacího systému, musí systém reagovat pouze na příkazy zaslané z předem stanovených telefonních čísel patřících oprávněným osobám. Samotný proces deaktivace zabezpečovacího systému pomocí mobilního telefonu je oproti jiným přístupovým systémům zbytečně zdlouhavý, zato ale tento způsob odstřežení připravuje objekt s předstihem pro bezproblémový vstup majitele. Zabezpečovací systémy s tímto typem přístupového systému by měly být vybaveny i dalším přístupovým systémem pracujícím na jiném principu, aby majitel objektu nebyl odkázán pouze na zdlouhavý mobilní způsob odstřežení objektu.

3.2 MOBILNÍ TELEFON JAKO POPLACHOVÉ ZAŘÍZENÍ

K hlášení poplachu může sloužit mobilní telefon, který je napojen na ústřednu zabezpečovacího systému. Takovémuto mobilnímu systému se říká GSM pager. Díky němu se majitel včas dozví, je-li jeho majetek ohrožen, a může tak včas začít jednat. Hlášení o poplachu může být podáváno SMS zprávou, kterou systém zašle majiteli na jeho osobní mobilní telefon. Systém může také při poplachu majitele prozvonit, tehdy je zpráva o poplachu podávána zdarma. Ovšem v obou těchto případech vzniká riziko, že majitel poplachovou informaci nezaregistruje, protože mu není podávána intenzivně. Účinnější formou hlášení poplachu mobilním telefonem je hlášení prostřednictvím telefonního hovoru, kdy po registraci neoprávněného vniknutí do objektu zabezpečovací systém majiteli zavolá. I zde je možnost, že majitel hovor nezaregistruje. Nejúčinnější formou je hlášení poplachu

více než jedné osobě s využitím zpětné vazby – potvrzení. Pokud osoba během stanoveného času nepotvrdí, že poplach zaregistrovala, systém hlásí poplach jiné osobě. V případě rozesílání poplachových SMS může být jako zpětná vazba využita potvrzovací SMS v předem stanoveném tvaru, kterou osoba zasílá zpět po přečtení poplachové SMS. V případě, že systém hlásí poplach prostřednictvím vytočení hovoru, může být jako zpětná vazba využita indikace přijetí či zamítnutí hovoru osobou, které je poplach hlášen (ovšem mobilní telefony tuto indikaci nenabízejí, strojově nelze zjistit, zda volaný hovor přijal či zamítnul). Je tedy důležité, aby v systému bylo uloženo nejen telefonní číslo majitele, ale také telefonní čísla dalších osob, na která bude hlášen poplach v případě, že majitel systému nepotvrdí, že zprávu o poplachu zaregistroval. Tyto osoby se postarají o zajištění napadeného objektu.

3.3 MOBILNÍ TELEFON JAKO ODPOSLECH

Každý mobilní telefon je opatřen vestavěným mikrofonem. Je to jedna z hlavních částí mobilního telefonu, pomocí které je možné snímat zvuk v okolí. Přenos nasnímané informace pak zajišťuje mobilní síť. Některé zabezpečovací systémy využívají mikrofon mobilního telefonu k odposlechu prostoru střeženého objektu. Pokud je to možné, je mobilní telefon v místnosti umístěn tak, aby byl schopen pojmout větší část zvukových informací v místnosti. K některým mobilním telefonům lze připojit také externí mikrofon, jehož umístění v místnosti je jednodušší. V případě poplachu si majitel může vyžádat hovor na mobilní telefon zabezpečovacího systému. Po uskutečnění hovoru majitel slyší zvukové projevy ve střeženém objektu, které snímá mikrofon telefonu zabezpečovacího systému. Může se tak dozvědět např. jména lupičů, ti také mohou prozradit, kam se chystají lup uschovat, případně jak hodlají s lupem naložit. Charakter hluku může také napovědět, co se v místnosti právě děje. Tyto informace pak mohou být stěžejní při odhalování totožnosti pachatelů, nebo mohou pomoci při hledání odcizeného majetku.

3.4 FUNKCE PRO KREDITNÍ TARIFY*

Aby byly zabezpečovací systémy schopny kvalitně pracovat i s kreditními tarify, měly by kromě obsluhy funkcí pro využití mobilních služeb zajišťovat také údržbu kreditního tarifu. Údržba kreditního tarifu spočívá ve sledování výše a platnosti kreditu a v zasílání informačních zpráv v případech, kdy je nutné kredit doplnit. Implementace těchto funkcí zvyšuje úroveň uživatelského komfortu elektronického zabezpečovacího systému.

3.4.1 Upozornění na nízký kredit

Platby za využívání mobilních služeb jsou v případě kreditních tarifů čerpány z kreditu, který není bezedný. Jakmile dojde k vyčerpání kreditu, je možnost využívání mobilních služeb pozastavena do doby, než majitel kredit opět navýší. Je-li kreditní tarif využíván v zabezpečovací technice, nemělo by dojít k situaci, kdy je možnost využívání mobilních služeb zastavena. Proto je nutné provádět neustálé kontroly výše kreditu a včas jej doplňovat. Je-li zabezpečovací systém vybaven funkcemi zajišťující údržbu kreditního tarifu, majitel přenechává tyto kontroly ústředně zabezpečovacího systému. Ta si v pravidelných intervalech nebo po každé zpoplatněné akci vyžádá od operátora zprávu o stavu kreditu, ze které dokáže výši kreditu vyčíst. V případě, že je kredit nižší než předem stanovené minimum, zasílá ústředna majiteli upozornění ve formě SMS, ve které majitele vyzývá, aby zajistil navýšení kreditu.

3.4.2 Upozornění na vypršení platnosti kreditu

Mobilní operátoři požadují po uživatelích kreditních tarifů, aby v půlročním nebo ročním intervalu (záleží na mobilním operátorovi) alespoň jednou navýšili kredit. Neučiní-li tak, aktuální kredit propadne ve prospěch operátora. Navýší-li uživatel kredit včas, doba platnosti zbývajícího kreditu je prodloužena na dobu platnosti nového kreditu. Je-li zabezpečovací systém vybaven funkcemi zajišťujícími

---

* Kreditní tarify viz kap. 4.2

údržbu kreditního tarifu, pak starost ohledně hlídání data vypršení kreditu přebírá ústředna EZS. Ta sleduje čas od posledního navýšení kreditu a podává majiteli upozornění, jakmile se sledovaný čas přiblíží k maximální době platnosti kreditu. Na základě upozornění pak majitel zajistí navýšení kreditu.

4. VOLBA VHODNÝCH KOMUNIKAČNÍCH PROSTŘEDKŮ

Základním prostředkem mobilní komunikace je přístroj, který zpracovává požadavky uživatele, registruje, odesílá, přijímá a interpretuje informace. Tuto funkci může plnit mobilní telefon. Velkou roli hraje také mobilní operátor, který komunikaci zprostředkovává. Mobilní operátoři nabízejí velké množství tarifů (předplacených služeb), každý z nich má své výhody i nevýhody.

4.1 VÝBĚR VHODNÉHO MOBILNÍHO TELEFONU

Mobilní telefon zabezpečovacího systému často obsluhuje pouze základní funkce, kterými jsou telefonní spojení a odesílání nebo příjem krátkých textových zpráv. Tyto funkce dokázaly obsluhovat již jedny z prvních mobilních telefonů, jejichž výhoda dnes tkví v nízké ceně a jejich dostupnost v bazarech je prozatím takřka neomezená. Požadavek je kladen pouze na komunikační rozhraní. V mobilním telefonu musí být implementován hardwarový modem, který přes systémový konektor zajišťuje komunikaci po sériové lince (RS232) a umožňuje ovládat mobilní telefon tzv. AT příkazy. Této možnosti komunikace a ovládání využívá ústředna zabezpečovacího systému. Stav zevnějšku telefonu není důležitý, ústředna zabezpečovacího systému, která s telefonem komunikuje pouze přes systémový konektor, nevyužívá displej ani klávesnici telefonu. Nevyžaduje také, aby byl telefon umístěn v plastovém krytu. Vhodnými mobilními telefony schopnými spolupracovat s ústřednou zabezpečovacího systému mohou být např. starší telefony značky Siemens (C35, M35, S35, C45, M50, MT50 atd.), Ericsson (A1018, T10, T18 atd.) aj. Mobilní telefony značek Nokia, Philips, Alcatel, Sagem, Motorola aj. nejsou vybaveny potřebnými funkcemi nebo nemají vyvedenu komunikační linku do systémového konektoru, a tudíž nejsou schopny s ústřednou spolupracovat.

4.2 VÝBĚR VHODNÉHO OPERÁTORA A TARIFU

Aby byl mobilní telefon zabezpečovacího systému provozuschopný, musí být vybaven SIM kartou s tarifem některého z mobilních operátorů. Nejdůležitějším kritériem při výběru operátora je jeho nabídka pokrytí území, na kterém se bude mobilní telefon se zabezpečovacím systémem nacházet. Pokud by se telefon nacházel mimo dosah signálu mobilního operátora, nebylo by možné majitele dálkově upozornit na neoprávněné aktivity v zabezpečeném objektu. Mobilní operátoři nabízejí předplacené tarify, u kterých jsou mobilní služby předem zaplaceny prostřednictvím měsíčního paušálu. Nezáleží pak, zda jsou mobilní služby využity či nikoli. Tyto tarify jsou vhodné pro časté využívání služeb mobilní sítě. Pokud majitel předpokládá, že bude se systémem spolupracovat velmi často (denní uskutečnění telefonního hovoru, výměna několika SMS zpráv denně apod.), pak je vhodné uvažovat o předplaceném tarifu. Při volbě vhodného předplaceného tarifu se zohledňuje charakter a četnost využití zabezpečovacího systému, cena měsíčního paušálu a výše poplatků za služby mobilní sítě. Zabezpečovací systémy, které pracují s mobilním telefonem pouze v případě neoprávněného vniknutí do objektu, využívají služeb mobilní sítě velmi zřídka. Je pak zbytečné platit měsíční paušál, protože je možné, že mobilní telefon zabezpečovacího systému neuskuteční v daném měsíci žádný hovor a nepošle žádnou SMS. V tomto případě se předplacené tarify nevyplácejí a je vhodnější využít kreditní tarify. U těchto tarifů jsou také služby placeny předem, ovšem předplacená částka (tzv. kredit) je čerpána při využívání služeb sítě. Pokud tedy telefon v průběhu měsíce nevyužije mobilních služeb, není třeba za ně platit, částka je odečtena z kreditu pouze za využití některé ze služeb sítě. Jakmile je kredit vyčerpán, služby mobilní sítě nelze využívat a je potřeba znovu služby předplatit. Mobilní operátoři požadují, aby uživatelé kreditních tarifů alespoň jednou za půl roku nebo jednou za rok (záleží na mobilním operátorovi) kredit navýšili. Minimální částka, kterou lze kredit navýšit, je u všech operátorů stanovena na 200,- Kč*. Za předpokladu, že střežený objekt nebude v častém ohrožení, tzn., že nebude např. v průběhu roku napaden a mobilní služby nebudou po celou dobu

* Platí ke dni 11. 5. 2009

využity, roční náklady pak tedy v případě kreditních tarifů s podmínkou ročního doplňování vychází na 200,- Kč. U kreditních tarifů s půlročním doplňováním kreditu jsou náklady dvakrát vyšší.

Není ovšem pravidlem, že předplacené tarify musejí být finančně náročné a vyplácejí se jen při vysoké četnosti využívání mobilních služeb. Výjimku mezi předplacenými tarify tvoří tarif s názvem Odepiš* od společnosti Vodafone, jehož měsíční paušální poplatek vychází na 11,90 Kč*. V ceně je zahrnuto 40 minut volání* na telefonní čísla pod sítí operátora Vodafone, čehož může majitel využít, pokud je jeho osobní telefonní číslo pod tímto operátorem. Za předpokladu, že střežený objekt nebude v častém ohrožení, tzn., že roční statistiky napadení se budou blížit nule a mobilní služby tak zůstanou nevyužité, je používání předplaceného tarifu Odepiš nejefektivnější. Jeho roční provoz pak vychází na 142,80 Kč, což je o 57,20 Kč méně než v případě kreditních tarifů s podmínkou ročního doplňování kreditu za stejného předpokladu četnosti využití mobilních služeb.

* Platí ke dni 11. 5. 2009

5. MIKROKONTROLÉRY ATMEL AVR

V druhé polovině devadesátých let uvedla na trh firma Atmel rodinu mikrokontrolérů AVR, jejichž koncepci koupila od skupiny norských vývojářů. Výsledkem práce této skupiny bylo optimalizované jádro nové řady mikrokontrolérů s redukovanou instrukční sadou. Struktura mikrokontrolérů byla navržena tak, aby vyhovovala překladačům vyšších programovacích jazyků, zejména překladačům široce používaného jazyka C.

Parametry mikrokontrolérů rodiny AVR:

- Šíře instrukčního slova: 16 bitů
- Propojení ALU s polem 32 pracovních registrů
- Pipelining (zatímco je jedna instrukce prováděna, druhá je přesouvána z programové paměti)
- Vykonání instrukce registr-registr: 1 hodinový takt (na 1MHz hodinového kmitočtu připadá výkon 1Mips)
- Harwardská architektura (rozdělená paměť - část paměti vyhrazena pro program, část paměti vyhrazena pro data)
- Paměť EEPROM pro data
- Možnost připojení externí paměti dat až do velikosti 64kB (rozhraní pro externí paměť používá 16 bitovou adresovou sběrnici)
- Integrovaný obvod Watchdog

5.1 ZPŮSOB PROGRAMOVÁNÍ MIKROKONTROLÉRŮ AVR

Mikrokontroléry AVR lze programovat přímo v aplikaci („in circuit programming“) s využitím sériového rozhraní tvořeného čtyřmi vodiči. Dříve byly mikrokontroléry uzpůsobené pro paralelní programování, které využívalo vývody I/O portů pro přístup k paměti programu. Po připojení programovacího napětí na pin obvodu bylo provedeno přiřazení těchto vývodů k adresovým a datovým vývodům vnitřní programové paměti, což umožnilo do paměti paralelně zaznamenat data

(příslušný program). Po dokončení zápisu dat je mikrokontrolér uveden zpět do počátečního stavu (reset). Poté pracuje dle instrukcí nově zapsaného programu. Při tomto způsobu programování je nutné, aby byl mikrokontrolér odpojen od všech obvodů (např. periferií). Je tedy nezbytné mikrokontrolér vyjmout z patice, případně vyletovat z plošného spoje a vložit jej do programátoru. Tato nevýhoda odpadá při „in circuit programming“, kdy mikrokontrolér zůstává v aplikaci a pomocí čtyř signálů (u většiny AVR mikrokontrolérů to jsou signály MOSI, MISO, SCK a RESET) připojených k programátoru lze jednoduše programovat.

5.2 ŘADY MIKROKONTROLÉRŮ AVR

Základní řada

Obsahuje typy AT90S1200, AT90S2313, AT90S2323, AT90S2343, AT90S4433, AT90S4434, AT90S8515, AT90S8534 a AT90S8535. Tyto typy (výjimkou AT90S1200) mají 118 instrukcí. Typ AT90S1200 má 89 instrukcí a oproti dalším typům nemá paměť SRAM. Dnes už se základní řada mikrokontrolérů AVR nevyrábí.

Řada ATtiny

Obsahuje typy ATtiny11, ATtiny12, ATtiny13, ATtiny15, ATtiny28, ATtiny26 a ATtiny2313. S výjimkou typu ATtiny26 (118 instrukcí) a ATtiny2313 (120 instrukcí) mají tyto typy 90 instrukcí. Disponují flash pamětí do 4kB. Jsou nejlevnějšími typy mikrokontrolérů AVR. Např. ATtiny2313 nabízí zajímavý kompromis mezi rychlostí, nabídkou periférií a cenou, dokáže pracovat na frekvenci 20MHz.

Řada ATmega

Obsahuje starší řadu ATmega103, ATmega161, ATmega163 a ATmega323 a novější řadu ATmega8, ATmega16, ATmega64 a ATmega128. S výjimkou typu ATmega103 mají tyto mikrokontroléry 130 instrukcí. Jsou vybaveny flash pamětí od 8kB do 128kB. Oproti základní řadě obsahuje navíc instrukce pro násobení. Novější

řada je navíc vybavena rozhraním JTAG pro ladění softwaru přímo v aplikaci. Jsou také schopny využívat bootloader k programování flash a EEPROM paměti.

Architektura těchto řad je stejná nebo velmi podobná, hlavní rozdíly jsou ve velikosti pouzder a tedy v počtu vstupů/výstupů. ATmega disponuje větší pamětí flash a RAM, nabízí více periférií, ale také je dražší.

6. KOMUNIKACE MOBILNÍHO TELEFONU S ÚSTŘEDNOU EZS

Obsluhu mobilního telefonu zajišťuje ústředna EZS. Mobilní telefon je připojený systémovým kabelem přímo k řidící jednotce EZS. Řidící jednotka generuje obslužné signály a registruje aktivity na mobilním telefonu.

Díky hardwarovému modemu lze mobilní telefony ovládat pomocí tzv. AT příkazů. AT příkazy zastupují běžného uživatele, který k ovládání telefonu používá klávesnici a zpětná vazba je mu podávána prostřednictvím displeje. Mikrokontrolér nevyužívá ani klávesnici, ani displej telefonu, využívá jeho systémový konektor a sériovou linku k odesílání AT příkazů. Ty tvoří jakýsi soubor příkazů, které slouží ke spuštění, ovládání a nastavení jednotlivých funkcí mobilního telefonu. AT příkazy jsou tvořeny ASCII znaky, které jsou vysílány mikrokontrolérem po lince TxD do mobilního telefonu. Telefon po každém přijetí AT příkazu odpovídá zasláním příslušných ASCII znaků po lince RxD zpět do mikrokontroléru.

Mobilní telefon Siemens C35 je přizpůsoben pro tyto parametry přenosu: přenosová rychlost 19200Bd, 8 datových bitů, bez parity, 1 stop bit.

AT příkaz může mít tyto podoby:

- Testovací, kterým lze zjistit, zda telefon daný příkaz podporuje.

  AT+<příkaz>=? <CR>

- Čtecí, kterým lze vyčíst nastavení telefonu.

  AT+<příkaz>? <CR>

- Zapisovací, kterým lze telefon nastavit nebo do něj zapsat data.

  AT+<příkaz>=<parametr> <CR>

Při komunikaci mobilního telefonu s mikrokontrolérem, je část *<CR>* nahrazena znakem $0D_{hex}$.

Mobilní telefon po každém přijatém AT příkazu zasílá zpět odpověď, která může mít tyto tvary:

- Potvrzovací, kterou oznámí, že danému příkazu rozuměl

  <CR> <LF> OK <CR> <LF>

- Chybová, kterou oznámí, že danému příkazu nerozuměl

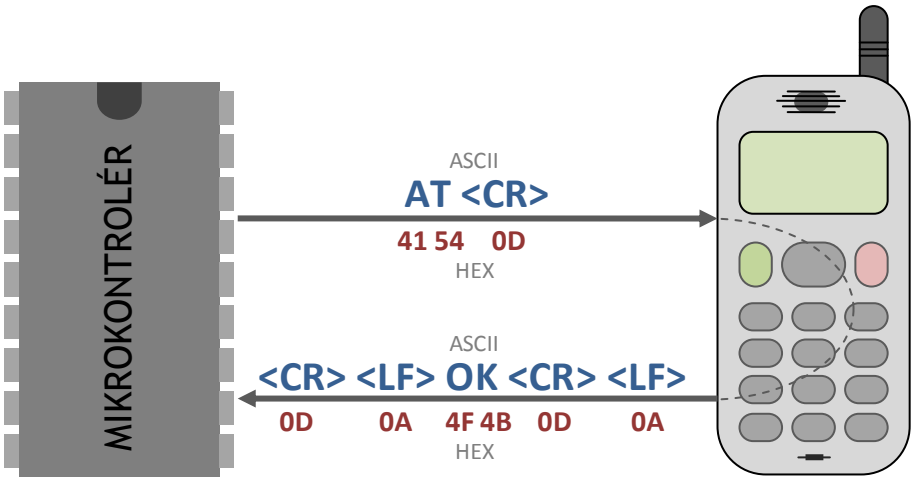
  <CR> <LF> ERROR <CR> <LF>

- Přesná odpověď, kterou zpětně zasílá po přijetí takových AT příkazů, které žádají konkrétní odpověď (např. výčet telefonních čísel z paměti telefonu, výpis SMS apod.). Za touto odpovědí bývá přiřazena i potvrzovací odpověď *OK*.

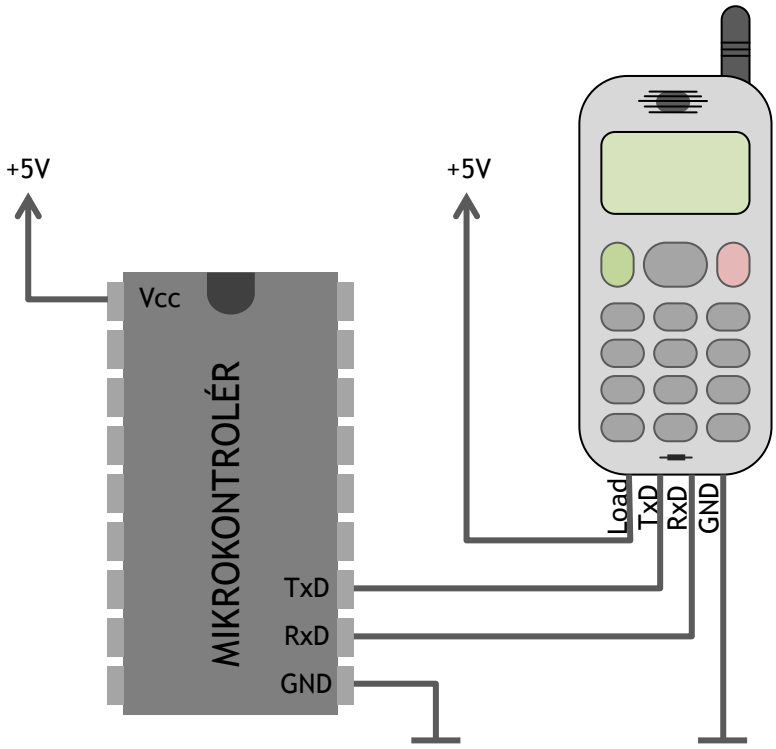
  <CR> <LF> <odpověď> OK <CR> <LF>

Při komunikaci mobilního telefonu s mikrokontrolérem, je část *<LF>* nahrazena znakem $0A_{hex}$.

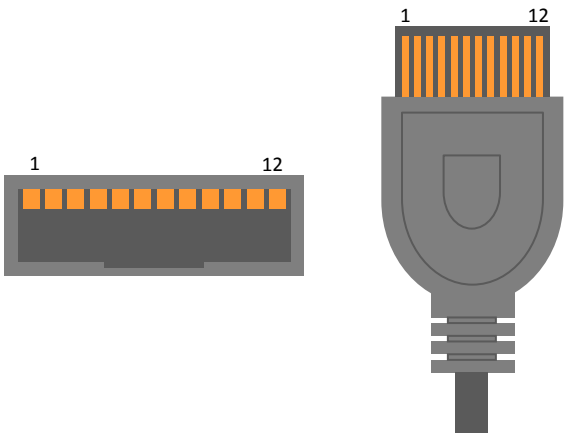
Nejjednodušším AT příkazem je příkaz **AT**, který ověří spojení s mobilním telefonem. Je-li vše v pořádku, mobilní telefon odpovídá znaky **OK**.



Obrázek 14: Příklad komunikace mobilního telefonu s mikrokontrolérem



Obrázek 15: Blokové schéma připojení mobilního telefonu k mikrokontroléru



a) b)

PIN	POPIS
1	GND
2	Self Service (informace o nabíjení)
3	Load (vstup pro nabíjení)
4	Výstup baterie
5	Data TxD
6	Data RxD
7	Detekce/CLK
8	Detekce/Data
9	GND pro externí mikrofon
10	Vstup pro externí mikrofon
11	Výstup pro externí reproduktor
12	GND pro externí reproduktor

Obrázek 16: Rozložení pinů systémového konektoru Siemensu C35

a) systémový konektor v telefonu, b) přívodní kabel k systémovému konektoru

AT příkaz	Příklad povelu do MT	Příklad odpovědi z MT	Popis
ATE	ATE0	OK	zapnutí/vypnutí echo (echo. MT před potvrzováním příkazů vrací také přijatý příkaz)
AT+CMGS	AT+CMGS=21 <CR> 0100 0C 91 247077214365 000009 4424685E96DBD373 <CTRL-Z>	> +CMGS: (mr) OK mr=reference zprávy	odeslání SMS ve tvaru PDU
AT+CPMS?	AT+CPMS?	+CPMS: "SM",1,15,"SM",0,15,"SM",2,15 OK	výčet obsazení paměťového prostoru SMS zpráv (číslo za symbolem "SM" udává počet přijatých zpráv – přečtené+nepřečtené)
AT+CMGR	AT+CMGR=1	+CMGR: 0,,21 07912460305001300 40C9124707347696500F19050713163128002CF25 OK	přečtení zprávy (číslo udává pozici zprávy, která má být přečtena)
AT+CMGD	AT+CMGD=1	OK	vymazání SMS zprávy (číslo udává pozici zprávy, která má být smazána)
ATD	ATD0602123456;	OK	vytočení telefonního čísla

Tabulka 1: Využité AT příkazy v modelu EZS [27]

AT příkaz	Příklad povelu do MT	Příklad odpovědi z MT	Popis
ATA	ATA	OK	vyzvednutí příchozího hovoru
ATH	ATH	OK	zrušení probíhajícího hovoru (zavěšení)
AT+CPBR	AT+CPBR=1,2	CPBR: 1,"931123456",129,"PEPA" +CPBR: 2,"9501234567",129,"TONDA" OK	vyčtení seznamu telefonních čísel z MT od pozice 1 do pozice 2
AT+CMSS	AT+CMSS=1 AT+CMSS=1,+420603123456	+CMSS:.12 OK	odeslání zprávy uložené v seznamu (číslo udává pozici zprávy, která má být smazána)
AT+CMGS	AT+CMGS=21 <CR> 0100 0C 91 247077214365 000009 4424685E96DBD373 <CTRL-Z>	+CMGS: (mr) OK mr=reference zprávy	odeslání SMS ve tvaru PDU
AT+CLIP	AT+CLIP=1	OK	zapnutí zobrazování telefonního čísla příchozího hovoru
AT+CCLK	AT+CCLK?	+CCLK: "03/01/04,16:30:04"	vyčtení data a času z MT

Tabulka 2: Příklady dalších AT příkazů [27]

6.1 PDU FORMÁT SMS ZPRÁV

Mobilní telefon přenáší, zpracovává a ukládá SMS zprávy ve formátu PDU (Protocol Description Unit). Pouze pro zobrazení na displej mobilního telefonu jsou SMS zprávy převáděny z formátu PDU do souvislého textu seskládaného z ASCII znaků. SMS zpráva ve formátu PDU je tvořena hexadecimálním kódem reprezentujícím užitečná data, ve kterých je zakódován text zprávy, a hlavičkou se zápatím, které nesou řidící informace. PDU rámec je odlišný pro přijaté a odesílané SMS zprávy (pro příjem je využit protokol SMS-DELIVER, pro odesílání protokol SMS-SUBMIT).

SMS zprávy přenášené po sériové lince mezi mikrokontrolérem a mobilním telefonem jsou rovněž ve formátu PDU. Zprávy směřující z mobilního telefonu do mikrokontroléru (tj. zprávy doručené na mobilní telefon) si mikrokontrolér vždy vyžádá a následně je zpracovává (porovnání zpráv, vyhodnocení zpráv apod.). Zprávy směřující z mikrokontroléru do mobilního telefonu (tj. zprávy mikrokontrolérem vygenerované) jsou určeny k odeslání po síti GSM (samotný proces odesílání po síti GSM zajišťuje již mobilní telefon). Jelikož tyto zprávy mají formát PDU, musí být mikrokontrolér, který řídí odesílání a příjem SMS zpráv prostřednictvím mobilního telefonu, schopen pracovat s informacemi v tomto formátu.

6.1.1 Skladba doručené SMS zprávy v PDU formátu

Příklad SMS zprávy v PDU formátu:

07 91 247077214365 04 0C 91 247077896745 00 00 80211002219480 06 5AB83C6C0F03

07	počet oketů tel. čísla SMS centra ($07_{hex} = 7_{dec}$) (91 24 07 77 21 43 65 → tj. 7 oketů)
91	formát tel. čísla SMS centra (91 – mezinárodní, 81 – národní)
247077214365	tel. číslo SMS centra (420 777 123 456 – viz kapitola 6.2.3)
04	typ PDU (první oket PDU rámce)
0C	počet čísel telefonního čísla odesílatele ($0C_{hex} = 12_{dec}$)
91	formát tel. čísla odesílatele (91 – mezinárodní, 81 – národní)
247077896745	tel. číslo odesílatele (420 777 987 654 – viz kapitola 6.2.3)
00	byte PID – určuje protokol a formát SMS zprávy, např.: 00 – obyčejná SMS 01 – telex 02 – fax (skupina 3) 03 – fax (skupina 4) 04 – telefon pevné linky (tj. konverze do hlasu)
00	DCS – určuje kódovací schéma dat, např.: 00 – 7 bitová abeceda F6 – 8 bitové datové kódování dle Class 2
80211002219480	datum doručení – rok-měsíc-den-hodina-minuta-vteřina-čas.zóna (01.12.08 20:12:49 GMT+2,00)
06	počet znaků ve zprávě ($06_{hex} = 6_{dec}$)
5AB83C6C0F03	zakódovaný text zprávy – více viz kapitola 6.2.4

Tabulka 3: Skladba doručené SMS zprávy v PDU formátu [32] [33] [34]

6.1.2 Skladba odesílané SMS zprávy v PDU formátu

Příklad SMS zprávy v PDU formátu:

07 91 247077214365 01 00 0C 91 247077896745 00 00 AA 06 5AB83C6C0F03

07	**00**	počet oketů tel. čísla SMS centra ($07_{hex} = 7_{dec}$) (91 24 07 77 21 43 65 → tj. 7 oketů) pokud je na tomto místě uvedeno 00, pak bude použito tel. číslo SMS centra uložené v telefonu.
91	není	formát tel. čísla SMS centra (91 – mezinárodní, 81 – národní)
247077214365	není	tel. číslo SMS centra (420 777 123 456 – viz kapitola 6.2.3)
01		typ PDU (první oket PDU rámce)
00		referenční číslo odeslané zprávy z telefonu do SMS centra (toto číslo přiřazuje telefon)
0C		počet čísel telefonního čísla příjemce ($0C_{hex} = 12_{dec}$)
91		formát tel. čísla příjemce (91 – mezinárodní, 81 – národní)
247077896745		tel. číslo příjemce (420 777 987 654 – viz kapitola 6.2.3)
00		byte PID – určuje protokol a formát SMS zprávy, např.: 00 – obyčejná SMS 01 – telex 02 – fax (skupina 3) 03 – fax (skupina 4) 04 – telefon pevné linky (tj. konverze do hlasu)
00		DCS – určuje kódovací schéma dat, např.: 00 – 7 bitová abeceda F6 – 8 bitové datové kódování dle Class 2
AA		doba platnosti SMS zprávy (AA – 4 dny) - nepovinné (používá se délka 1 nebo 7 oketů)
06		počet znaků ve zprávě ($06_{hex} = 6_{dec}$)
5AB83C6C0F03		zakódovaný text zprávy – více viz kapitola 6.2.4

Tabulka 4: Skladba odesílané SMS zprávy v PDU formátu [32] [33] [34]

6.1.3 Dekódování telefonních čísel v PDU formátu

Telefonní čísla (SMS centrum, příjemce, odesílatel) jsou v PDU rámci zakódovaná. Kódování spočívá v rozdělení souboru čísel do dvojic a přemístění polohy čísel v každé dvojici.

příklad dekódování:

číslo v PDU formátu: **247077214365**

původní číslo: **420777123456**

6.1.4 Dekódování textu SMS zprávy v PDU formátu

Každý znak vlastního textu SMS zprávy je zakódován do jednoho oketu, který je vložen do rámce zprávy v PDU formátu. Jelikož se v SMS zprávách neobjevuje diakritika, je využito pouze 128 znaků z ASCII souboru. Na zakódování 128 znaků do binární podoby postačí pouze 7 bitů, proto je vždy na nejvyšší pozici (MSB) binárního kódu „0“.

Při dekódování SMS zprávy z PDU formátu je nutné postupovat v těchto krocích:

1. Rozdělení zápisu zprávy do částí po osmi oketech
2. Převedení každého oketu do binárního vyjádření
3. Odebrání nejvyššího bitu (MSB) prvního oketu
4. Odebrání dvou bitů na nejvyšší pozici druhého oketu a přidání odebraného bitu na nejnižší pozici z předchozího oketu
5. Odebrání tří bitů na nejvyšší pozici třetího oketu a přidání dvou odebraných bitů na nejnižší pozici z předchozího oketu
6. Odebrání čtyř bitů na nejvyšší pozici čtvrtého oketu a přidání tří odebraných bitů na nejnižší pozici z předchozího oketu

7. Odebrání pěti bitů na nejvyšší pozici pátého oketu a přidání čtyř odebraných bitů na nejnižší pozici z předchozího oketu
8. Odebrání šesti bitů na nejvyšší pozici šestého oketu a přidání pěti odebraných bitů na nejnižší pozici z předchozího oketu
9. Odebrání sedmi bitů na nejvyšší pozici sedmého oketu a přidání šesti odebraných bitů na nejnižší pozici z předchozího oketu
10. Odebrání osmi bitů na nejvyšší pozici osmého oketu a přidání sedmi odebraných bitů na nejnižší pozici z předchozího oketu

Tím je získán binární kód ASCII znaků pro první osmici oketů. Pro rozkódování další osmice oketů je potřeba postupovat opět od kroku 3.

11. Převedení získaných 7-bitových binárních kódů do hexadecimální podoby
12. Získání ASCII znaků na základě hexadecimálního kódu

Příklad textu SMS zprávy v PDU formátu:

5AB83C6C0F03

$5A_{hex}$	$B8_{hex}$	$3C_{hex}$	$6C_{hex}$	$0F_{hex}$	03_{hex}
01011010_{bin}	10111000_{bin}	00111100_{bin}	01101100_{bin}	00001111_{bin}	00000011_{bin}
01011010	10111000	00111100	01101100	00001111	00000011
1011010	1110000	1110010	1100001	1110110	1100001
01011010_{bin}	01110000_{bin}	01110010_{bin}	01100001_{bin}	01110110_{bin}	01100001_{bin}
$5A_{hex}$	70_{hex}	72_{hex}	61_{hex}	76_{hex}	61_{hex}
Z	p	r	a	v	a

Tabulka 5: Dekódování textu SMS zprávy v PDU formátu

7. NÁVRH PERIFÉRNÍHO VYBAVENÍ EZS

Model EZS je určen pro zabezpečení menšího objektu s jedním vchodem. Zajišťuje účinné zabezpečení s dálkovým hlášením poplachu. Prostor objektu je monitorován jedním nebo až čtyřmi PIR detektory pohybu a akustické hlášení poplachu obstarává interiérová siréna. Interakci mezi uživatelem a systémem zprostředkovává číselná klávesnice a LCD displej, který uživateli podává zpětnou vazbu ze systému. Systém je také vybaven mobilním telefonem, který zajišťuje dálkovou komunikaci s uživateli.

7.1 DETEKTOR POHYBU

Detekci pohybu v prostoru zajišťuje pasivní infračervený detektor PIR typu F-PDS-901A. Detektor má 6 vývodů, z nichž 2 jsou napájecí (9-16V a GND). Zbývající vodiče, které jsou rozděleny do dvojic (pro čidlo a spínač monitorující kryt detektoru.), slouží pro volání poplachu. Jeden vývod z každé dvojice je vstupní (podává informace z vnějšku do detektoru), druhý výstupní (podává informace z detektoru ven). První dvojici vodičů využívá čidlo snímající pohyb, druhá dvojice náleží rozpínacímu tlačítku, které monitoruje sejmutí krytu detektoru. Detektor je vybaven časovačem, který odpočítává čas 5, 10 nebo 15 sekund (uživatelsky nastavitelné – v modelu EZS nastaveno na 5 sekund). Tato doba určuje, jak dlouho má být rozpojen vstupní vodič s výstupním v případě zaznamenání pohybu. Detektor se umisťuje do výšky 2,2 m a je schopen monitorovat prostor na dálku 12 m do šířky pod úhlem 110° od detektoru.

Do modelu EZS lze připojit celkem 4 PIR detektory pohybu. Jeden z nich je hlavní, který je nutné umístit tak, aby monitoroval pohyb v prostoru hlavního vchodu, v jehož blízkosti je umístěn ovládací panel (klávesnice, LCD displej). Ostatní tři detektory jsou vedlejší a jsou určeny k hlídání ostatních místností v objektu. Hlavní detektor musí být v systému připojen vždy, vedlejší detektory nemusí být připojeny.

Vyhodnocení signálů z PIR detektorů mikrokontrolérem

Vstupní vývod z každé dvojice vývodů (pro čidlo i tlačítko), je nutné napojit na log. 0 a výstupní vývod na pin mikrokontroléru. Tento pin je nutné nastavit jako vstupní a zvednout jeho klidovou úroveň pomocí PULL-UP na log. 1. Není-li v prostoru indikován pohyb, čidlo se nachází v klidovém stavu a propojuje vstupní vodič s výstupním. Do miktokontroléru je tedy přivedena log. 0. Zaznamená-li čidlo pohyb, rozpojí kontakt mezi vstupním a výstupním vodičem. Výstupní vodič tedy ztrácí informaci o log. 0 a nepodává pinu mikrokontroléru úroveň napětí odpovídající log. 0. PULL-UP zvedne napětí na tomto pinu na log. 1, kterou mikrokontrolér zaznamená, čímž dostává informaci, že ve střeženém objektu došlo k pohybu. Na stejném principu rozpínání kontaktu pracuje také rozpínací tlačítko, které monitoruje sejmutí krytu detektoru. Dostane-li se kryt mimo detektor, tlačítko rozepíná obvod a podává tak informaci o absenci krytu.

Obrázek 17: Pasivní infračervený detektor použitý v modelu EZS
(vlevo – v pohotovostním stavu; vpravo – po sejmutí krytu) [22]

7.2 VÝSTUPNÍ ZAŘÍZENÍ

Výstupní zařízení v modelu EZS představuje interiérová siréna typu KPE-1500, která na pachatele útočí svým silným a nepříjemně pronikavým zvukem. Tím se mu snaží znepříjemnit pobyt v objektu a přispívá tak k jeho útěku.

Obrázek 18: Interiérová siréna použitá v modelu EZS [23]

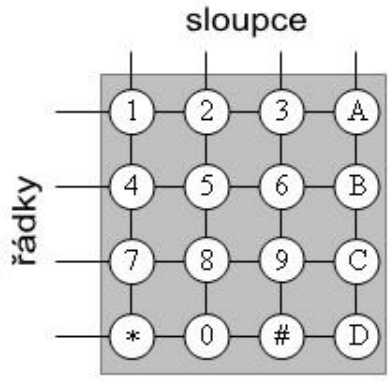
K ústředně je možné připojit také přídavné výstupní zařízení (např. venkovní sirénu). Pro připojení zařízení je ústředna EZS vybavena 2-pinovým konektorem. V případě poplachu vysílá mikrokontrolér na jeden z pinů log. 1, druhý pin je spojen se zemí (GND) systému. Přídavné výstupní zařízení musí být vybaveno vlastním zdrojem napájení, aby systém nezatěžovalo. Přívod z ústředny slouží pouze jako informační bod.

7.3 PŘÍSTUPOVÝ SYSTÉM

Jako přístupový systém byla použita 16-ti tlačítková klávesnice typu F-KV16KEY se čtyřmi sloupci a čtyřmi řádky tlačítek, pomoci nichž je zadáván čtyř místný číselný kód pro deaktivaci EZS. Slouží také k ovládání systému (pohyb v menu, změna nastavení, zadávání údajů). Obsahuje jak číselné klávesy s hvězdičkou a křížkem, tak i volitelné klávesy A, B, C a D.

Obrázek 19: Maticová klávesnice 4x4 použitá v modelu EZS [21]

Maticová klávesnice šetří vývody mikrokontrolérů, protože k 16 tlačítkům je přivedeno pouze 8 signálů (pro 4 řádky a 4 sloupce tlačítek). Každé tlačítko po sepnutí spojí řádek a sloupec, ve kterém se nachází, tím lze jednoduše identifikovat pozici stisknutého tlačítka.



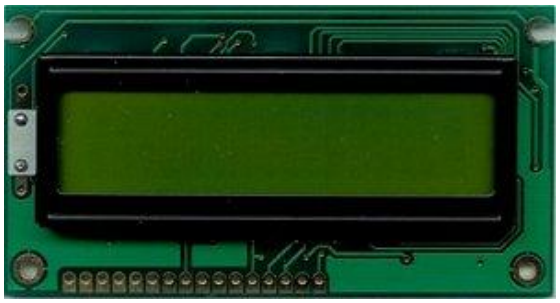
Obrázek 20: Vnitřní zapojení maticové klávesnice 4x4

Identifikace tlačítek mikrokontrolérem

8 vývodů z klávesnice je přivedeno na port mikrokontroléru. Piny portu, na kterých jsou napojeny řádky, jsou nastaveny jako výstupní a piny portu, na kterých jsou napojeny sloupce, jsou nastaveny jako vstupní. V klidovém stavu výstupní piny vysílají na řádky klávesnice log. 1. Vstupní piny jsou pomocí PULL-UP nastaveny také na log. 1. Princip hledání stisknuté klávesy využívá spojení konkrétního řádku a sloupce konkrétním klávesou. Potřebuje-li tedy mikrokontrolér přečíst klávesu, pak nastaví na první řádek klávesnice log.0 a testuje, na kterém ze sloupců se tato log. 0 objeví. Neobjeví-li se log. 0 na žádném sloupci, pak nastaví log. 0 na druhý řádek a opět testuje, na kterém ze sloupců se log. 0 objeví. Takto pokračuje dále, dokud neprojde všechny kombinace řádků a sloupců. Pokud mikrokontrolér zachytí na některém vstupním pinu log. 0, má informaci o spojení řádku se sloupcem, na základě čehož je schopen identifikovat stisknutou klávesu.

7.4 ZOBRAZOVACÍ PRVEK

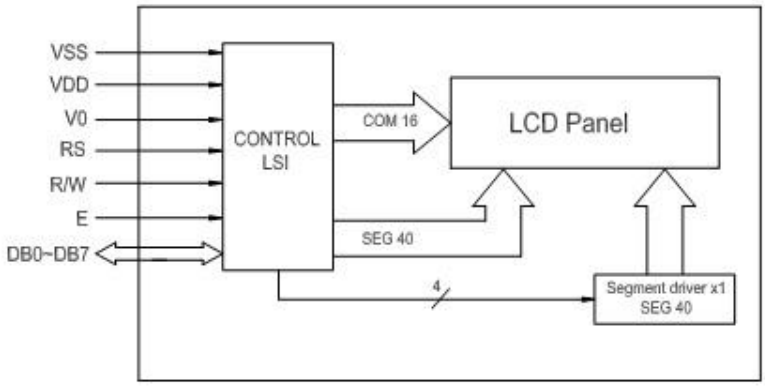
Jako zobrazovací prvek stavů a událostí modelu EZS je využit podsvícený LCD displej typu MC1602E-SYL/H, který je napájen 5V. Dokáže zobrazit 16 znaků na 2 řádcích. Displej je osazen řadičem HD44780 od firmy Hitachi. Lze předem zvolit, zda bude displej komunikovat s mikrokontrolérem po 8-bitové sběrnic (DB0 - DB7) nebo po 4-bitové sběrnici (DB4 - DB7), jak je tomu v případě modelu EZS. 4-bitovou komunikaci je vhodné použít při nedostatku vývodů procesoru, komunikace je ovšem 2x pomalejší, protože se data posílají nadvakrát. Nižší 4 bity (DB0 - DB3) na displeji se nezapojují. Pro komunikaci po 4-bitové sběrnici je využito celkem 12 vodičů (7 datových signálů, 1 signál pro nastavení kontrastu displeje, 2 vodiče pro napájení displeje, 2 vodiče pro napájení LED podsvícení). Každý znak je na displeji zobrazován jako matice 5x8 bodů, definice jednotlivých znaků je uložena napevno ve vnitřní paměti ROM. Je také možné vytvořit až 8 vlastních znaků a uložit je do paměti CGRAM. Dále je možné zobrazit kurzor, nastavit blikání kurzoru, definovat posouvání zobrazených znaků, smazat displej, zobrazovat znaky na konkrétní pozici apod. Každá matice 5x8 bodů má svou adresu, první řádek začíná od adresy 80_{hex}, končí na adrese $8F_{hex}$. Druhý řádek pak začíná od adresy $C0_{hex}$ a končí na adrese CF_{hex}. Displej dokáže pracovat v teplotách od -20°C do 70°C.



Obrázek 21: LCD displej MC1602E-SYL/H použitý v modelu EZS [15]

Vývod	Název	Popis
1	Vss	Napájení displeje GND
2	Vdd	Napájení displeje +5V
3	Vo	Kontrast (0V – 5V)
4	RS	Register Select (0 – instrukce; 1 – data)
5	R/W	Read/Write (0 – zápis; 1 – čtení)
6	E	Enable
7	DB0	Data Bus 0
8	DB1	Data Bus 1
9	DB2	Data Bus 2
10	DB3	Data Bus 3
11	DB4	Data Bus 4
12	DB5	Data Bus 5
13	DB6	Data Bus 6
14	DB7	Data Bus 7
15	A	Podsvícení displeje (Anoda LED +4.2V)
16	K	Podsvícení displeje (Katoda LED GND)

Tabulka 6: Zapojení vývodů LCD displeje MC1602E-SYL/H



Obrázek 22: Blokové schéma LCD displeje MC1602E-SYL/H [42]

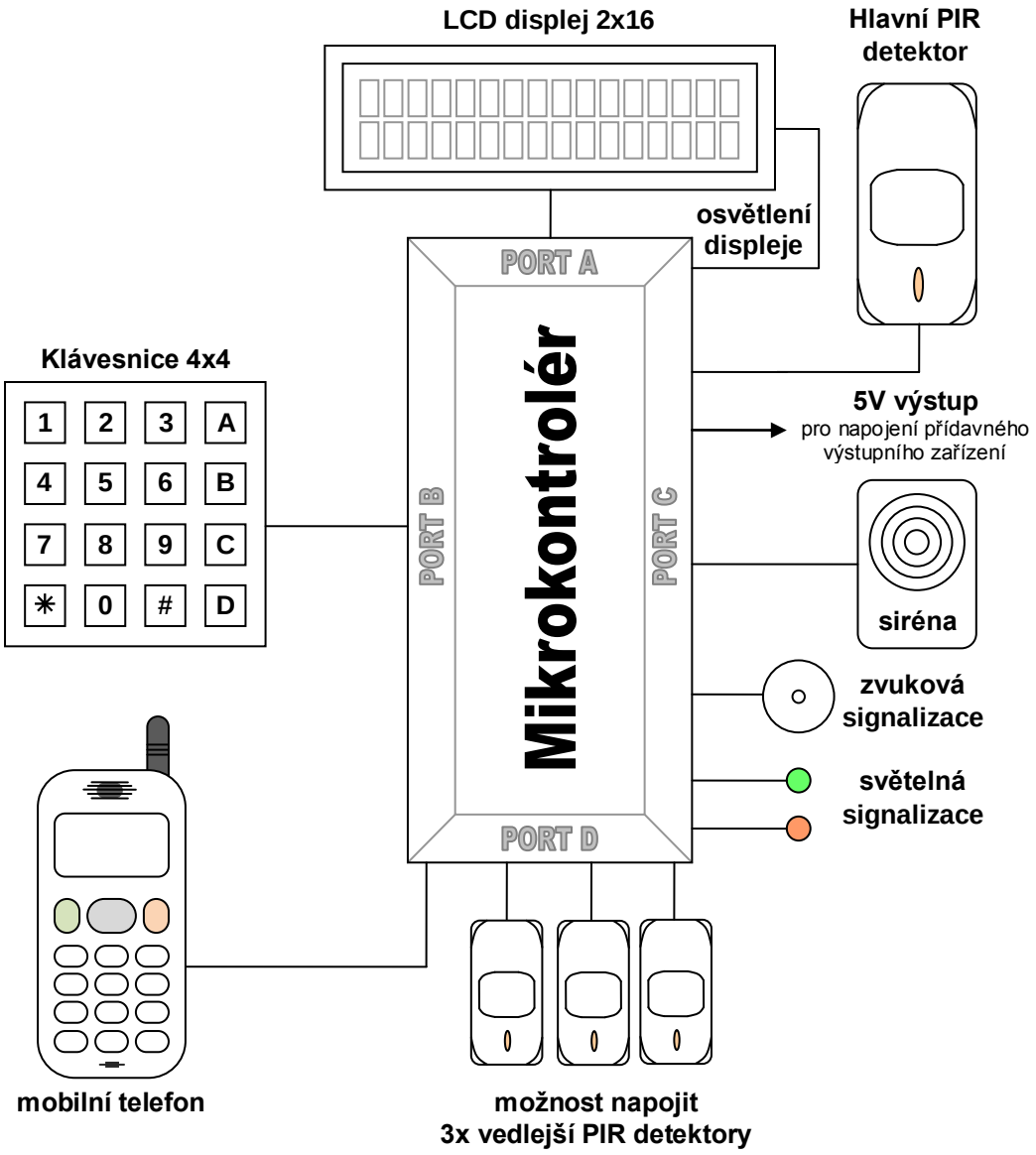
7.5 KOMUNIKAČNÍ ZAŘÍZENÍ

Funkci komunikačního zařízení v modelu EZS plní mobilní telefon Siemens C35. V telefonu je implementován hardwarový modem, který zajišťuje komunikaci po sériové lince. Prostřednictvím sériové linky mobilní telefon odesílá externě vyžádaná data a přijímá AT příkazy, které tvoří základ strojového ovládání telefonu. Strojové ovládání mobilního telefonu zajišťuje mikrokontrolér, jehož sériová linka je využita k odesílání řídících AT příkazů a příjmu vyžádaných dat z mobilního telefonu. Datové vodiče mobilního telefonu jsou křížově připojeny k datovým vodičům mikrokontroléru, tedy vysílání mobilního telefonu (TxD) je připojeno na příjem mikrokontroléru (RxD) a příjem mobilního telefonu (RxD) je připojen na vysílání mikrokontroléru (TxD). Spojením mikrokontroléru s mobilním telefonem vzniká řízený komunikační celek.

Obrázek 23: Komunikační zařízení Siemens C35 použité v modelu EZS [24]

8. NÁVRH ÚSTŘEDNY MODELU EZS

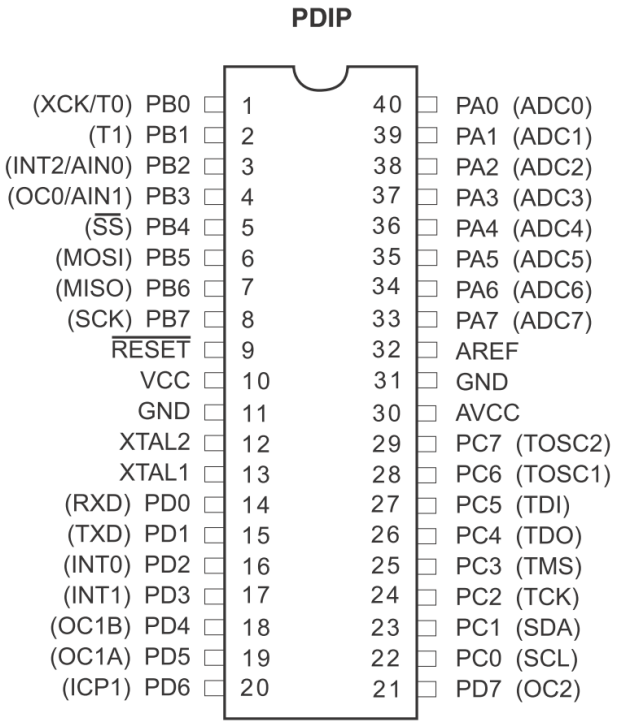
Ústředna zabezpečovacího systému zajišťuje kompletní řízení celého systému. Je vybavena řídícím mikrokontrolérem, který obsluhuje všechny komponenty zabezpečovacího systému. Ústředna je osazena konektory pro připojení všech těchto komponentů.



Obrázek 24: Blokové schéma modelu elektronického zabezpečovacího systému

8.1 VOLBA VHODNÉHO MIKROKOTROLÉRU ATMEGA PRO REALIZACI ÚSTŘEDNY EZS

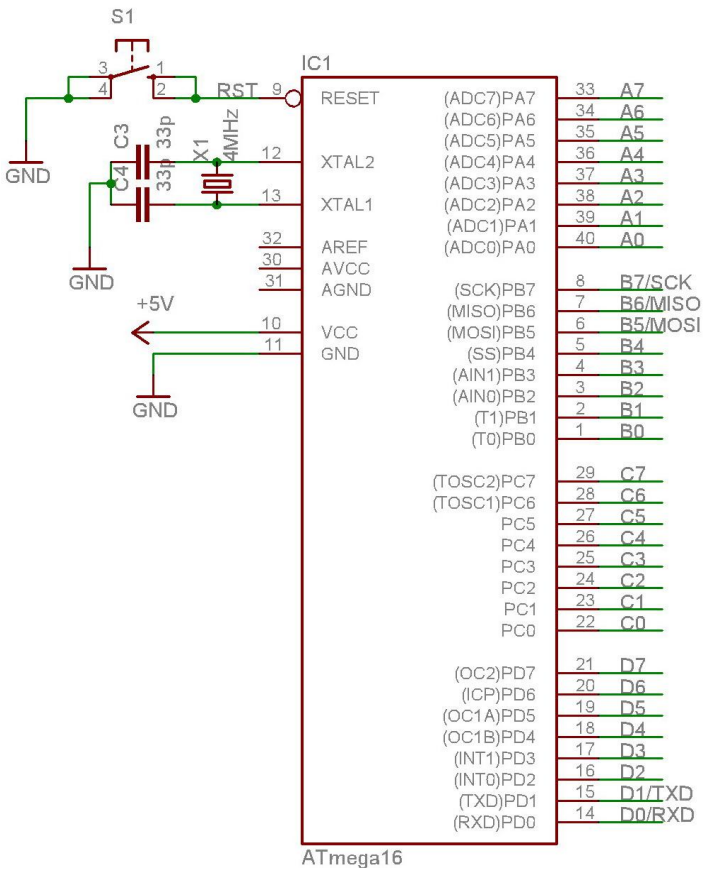
Jako nejvhodnější mikrokontrolér pro řízení elektronického zabezpečovacího systému pro zabezpečení menšího soukromého objektu se jeví 8-bitový mikrokontrolér ATmega16, který má 32 vstupů/výstupů, což je dostatečný počet pro realizaci EZS. Dokáže obsloužit všechny zvolené komponenty. ATmega8 se svými 23 vstupy/výstupy by také byla schopna obsluhovat EZS, ovšem jednalo by se pouze o velmi základní zabezpečení s malým počtem zabezpečovacích, zobrazovacích a signalizačních prvků. ATmega64 má již příliš mnoho vstupů/výstupů (konkrétně 53), což je pro elektronické zabezpečení menšího objektu zbytečně mnoho. Tento mikrokontrolér by byl vhodnější pro řízení zabezpečovacího systému určeného pro větší objekty. Mikrokontrolér ATmega16 je na českém trhu snadno dostupný za přijatelnou cenu.



Obrázek 25: Rozložení pinů mikrokontroléru AVR ATmega16 v pouzdře PDIP

[38]

8.1.1 Schéma zapojení mikrokontroléru



Obrázek 26: Schéma zapojení mikrokontroléru

Na pin VCC mikrokontroléru je připojeno napájecí napětí 5V. Pin GND je spojen se zemí. Na porty mikrokontroléru jsou připojeny všechny komponenty systému, které mikrokontrolér obsluhuje.

Reset mikrokontroléru obsluhuje tlačítko, které stiskem spojuje pin RST se zemí. Tím je mikrokontrolér resetován, tedy uveden do počátečního stavu.

Externí krystal 4MHz zajišťuje taktovací frekvenci mikrokontroléru, zapojení krystalu viz [38].

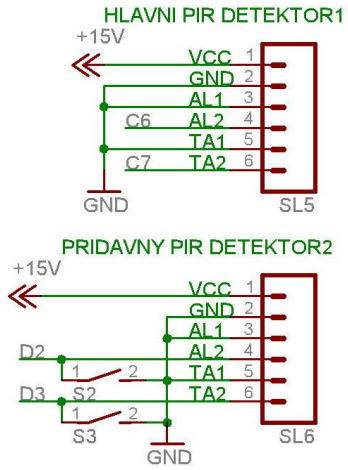
8.2 PŘIPOJENÍ PERIFÉRIÍ K MIKROKONTROLÉRU ATMEGA16

Periférie využívají všech čtyř 8-bitových portů mikrokontroléru ATmega16. Klávesnice je napojena na 8 bitů portu B. Port A je přiřazen LCD displeji, který informuje uživatele o stavu EZS nebo o prováděné akci na EZS. LCD displej využívá pouze 7 pinů portu A, jeden pin portu není zapojen. Na port C jsou napojeny komponenty modelu EZS, jako jsou hlavní detektor, siréna, 5V výstup pro napojení dalšího výstupního zařízení, dvoubarevná světelná signalizace, zvuková signalizace a osvětlení LCD displeje. Je využito všech pinů portu C. Na port D lze napojit až 3 přídavné detektory pohybu pro střežení dalších místností v objektu. Bity 0 a 1 portu D plní zároveň funkci datových pinů sériové linky mikrokontroléru, na které je napojen mobilní telefon. Následující tabulka detailně popisuje připojení periférií k jednotlivým portům mikrokontroléru ATmega16.

ATmega16		Periférie	ATmega16		Periférie
Port	**Bit**		**Port**	**Bit**	
A	0	LCD displej – Data Bus 4	C	0	osvětlení LCD displeje
	1	LCD displej – Data Bus 5		1	Světelná signalizace – červená LED dioda
	2	LCD displej – Data Bus 6		2	Světelná signalizace – zelená LED dioda
	3	LCD displej – Data Bus 7		3	Zvuková signalizace - bzučák
	4	Nezapojen		4	Siréna
	5	LCD displej – Read/Write		5	Výstup pro napojení přídavného výstupního zařízení
	6	LCD displej – Enable		6	Hlavní PIR detektor 1 – čidlo pohybu
	7	LCD displej – Register Select		7	Hlavní PIR detektor 1 - tlačítko
B	0	Klávesnice - sloupec 1	D	0	Mobilní telefon – TxD
	1	Klávesnice - sloupec 2		1	Mobilní telefon – RxD
	2	Klávesnice - sloupec 3		2	Vedlejší PIR (detektor 2) – čidlo pohybu
	3	Klávesnice - sloupec 4		3	Vedlejší PIR (detektor 2) – rozpínací tlačítko
	4	Klávesnice - řádek 1		4	Vedlejší PIR (detektor 3) – čidlo pohybu
	5	Klávesnice - řádek 2		5	Vedlejší PIR (detektor 3) – rozpínací tlačítko
	6	Klávesnice - řádek 3		6	Vedlejší PIR (detektor 4) – čidlo pohybu
	7	Klávesnice - řádek 4		7	Vedlejší PIR (detektor 4) – rozpínací tlačítko

Tabulka 7: Detailní výpis připojení periférií k mikrokontroléru ATmega16

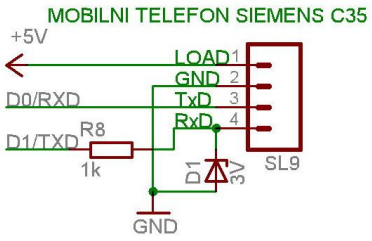
8.2.1 Připojení detektorů k mikrokontroléru



Obrázek 27: Schéma připojení detektorů k mikrokontroléru

Ke každému detektoru je potřeba přivést šest vodičů. Dva z nich jsou napájecí (VCC, GND), dva náleží čidlu pohybu (AL1, AL2), a zbylé dva jsou připojeny k tlačítku snímající nasazení krytu detektoru (TA1, TA2). Detektory je potřeba napájet napětím 9-16V. Jeden z dvojice vodičů, které náleží čidlu pohybu, je nutné spojit se zemí, čímž je v případě, že čidlo neregistruje pohyb, zajištěn přívod log. 0 do druhého tzv. komunikačního vodiče, který je napojen na příslušné piny portu mikrokontroléru. Prostřednictvím log. 0, která přichází po komunikačním vodiči, dostává mikrokontrolér informaci, že ve střeženém prostoru nedochází k pohybu. Stejný princip platí i pro dvojici vodičů připojených k tlačítku detektoru. Jelikož není připojení vedlejších přídavných PIR detektorů podmínkou, součástí komunikačního vodiče je spínač, který v případě absence vedlejšího PIR detektoru spojuje komunikační vodič se zemí.

8.2.2 Připojení mobilního telefonu k mikrokontroléru



Obrázek 28: Schéma připojení mobilního telefonu k mikrokontroléru

K telefonu jsou přivedeny 4 vodiče, z nichž dva jsou napájecí a dva datové. Datové vodiče zajišťují přenos AT příkazů. Mobilní telefon je napájen napájecím napětím 5V, které je přivedeno na pin LOAD konektoru mobilního telefonu. Datové vodiče TxD a RxD mobilního telefonu jsou připojeny k datovým vodičům sériové linky mikrokontroléru. Protože mobilní telefon pracuje ve 3V logice, je nutné 5V logiku mikrokontroléru snížit, konkrétně jde o snížení napěťové úrovně signálu TxD mikrokontroléru. Stabilizaci napětí zajišťuje Zenerova dioda 3V zapojena v závěrném směru a rezistor 1kΩ (viz [26]). Proud diodou je rezistorem omezen na 2mA. Jelikož mikrokontrolér je schopen rozlišovat příchozí signály i ve 3V logice, není potřeba úroveň signálu TxD z mobilního telefonu zvyšovat.

$$R_8 = \frac{U_{VST} - U_{VYST}}{I_{ZEN}} = \frac{5-3}{0{,}002} = 1000\,\Omega$$

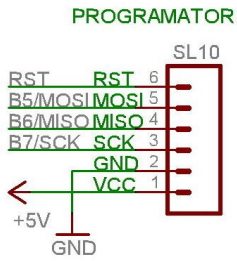
U_{VST} .....*vstupní napětí nepřizpůsobené*

U_{VYST} .....*přizpůsobené napětí pro logiku mobilního telefonu*

I_{ZEN} .....*zvolený proud diodou*

Z řady E12 byl vybrán odpor 1kΩ.

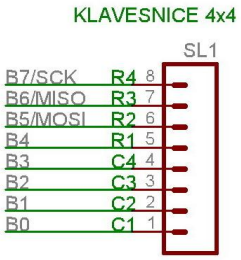
8.2.3 Připojení programátoru k mikrokontroléru



Obrázek 29: Schéma připojení programátoru k mikrokontroléru

K programátoru je potřeba přivést šest vodičů, z nichž dva jsou napájecí a čtyři programovací. Programátor používaný pro programování mikrokontroléru ATmega16 v modelu EZS není napájen vlastním zdrojem, proto je programátor nutné napájet přímo z mikroprocesorového systému a to napětím 5V. Programovací vodiče jsou připojeny na programovací piny mikrokontroléru.

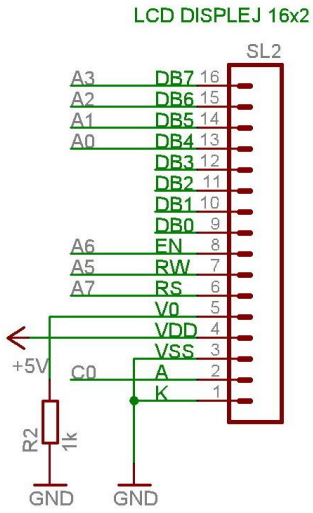
8.2.4 Připojení klávesnice k mikrokontroléru



Obrázek 30: Schéma připojení klávesnice k mikrokontroléru

Mikrokontrolér obsluhuje klávesnici bez jakýchkoli řídících obvodů, proto jsou sloupce i řádky klávesnice napojeny na mikrokontrolér přímo na piny portu B.

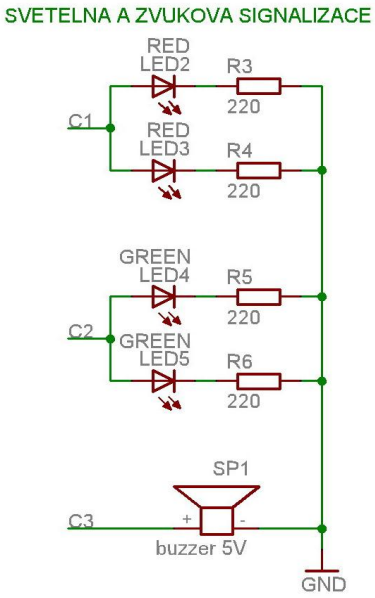
8.2.5 Připojení LCD displeje k mikrokontroléru



Obrázek 31: Schéma připojení LCD displeje k mikrokontroléru

Obsluhu displeje provádí mikrokontrolér, proto jsou řidící signály a datové vodiče displeje připojeny přímo na bity 5-7 portu A mikrokontroléru. Jas displeje lze nastavit velikostí odporu R_2 připojeného mezi zemí a pinem V0 displeje pro řízení jasu. Hodnota odporu R_2 byla stanovena experimentálně pomocí trimru. Při $R_2 = 1k\Omega$ lze nastavení jasu displeje označit za optimální. LCD displej je podsvícený, jeho osvětlení řídí mikrokontrolér bitem 0 na portu C. Displej pracuje ve 4-bitovém režimu, proto jsou nižší čtyři datové vodiče (DB0 – DB3) nezapojené.

8.2.6 Připojení světelné a zvukové signalizace k mikrokontroléru



Obrázek 32: Schéma připojení světelné a zvukové signalizace k mikrokontroléru

Světelná a zvuková signalizace v podobě červených LED diod, zelených LED diod a bzučáku je opět přímo připojena na piny portu C mikrokontroléru. Jedna z dvojic LED diod (červená+zelená) je určena pro umístění na ústřednu a druhá dvojice je určena pro umístění do ovládacího panelu. Velikost odporů, přes které jsou diody připojeny na GND, lze stanovit ze vztahu:

$$R_3 = R_4 = R_5 = R_6 = \frac{U_{NAP} - U_D}{I_{LED}} = \frac{5-2}{0{,}014} = 214{,}29\Omega$$

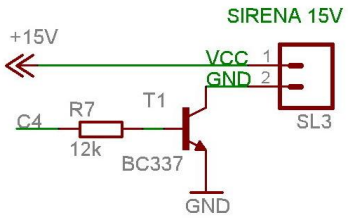
U_{NAP} .....nepájecí napětí diody

U_D .....úbytek napětí na diodě (viz [43])

I_{LED} .....optimální proud diodou (viz [43])

Z řady E12 byl vybrán odpor 220Ω.

8.2.7 Připojení sirény k mikrokontroléru



Obrázek 33: Schéma připojení sirény k mikrokontroléru

Sirénu je nutné napájet napětím 6-15V. Poplach sirény je řízen mikrokontrolérem, který je schopen poskytnout napětí pouze 5V. Jelikož k rozezvučení sirény jsou určeny pouze 2 napájecí vodiče, musel být použit tranzistor jako spínač, který na základě 5V signálu připojí napájecí vodiče sirény k napětí 15V, čímž se siréna rozezvučí.

Tranzistor BC337 byl zvolen na základě jeho maximálního dovoleného napětí mezi kolektorem a emitorem $U_{CE} = 45V$ a podle maximální zatížitelnosti kolektoru proudem $I_c=500mA$. Jelikož siréna je napájena napětím 15V a odebírá proud 300mA, není překročeno ani maximální dovolené napětí U_{CE} ani maximální zatížitelnost kolektoru proudem I_c a lze ji k tomuto tranzistoru bez problému připojit.

Spínání tranzistoru je řízeno prostřednictvím báze, která je přes odpor R_7 připojena k bitu 4 portu C mikrokontroléru. Jeho velikost je dána vztahem:

$$R_7 = \frac{U_{NAP} - U_{BE}}{I_B} = \frac{U_{NAP} - U_{BE}}{\frac{I_C}{\beta}} = \frac{5 - 0{,}6}{\frac{0{,}4}{100}} = 1100\,\Omega$$

U_{NAP} .....napětí z pinu mikrokontroléru, které je přes R_9 přivedeno na bázi

U_{BE} .....napětí na tranzistoru mezi bází a emitorem (viz [43])

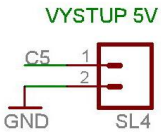
I_B .....proud báze

I_C .....proud v kolektoru

β ..... zesilovací činitel tranzistoru (viz [43])

Z řady E12 byl vybrán odpor 1,1kΩ.

8.2.8 Připojení 5V poplachového výstupu k mikrokontroléru



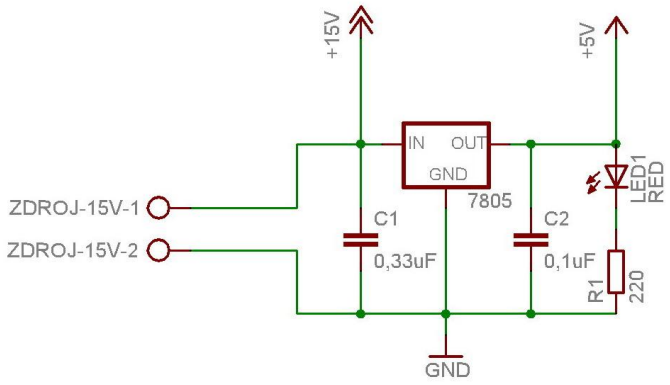
Obrázek 34: Schéma připojení 5V poplachového výstupu k mikrokontroléru

Na konektor pro připojení přídavného výstupního zařízení je přiveden signál z bitu 5 portu C mikrokontroléru, který v případě poplachu vysílá napětí 5V. Externí poplachové zařízení, které tento signál přijímá, by mělo být vybaveno vlastním napájecím zdrojem, aby nezatěžovalo mikroprocesorový systém. 5V signál by měl tomuto zařízení sloužit pouze jako indikátor poplachu, nikoli také jako napájecí bod.

8.3 NAPÁJENÍ ÚSTŘEDNY

Ústředna je vybavena konektorem pro připojení napájecího napětí, které napájí jak řídící jednotku, tak i všechny periférie kromě přídavného výstupního zařízení, které musí být napájeno vlastním napájecím zdrojem. Záloha napájení je řešena mimo ústřednu EZS. Pro tento účel je navržen blok záložního napájení, který řeší přepínání mezi hlavním zdrojem a záložním zdrojem napětí.

8.3.1 Schéma zapojení napájecího



Obrázek 35: Schéma připojení napájení do systému

Protože některé komponenty EZS vyžadují napájecí napětí 12-15V, jiné 5V, je nutné zajistit přítomnost obou napětí v systému. Napětí 15V je získáváno přímo ze zdroje napájecího napětí, stabilizované napětí 5V je získáváno ze stabilizátoru 7805/1A, na jehož vstup je přivedeno napětí 15V ze zdroje. Zapojení stabilizátoru viz [40]. Maximální proudový odběr systému je 900mA. K napájení systému je doporučen zdroj 15V/1A.

Červená LED dioda indikuje přítomnost napájecího napětí. Aby byl dodržen optimální proud diodou $I_{LED} = 14mA$ (viz [43]), je zapojena do série s odporem $R_2 = 220\Omega$.

$$R_1 = \frac{U_{NAP} - U_D}{I_{LED}} = \frac{5-2}{0{,}014} = 214{,}29\Omega$$

U_{NAP} .....*napájecí napětí diody*

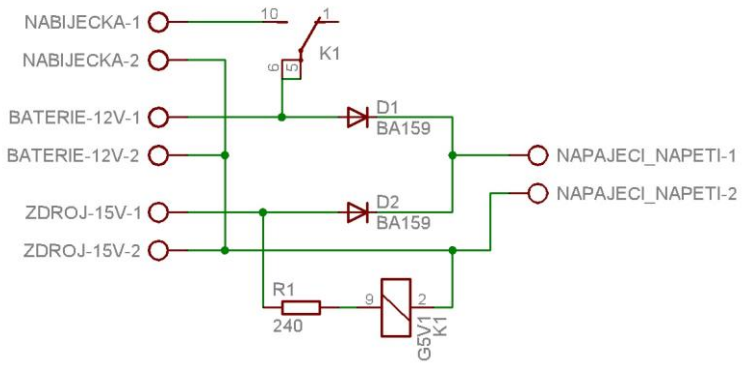
U_D .....*úbytek napětí na diodě (viz [43])*

I_{LED} .....*optimální proud diodou (viz [43])*

Z řady E12 byl vybrán odpor 220Ω.

8.3.2 Záloha napájecího napětí

Napájecí napětí je velmi citlivá součást zabezpečovacího systému. Pokud by byl zabezpečovací systém napájen nezálohovaným napájecím napětím a došlo by k výpadku této sítě, stal by se systém nečinným a přestal by střežit svěřený objekt. Je tedy nutné napájecí napětí zálohovat záložním zdrojem. Jako záložní zdroj lze využít olověný akumulátor 12V. V modelu EZS je využit akumulátor 12V/1,3Ah značky Long typu WP1.3-12. Záložní zdroj je připojen paralelně k hlavnímu napájecímu zdroji napětí. Před spojením kladných potenciálů zdrojů je do každé větve vřazena dioda, která zamezuje zpětnému toku proudu z jednoho zdroje do druhého. Je-li připojeno hlavní napájecí napětí (zdroj 15V), dioda D_1 je zavřená a ze záložního zdroje (baterie 12V) tak není odebírán proud. K vývodům baterie je připojena nabíječka akumulátoru, která zajišťuje nabíjení baterie. V modelu EZS je využita nabíječka typu MW126C05GS. Baterie je nabíjena pouze v případě přítomnosti hlavního napájení. Je totiž nežádoucí, aby baterie byla nabíjena v situaci, kdy se stává zdrojem napájení zabezpečovacího systému. Jelikož je nabíječka napájena ze stejné sítě jako hlavní napájecí zdroj, dochází vlivem výpadku sítě k odpojení hlavního zdroje i nabíječky současně. Pokud by došlo k výpadku hlavního napájení mimo napájecí síť (např. přerušení kabelu vedoucího od zdroje k systému), je obvod opatřen pojistným relé vypínačem, který vypíná spojení baterie a nabíječky v případě nepřítomnosti hlavního napájení. Spínací úroveň relé vypínače G5V1-12 je maximálně 12V. Protože hlavní napájecí zdroj napájí systém 15V, je nutné přizpůsobit napěťovou úroveň pro relé vypínač na 12V. Vřazením odporu R_1 mezi zdroj a relé vzniká napěťový dělič, který napěťovou úroveň přizpůsobí.



Obrázek 36: Schéma zálohy napájecího napětí

$$R_1 = R_{REL} \cdot \frac{U_{ZDR}}{U_{REL}} - R_{REL} = 960 \cdot \frac{15}{12} - 960 = 240\Omega$$

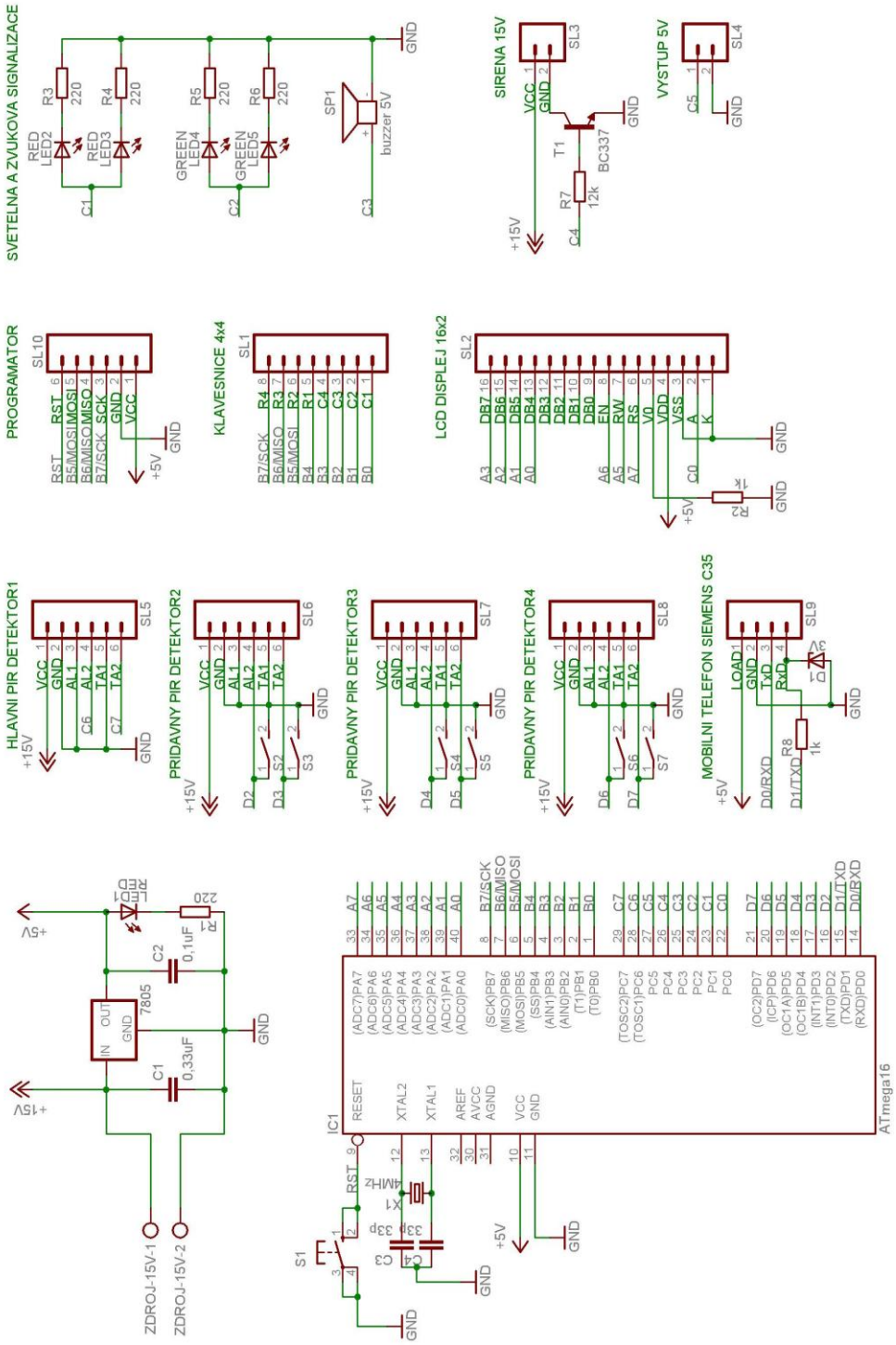
U_{ZDR}.....hlavní napájecí napětí (zdroj 15V)

U_{REL}.....požadované napětí pro relé vypínač

R_{REL}.....odpor relé vypínače (viz [41])

Z řady E12 byl vybrán odpor 240Ω.

8.4 SCHÉMA MIKROPROCESOROVÉHO SYSTÉMU EZS



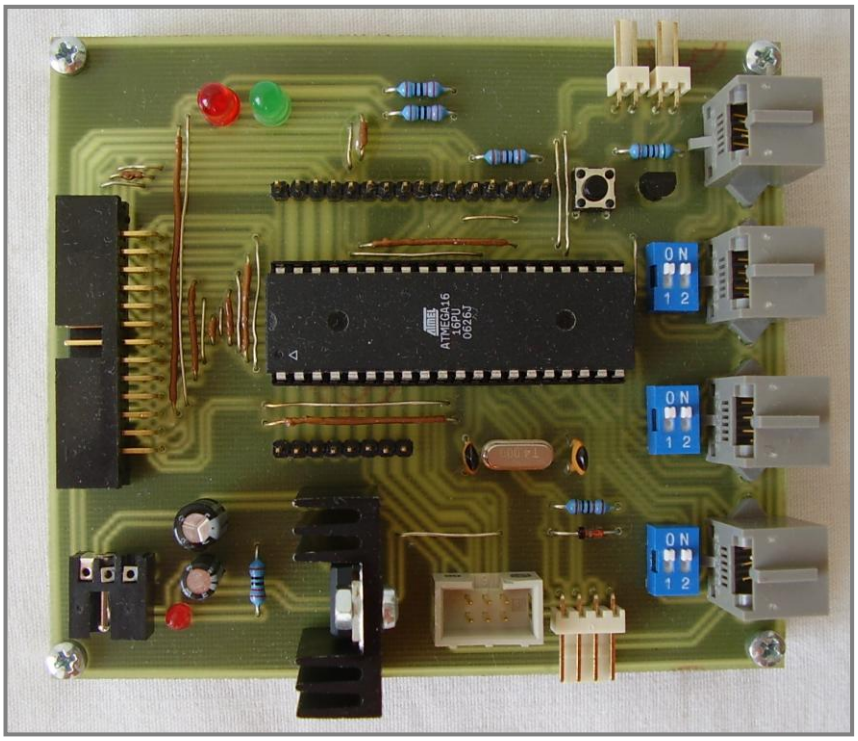
Obrázek 37: Schéma mikroprocesorového systému EZS

9. KONSTRUKČNÍ USPOŘÁDÁNÍ MODELU EZS

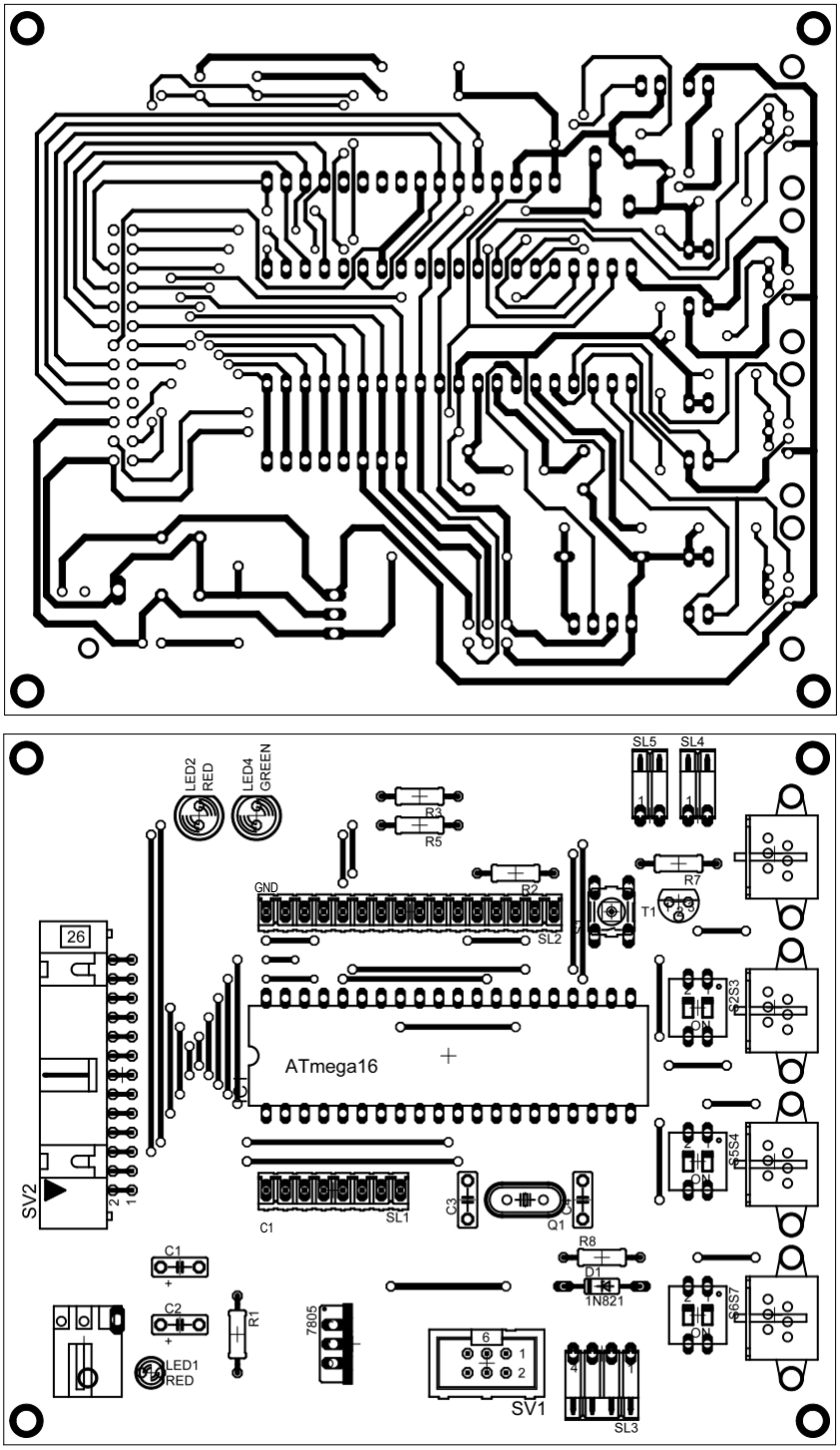
Ústředna EZS je z bezpečnostních důvodů oddělena od ovládacího panelu. Měla by být společně se záložní baterií a mobilním telefonem uložena na takovém místě, kam se nepovolaná osoba není schopna nejméně do 10 sekund od vstupu do objektu dostat. Toto místo by ovšem mělo zůstat zpřístupněné pro oprávněnou osobu (např. z důvodu revize). Ovládací panel by měl být umístěn co nejblíže ke vchodu do objektu, aby byla příchozí osoba schopna do 10 sekund systém deaktivovat.

9.1 ÚSTŘEDNA

Ústředna je nejdůležitější a nejcitlivější částí modelu EZS. Její součástí je řídící jednotka, tedy mikrokontrolér ATmega16, tlačítko reset pro uvedení systému do počátečního stavu v případě náhlé softwarové poruchy, kontrolní LED diody pro indikaci přítomnosti napájení a stavu, ve kterém se EZS nachází, a kontrolní konektory pro přímé napojení klávesnice a LCD displeje.

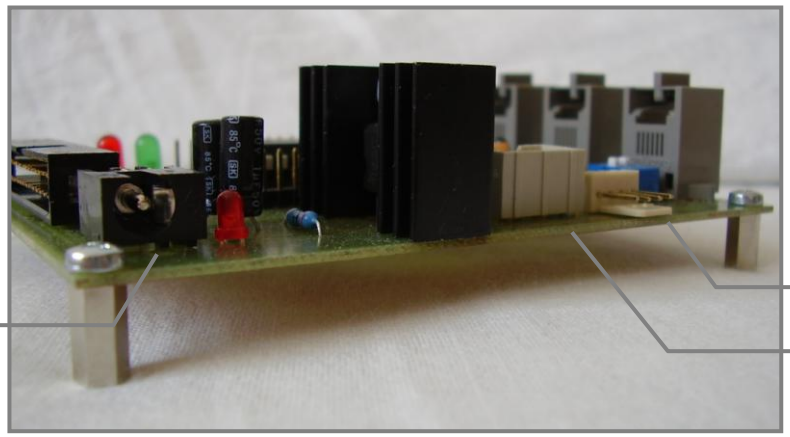


Obrázek 38: Pohled na osazenou desku plošných spojů pro ústřednu



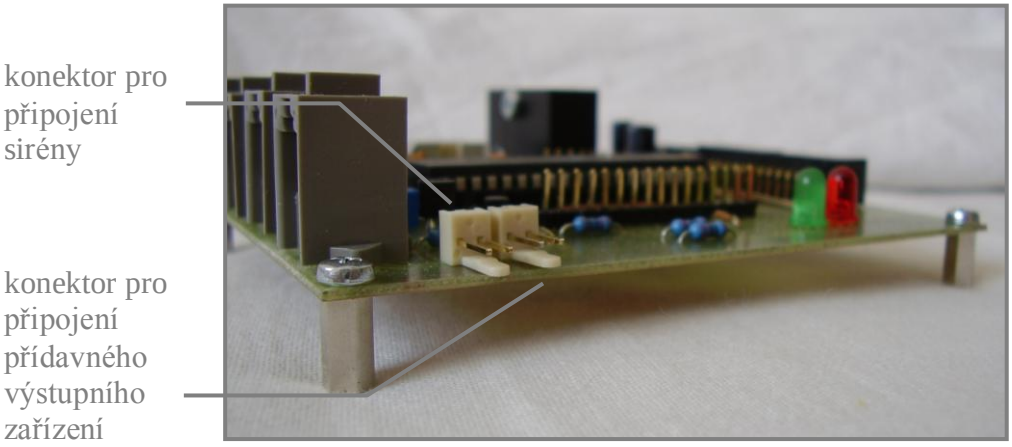
Obrázek 39: Detail desky plošných spojů pro ústřednu (nahoře: cesty, dole: osazení součástkami)

Po obvodu ústředny se nacházejí konektory pro napojení všech komponentů EZS. Čelní strana je osazena konektory pro přívod napájecího zdroje a pro připojení mobilního telefonu. Mezi nimi se nachází konektor pro připojení programátoru, který zajišťuje přívod programovacích signálů k mikrokontroléru v případě využití „in circuit programming“.



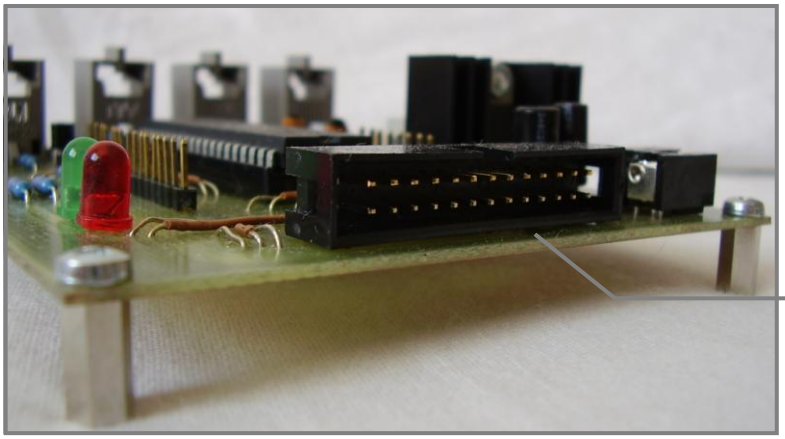
Obrázek 40: Pohled na čelní stranu ústředny

Protější strana je osazena konektory pro připojení výstupních poplachových zařízení. Nachází se zde konektor pro připojení interiérové sirény a konektor pro připojení přídavného poplachového zařízení.



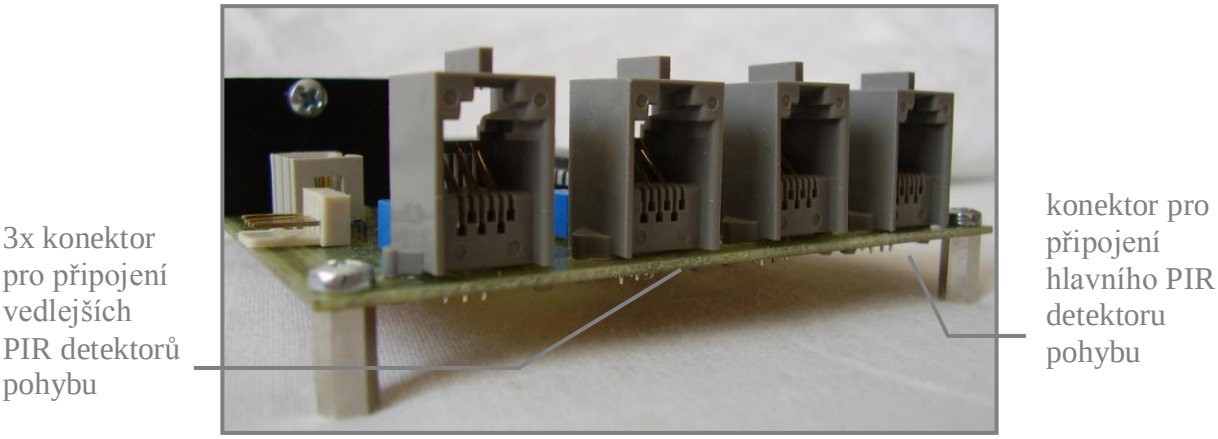
Obrázek 41: Pohled na protejší stranu ústředny

Na spodní straně se nachází konektor pro připojení ovládacího panelu (klávesnice, LCD displej, bzučák, LED diody).



Obrázek 42: Pohled na spodní stranu ústředny

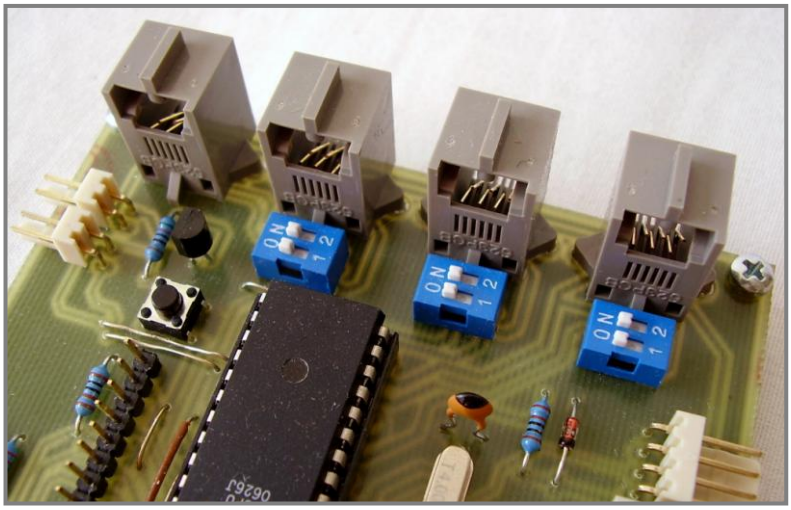
Konektory pro připojení PIR detektorů pohybu se nacházejí na horní straně desky plošných spojů. Lze zde připojit jeden hlavní a tři vedlejší PIR detektory.



Obrázek 43: Pohled na horní stranu ústředny

Každému konektoru pro připojení vedlejšího detektoru náleží dvojitý DIP spínač, který je umístěn za konektorem. Je-li v konektoru připojený detektor a neregistruje-li pohyb, dodává odpovídajícímu pinu mikrokontroléru log. 0. Pokud

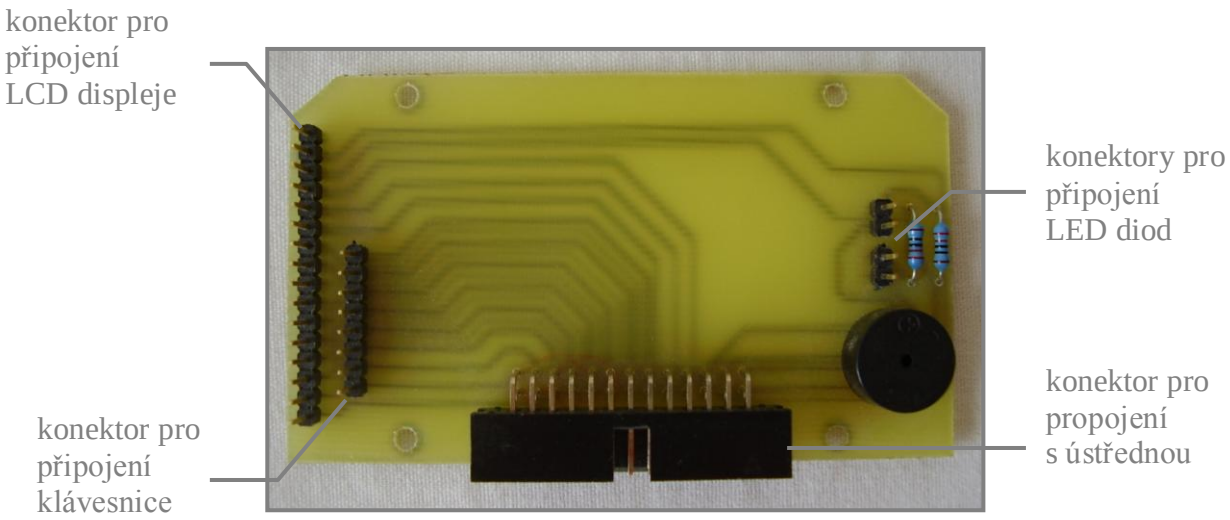
připojený detektor pohyb registruje, nedodává mikrokontroléru žádný signál, z čehož mikrokontrolér vyhodnotí, že detektor zaznamenal pohyb. Není ovšem podmínkou, aby byly v systému vedlejší detektory připojeny. Není-li detektor v konektoru připojen, mikrokontroléru tím pádem není dodáván žádný signál, což navozuje dojem registrace pohybu. Tato kolize je řešena zmiňovanými DIP spínači. V případě absence konkrétního detektoru je nutné sepnout jeho DIP spínač do polohy ON. Tím je přivedena log. 0 na pin mikrokontroléru, na který by měl být detektor připojen. Každý DIP obsahuje dva spínače. První spínač zastupuje čidlo pohybu, druhý spínač zastupuje rozpínací tlačítko, které dodává signál do mikrokontroléru na stejném principu, jako čidlo pohybu. Konektoru pro připojení hlavního PIR detektoru není přiřazen DIP spínač, protože hlavní detektor musí být do systému připojen vždy.



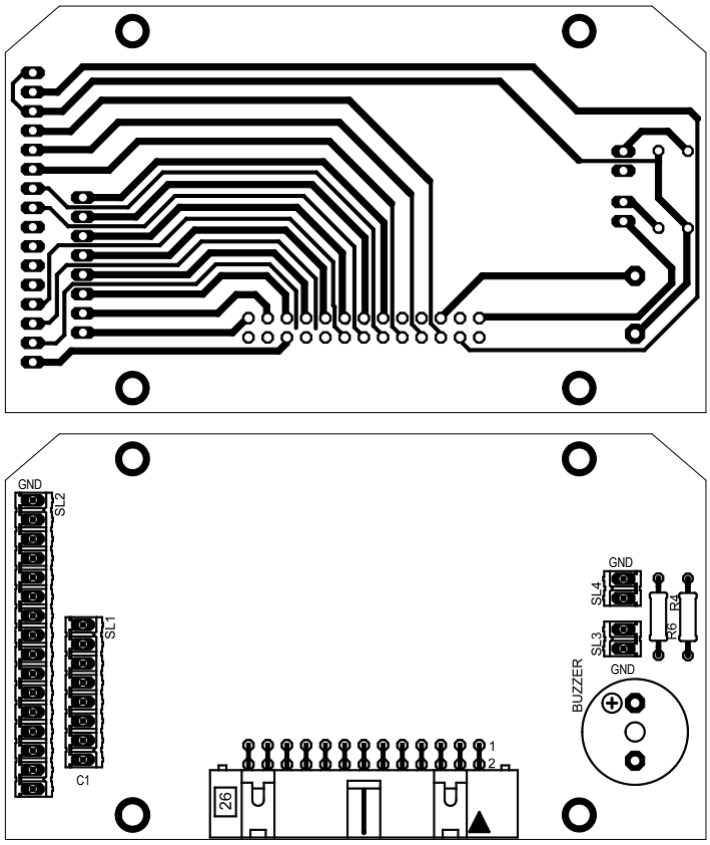
Obrázek 44: Pohled na DIP spínače

9.2 OVLÁDACÍ PANEL (PŘÍSTUPOVÝ SYSTÉM)

Ovládací panel slouží k ovládání modelu EZS a k vizuální kontrole činnosti modelu. Panel obsahuje klávesnici, LCD displej, světelnou signalizaci v podobě červené a zelené LED diody a zvukovou signalizaci.



Obrázek 45: Pohled na osazenou desku plošných spojů pro ovládací panel

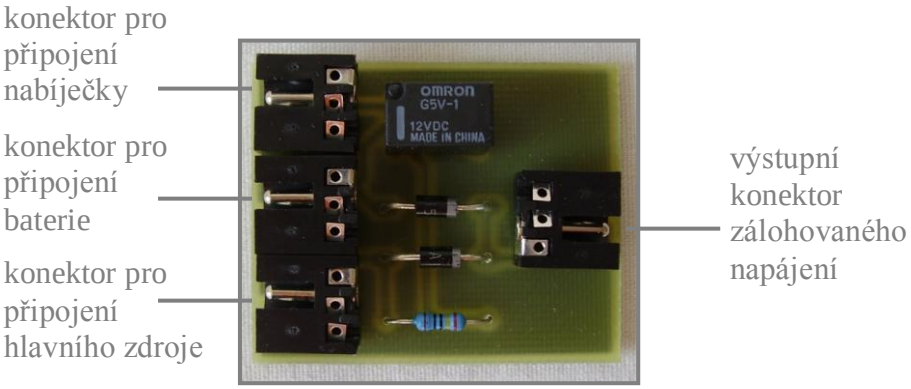


Obrázek 46: Detail desky plošných spojů pro ovládací panel (nahoře: cesty, dole: osazení součástkami)

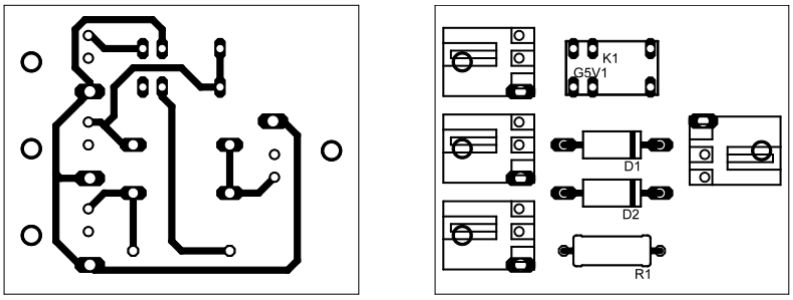
Obrázek 47: Zapouzdřený ovládací panel

9.3 BLOK ZÁLOŽNÍHO NAPÁJENÍ

Blok záložního napájení slouží k rozšíření napájecího zdroje o jeho zálohu. Blok je na čelní straně osazen třemi vstupními konektory pro připojení hlavního zdroje napájení, záložního zdroje napájení a nabíječky pro nabíjení záložního zdroje. Na protější straně se nachází výstupní konektor, z něhož lze odebírat zálohované napájecí napětí pro zabezpečovací systém.



Obrázek 48: Pohled na osazenou desku plošných spojů bloku záložního napájení



Obrázek 49: Detail desky plošných spojů bloku záložního napájení (vlevo: cesty, vpravo: osazení součástkami)

10. FUNKCE MODELU EZS

Model EZS je sestrojen pro zabezpečení menšího objektu s jedním vchodem proti neoprávněnému vniknutí cizí osoby. Je vybaven infračerveným pasivním detektorem PIR, který monitoruje střežený prostor. Zaznamená-li pohyb v zastřeženém prostoru, podá tuto informaci ústředně, která vyčká 10 sekund a dá tak prostor oprávněné osobě zadat pomocí klávesnice čtyř místný uživatelský kód, čímž prostor odstřeží. Nedojde-li do 10 sekund k zadání správného kódu, ústředna dá siréně pokyn k poplachu. Siréna je aktivní maximálně po dobu 5 minut. K zabezpečovacímu systému je připojen mobilní telefon, který zastupuje funkci komunikačního zařízení. Mobilní telefon slouží k hlášení poplachu a ovládání systému.

Kromě těchto základních funkcí, má model EZS ještě tyto vlastnosti:

- LCD displej je podsvícený, systém lze tedy bez problému ovládat i v temných místnostech. Rozsvícení i zhasnutí displeje probíhá automaticky, ovšem je možné displej rozsvítit také manuálně.
- Uživateli je umožněno nastavit si nebo změnit svůj uživatelský kód, který je uložen v EEPROM paměti mikrokontroléru.

přednastavený kód: **5555**

- Lze nastavit a změnit 3 telefonní čísla, na které bude hlášen poplach, a 9 telefonních čísel, která mají oprávnění k dálkovému ovládání systému. Telefonní čísla jsou uložena v EEPROM paměti mikrokontroléru.
- V modelu je implementováno tzv. číslo VK (výrobní kód), kterým lze systém odblokovat v případě zapomenutí uživatelského kódu. Číslo je neměnné.

číslo VK: **2312**

- Model je odolný proti rušení (zákmity) vznikající na klávesnici a v PIR detektorech pohybu.
- Systém využívá mobilní telefon k hlášení poplachu a základnímu ovládání systému.

- Je stanovena maximální doba poplachu. Jestliže nedojde k deaktivaci poplachu, siréna houká 5 minut.
- Po uplynutí maximální doby poplachu, kdy dojde k vypnutí sirény, je nutné, aby uživatel, který později přijde do objektu, byl informován o tom, že došlo k poplachu. Tuto informaci může uživatel odvodit z faktu, že systém nevyžaduje zadání 4 místného uživatelského kódu, ale požaduje zadání čísla VK. Navíc po zadání čísla VK systém uživatele o poplachu upozorní zprávou na displeji.
- Systém zahrnuje diagnostiku hlavního PIR detektoru pohybu. Dokáže zachytit selhání detektoru v případě, že detektor nezaregistruje pohyb ve střežené místnosti dřív, než dojde k zadávání uživatelského kódu příchozí osobou. Systém informuje o selhání detektoru prostřednictvím LCD displeje.
- Systém průběžně ověřuje spojení mezi mikrokontrolérem a mobilním telefonem. Dojde-li k výpadku spojení, systém zobrazí zprávu na LCD displeji s pokyny k odstranění problému.
- Do systému lze zapojit navíc až tři PIR detektory pohybu, které mohou hlídat další místnosti. Systém vyvolává poplach ihned po registraci pohybu některým z těchto čtyř detektorů.
- Model je vybaven výstupem, na který je v případě poplachu vysílána log. 1. Na tento výstup lze napojit přídavné výstupní zařízení, jehož vstup je uzpůsoben pro příjem log. 1 nebo log. 0. Toto zařízení musí být vybaveno vlastním napájecím zdrojem.
- Součástí systému je záložní baterie, která dočasně zajišťuje napájení systému v případě výpadku hlavního zdroje energie.
- Je využito možnosti „in circuit“ programování mikrokontroléru přímo v aplikaci. Deska plošného spoje ústředny je osazena konektorem pro připojení programátoru, což umožňuje mikrokontrolér rychle a bez problému přeprogramovat. Lze tak zajistit případné aktualizace řidícího programu nebo je možné řidící program v rámci možností přizpůsobit uživateli.
- Zničení ovládacího panelu, nemá na funkci systému vliv. Pokud nepovolaná osoba znehodnotí PIR detektor pohybu, je vyvolán poplach.

10.1 VYUŽITÍ MOBILNÍHO TELEFONU V MODELU EZS

Připojení mobilního telefonu do zabezpečovacího systému zvyšuje úroveň míry zabezpečení, neboť hlášení poplachu přímo oprávněné osobě je o mnoho efektivnější. Mobilní telefon vnáší také vyšší komfort do oblasti ovládání systému, lze jej totiž zkontrolovat či odstřežit odkudkoli.

10.1.1 Hlášení poplachu

Mobilní telefon je v modelu EZS využit mimo jiné k hlášení poplachu na dálku. Poplach je hlášen prostřednictvím SMS zpráv až na tři telefonní čísla, která jsou uložena v paměti EEPROM mikrokontroléru. Zaznamená-li zabezpečovací systém neoprávněné vniknutí do objektu, ústředna zadá pokyn mobilnímu telefonu k zaslání první SMS zprávy na telefonní číslo uložené na první pozici v paměti. SMS zpráva má tvar:

POPLACH AKTIVNI.
Po precteni poslete zpet
potvrzovaci SMS ve tvaru:
OK

Příjemce je v SMS zprávě informován o poplachu v objektu a současně je vyzván ke zpětnému zaslání potvrzovací SMS zprávy ve tvaru:

OK

Pokud osoba do 30 sekund odešle potvrzovací SMS zpět na mobilní telefon EZS, je hlášení poplachu považováno za úspěšné a ukončí se (siréna je stále v provozu). Pokud ovšem ústředna EZS nezaznamená příjem potvrzovací SMS zprávy do 30 sekund, vysílá druhou poplachovou SMS zprávu na telefonní číslo uložené na druhé pozici v paměti. Pokud první ani druhá osoba nezašle do 30 sekund potvrzovací SMS, odesílá se třetí poplachová SMS zpráva na telefonní číslo uložené na třetí pozici v paměti. Ústředna nyní očekává do 30 sekund potvrzovací SMS od první, druhé nebo třetí osoby. Pokud informované osoby opět nepodají ve

stanoveném časovém úseku zpětnou vazbu o registraci poplachu, systém vytáčí hovor na telefonní číslo první osoby, čímž osobu informuje o poplachu intenzivnější formou.

10.1.2 Odstřežení objektu

Mobilní telefon je v modelu EZS využit také jako prostředek k odstřežení objektu. K tomuto účelu slouží SMS zpráva, kterou oprávněná osoba zasílá na mobilní telefon zabezpečovacího systému. Mobilní telefon ovšem neslouží jako jediný ovládací prvek, modelu EZS zůstává maticová klávesnice, která stále plní funkci hlavního přístupového systému. Mobilní telefon slouží pouze jako doplňková možnost přístupu. Výhoda dálkového odstřežení spočívá ve včasné deaktivaci zabezpečení, kterou se majitel po vstupu do objektu již nemusí zabývat. Systém lze dálkově odstřežit zasláním SMS zprávy na mobilní telefon EZS ve tvaru:

ODKODOVAT

Aby kdokoli nemohl zneužít dálkového odstřežení ve svůj prospěch, ústředna akceptuje pouze ty pokyny, které jsou zadávány z čísel oprávněných osob, jež jsou uložené v paměti mikrokontroléru. Také vzniká riziko odcizení mobilního telefonu oprávněné osoby, kterým by pachatel mohl zabezpečovací systém odstřežit. Pro tento případ je v systému implementována funkce pro vypnutí dálkového ovládání pomocí textové zprávy. V případě odcizení mobilního telefonu, z jehož čísla jsou příkazy zabezpečovacím systémem akceptovány, má oprávněná osoba možnost deaktivovat dálkové ovládání systému. Deaktivační textovou zprávu lze zaslat z jakéhokoli telefonního čísla. Systém pak neakceptuje příkazy odstřežení nebo zastřežení z žádného telefonního čísla. Zpětnou aktivaci dálkového ovládání systému lze provést pouze prostřednictvím klávesnice systému, pomocí které lze také ze seznamu oprávněných telefonních čísel odcizené číslo odstranit. Deaktivační textová zpráva musí být odeslána na mobilní telefon zabezpečovacího systému ve tvaru:

BLOKOVAT

Je-li dálkové ovládání systému blokováno a oprávněná osoba zašle požadavek k odstřežení systému, pak systém tento požadavek neakceptuje a odesílá osobě informační SMS zprávu ve tvaru:

Zadost byla zamitnuta.
Dalkove ovladani je zablokovano.

10.1.3 Hlášení o stavu EZS

Oprávněné osoby si mohou vyžádat informaci o stavu EZS. Zabezpečovací systém zpětně zasílá textovou zprávu s informací o stavu zabezpečení, tedy je-li aktivní či nikoli, a o stavu dálkového ovládání, je-li povoleno či zakázáno. Tyto informace uživatel využije např. v případech, kdy si není jist, zda při odchodu z objektu zastřežení aktivoval. Žádost o zaslání informací o stavu sytému je podávána formou textové zprávy, kterou oprávněná osoba zašle na mobilní telefon zabezpečovacího systému. Zpráva musí být zadána ve tvaru:

STAV?

Zabezpečovací systém obratem odesílá zpět informační textovou zprávu, která má tvar např.:

Stav: ZAKODOVANO,
Dalkove ovladani: ZAPNUTO

nebo také:

Stav: ODKODOVANO,
Dalkove ovladani: VYPNUTO

a jiné kombinace.

11. SOFTWAROVÉ VYBAVENÍ MODELU EZS

Řidící software mikrokontroléru je napsán v programovacím jazyce C. Výstupem překladu je HEX soubor, v němž je řidící program zakódován. HEX soubor je určen pro naprogramování mikrokontroléru, který dokáže formát souboru zpracovat.

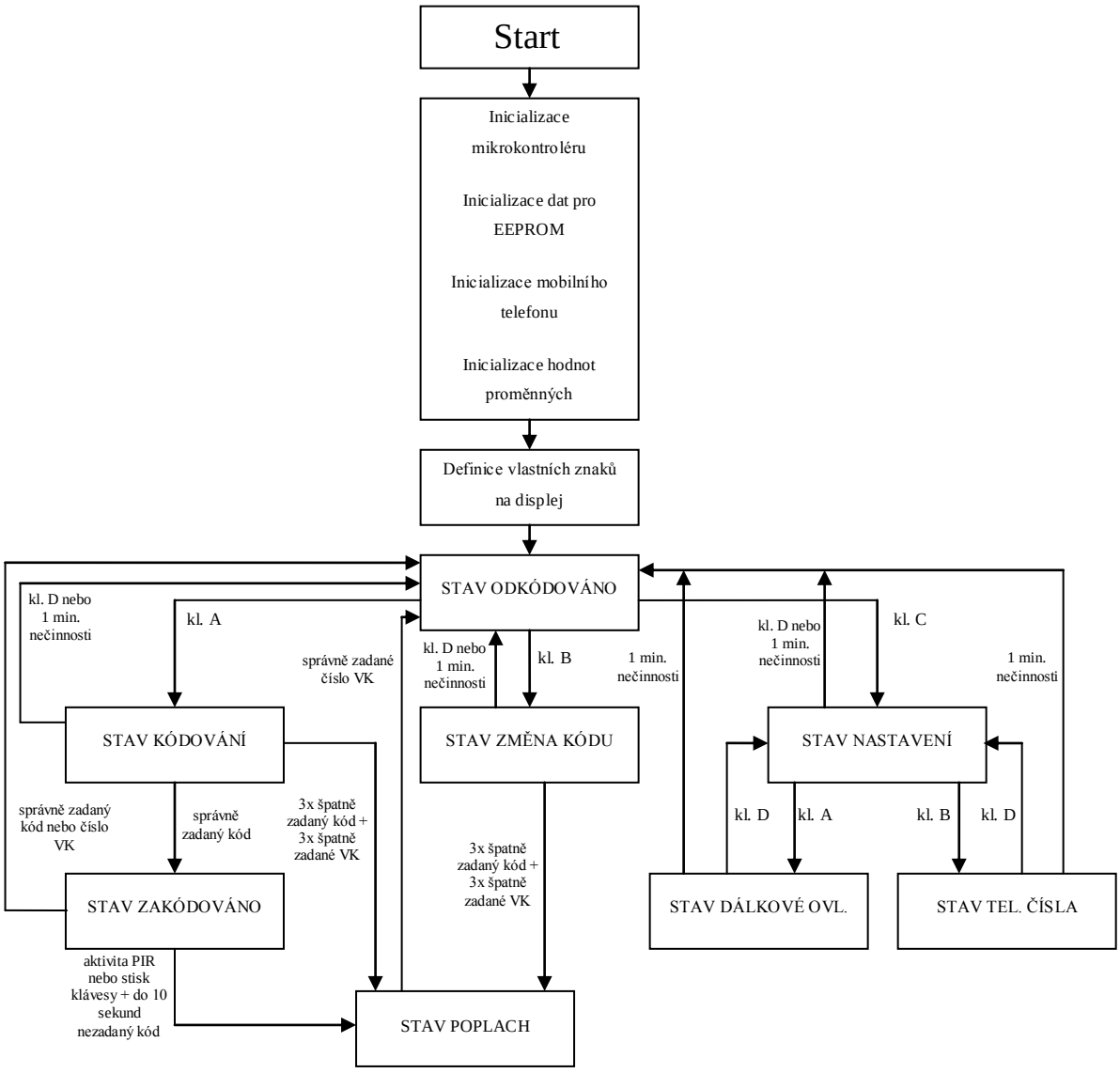
Hlavní část programu (main) zajišťuje inicializaci mikrokontroléru a počáteční nastavení mobilního telefonu. Poté obsluhuje přechody mezi jednotlivými stavy systému. Systém pracuje v osmi stavech: Odkódováno, Kódování, Zakódováno, Změna kódu, Nastavení, Dálkové ovládání, Tel. čísla a Poplach.

Software využívá vnitřní paměti EEPROM mikrokontroléru pro uložení uživatelského kódu, oprávněných telefonních čísel a nastavení dálkového ovládání. Paměť EEPROM uchovává tato data i v případě náhlého odpojení napájení systému. Přerušení od časovače 0 zajišťuje nezávislé počítání doby pro periodické prohledávání paměti SMS zpráv v mobilním telefonu, odpočet doby pro zadání kódu, pro odesílání poplachových SMS, pro kontrolu komunikace s mobilním telefonem a odpočet doby pro vypnutí sirény. Sériová linka je využita ke komunikaci s mobilním telefonem.

Řídící program je uložen v 18 souborech:

EZS(main).c	obsahuje hlavní část programu
displej.c	obsahuje funkce pro obsluhu LCD displeje
klavesnice.c	obsahuje funkce pro čtení kláves z klávesnice
compare.c	obsahuje funkce pro porovnání obsahu polí
casinterrupt.c	obsahuje obsluhu přerušení od časovače 0
usart.c	obsahuje obsluhu sériové linky
init.c	obsahuje funkce s inicializačními nastaveními parametrů mikrokontroléru a mobilního telefonu
sms.c	obsahuje funkce pro práci s SMS zprávami v mobilním telefonu

zadat.c	obsahuje funkce pro čtení kódu, čísla VK a 9-ti místného čísla (telefonní číslo) z klávesnice
spravatc.c	obsahuje funkci pro správu telefonních čísel
infozpravy.c	obsahuje funkce pro zobrazení informačních zpráv na displej
obsluhapir.c	obsahuje funkci pro obsluhu PIR detektorů
waiting.c	obsahuje funkce časové smyčky
mega16.h	obsahuje makra a definuje přístupy k registrům, slouží pro usnadnění práce s ATmega16
stdio.h, stdio.lib	obsahuje funkce pro standardní vstup a standardní výstup
string.h, string.lib	obsahuje funkce pro práci s řetězci



Obrázek 50: Stavový diagram hlavní funkce main

11.1 POPIS ČINNOSTI JEDNOTLIVÝCH STAVŮ

Mezi jednotlivými stavy systém přechází v závislosti na vnějších situacích (stisk klávesy, zadání kódu, detekce pohybu, vyvolání změny kódu, časové závislosti apod.).

11.1.1Stav Odkódováno

V tomto stavu se systém nachází po uvedení do provozu. Zabezpečení je deaktivováno, svítí zelená LED dioda a na displeji se po krátkém čase střídají tři texty. První text informuje o stavu, ve kterém se systém nachází:

ZABEZPECENI JE
VYPNUTO

Druhým textem je první část legendy, jež napovídá, kterými tlačítky se lze přepnou do jiného stavu:

[A] ZAPNOUT
[B] ZMENIT KOD

Třetím textem je druhá část legendy:

[B] ZMENIT KOD
[C] NASTAVENI

Před každým zobrazením prvního informačního textu je prohledána paměť mobilního telefonu. V případě nalezení nové nepřečtené SMS zprávy je zpráva vyhodnocena a vyřízena. Dálkově lze zjistit stav systému nebo je možné systém dálkově blokovat. Pokud selže spojení mezi mikrokontrolérem a mobilním telefonem, na displeji se objeví upozornění s pokyny k odstranění problému:

UPOZORNENI

rotace textu

CHYBA KOMUNIKACE S MOBILNIM TELEFONEM. VYPNETE A ZAPNETE TELEFON A PROVEDTE RESET SYSTEMU.

Dokud není problém odstraněn, nelze systém využívat.

Ve stavu Odkódováno jsou funkční všechna tlačítka z klávesnice. Stiskem tlačítka A se systém dostává do stavu Kódování, stiskem tlačítka B se systém dostává do stavu Změna kódu a stiskem tlačítka C se systém dostává do stavu Nastavení. Stiskem ostatních tlačítek lze aktivovat osvětlení displeje pro jeho lepší čitelnost v temných objektech. Osvětlení displeje po krátkém čase automaticky zhasne.

11.1.2 Stav Kódování

Systém je připraven přijmout čtyř místný uživatelský kód. Svítí zelená LED dioda, displej je osvětlen a zobrazuje text:

ZADEJTE KOD
[ ]

Aktivními klávesami jsou číselná tlačítka, kterými je zadáván kód do systému, a klávesa D, který kdekoli v menu systému funguje jako tlačítko ZPĚT. Stiskem klávesy D v tomto stavu se systém dostává zpět do stavu Odkódováno. Pokud zůstane systém v tomto stavu nečinný po dobu 1 minuty (není proveden stisk tlačítek), přechází automaticky do stavu Odkódováno. Při zadávání kódu jsou jednotlivá čísla zastoupena hvězdičkami, které se zobrazují na displeji mezi hranatými závorkami, např. jsou-li zadána 2 čísla z kódu, displej zobrazuje:

ZADEJTE KOD
[**]

Zadá-li uživatel správný kód, pak zelená LED dioda zhasne a systém začne odpočítávat 10 sekund, což je čas vyhrazený pro opuštění místnosti. Odpočítávání doprovází pípání bzučáku a blikání červené LED diody. Po uplynutí 10 sekund systém před přechodem do stavu Zakódováno kontroluje aktivitu hlavního PIR detektoru. Pokud nepodává informaci o registraci pohybu, systém okamžitě přechází od stavu Zakódováno. Pokud je ovšem detektor aktivní, systém čeká na jeho

deaktivaci, poté přechází do stavu Zakódováno. Při čekání na deaktivaci hlavního PIR detektoru je na displeji zobrazen text:

DEAKTIVACE
DETEKTORU

Pozn.: *Pokud totiž PIR detektor registruje pohyb, podává informaci o registraci celých 5 sekund, poté opět začne monitorovat prostor. Může se stát, že při opouštění místnosti po zadání kódu zaregistruje detektor pohyb ještě v 9. sekundě odpočtu. Protože detektor podává informaci o pohybu po dobu 5 sekund, pak po vypršení odpočtu 10 sekund je detektor stále aktivní. Aktivitu detektoru ve stavu Zakódováno systém vyhodnocuje jako neoprávněný pohyb. Proto systém před přechodem do stavu Zakódováno čeká na deaktivaci detektoru (tj. stav detektoru, kdy přestane podávat informaci o registraci pohybu).*

Nepodaří-li se ovšem uživateli při zadávání kódu zadat kód správně, displej zobrazí text:

NESPRAVNY KOD

K zadání kódu jsou vyhrazeny celkem tři pokusy. Pokud ani při třetím pokusu nezadá uživatel správný kód, k zelené LED diodě se rozsvítí červená LED dioda a uživatel je vyzván k zadání čísla VK (výrobní kód), který je dán od výroby a je neměnný. Na displeji se objeví text:

ZADEJTE CISLO VK
[ ]

Aktivními klávesami jsou pouze číselné klávesy, kterými lze zadat číslo VK (nefunguje klávesa D – zpět). Není také aktivní počítání doby nečinnosti systému (zmíněná 1 minuta), systém nepřechází do stavu Odkódováno, dokud není zadáno správné číslo VK. Každých 10 sekund je prohledávána paměť SMS zpráv mobilního telefonu. Pokud je nalezena nová nepřečtená SMS, systém ji vyhodnotí a vyřídí.

SMS zprávou si lze vyžádat zaslání informace o stavu systému nebo lze blokovat dálkové ovládání.

K zadání čísla VK jsou opět vyhrazeny tři pokusy. Po správném zadání VK se systém vrací do stavu Odkódováno. O špatně zadaném VK informuje displej textem:

NESPRAVNE
CISLO VK

Nepodaří-li se osobě ani při třetím pokusu zadat správné číslo VK, systém předpokládá, že je ovládán neoprávněnou osobou, zhasne zelenou LED diodu a přejde do stavu Poplach.

11.1.3 Stav Zakódováno

V tomto stavu je objekt střežen proti neoprávněnému vniknutí. Svítí pouze červená LED dioda, displej není osvětlen. Displej zobrazuje text:

ZABEZPECENI JE
ZAPNUTO [ ]

Jsou aktivní pouze číselné klávesy, pomocí kterých může příchozí osoba zadáním kódu systém deaktivovat. Každých 10 sekund je prohledáván paměťový prostor SMS zpráv mobilního telefonu. Nalezené nepřečtené zprávy jsou vyhodnoceny a vyřízeny. Dálkově lze systém odkódovat, v tom případě systém přechází okamžitě do stavu Odkódováno. Lze také dálkově zjistit stav systému nebo je možné dálkové ovládání blokovat.

Vejde-li osoba do místnosti, hlavní detektor registruje její pohyb. Na registraci pohybu upozorňuje krátká zvuková signalizace bzučáku. Současně se rozsvítí displej a poté je zahájen odpočet 10 sekund, což je čas vyhrazený pro zadání uživatelského kódu, kterým lze systém deaktivovat. Po správném zadání kódu systém přechází do stavu Odkódováno, při chybném zadání kódu informuje displej textem:

NESPRAVNY KOD

Pokud se osobě nepodaří zadat kód do 10 sekund od příchodu, systém přechází do stavu Poplach.

Může se stát, že hlavní detektor selže a nezaregistruje pohyb osoby, která vešla do místnosti. I v tomto případě je možné zadat uživatelský kód. Displej se rozsvítí po zadání prvního čísla z kódu. Z faktu, že k zadávání kódu došlo dříve, než hlavní detektor zaregistroval pohyb, systém rozpozná, že detektor selhal. O selhání detektoru informuje poté, co uživatel zadá správný kód a systém přejde do stavu Odkódováno. Těsně po přechodu do tohoto stavu displej bliká a zobrazuje text:

POZOR!!!! DETEKTOR
NEZACHYTIL POHYB

Systém takto doporučuje provést revizi hlavního PIR detektoru pohybu. Informaci o selhání detektoru lze z displeje smazat libovolnou klávesou, systém pak pokračuje v činnosti odpovídající stavu Odkódováno.

Do systému lze zapojit až 3 přídavné PIR detektory pohybu pro hlídání dalších místností. Nachází-li se systém ve stavu Zakódováno a zaregistruje-li některý z těchto přídavných detektorů pohyb, systém okamžitě přechází do stavu Poplach.

Všechny PIR detektory pohybu jsou vybaveny tlačítkem, které monitoruje, zda je sejmut kryt detektoru. Je-li z kteréhokoli detektoru odstraněn kryt ve stavu Zakódováno, systém opět okamžitě přechází do stavu Poplach.

11.1.4 Stav Změna kódu

Systém je připraven na změnu čtyřmístného uživatelského kódu. Svítí zelená LED dioda a podsvícení displeje je zapnuto. Aktivními tlačítky jsou číselné klávesy pro zadání kódu a klávesa D, která systém vrací zpět do stavu Odkódováno. Pokud zůstane systém v tomto stavu nečinný po dobu 1 minuty (není proveden stisk tlačítek), přechází automaticky do stavu Odkódováno.

Displej zobrazuje text:

ZADEJTE STARY
KOD [ ]

Uživatel je vyzván k zadání stávajícího platného kódu, který chce změnit. Pro zadání kódu má opět tři pokusy. Podaří-li se uživateli zadat kód třikrát špatně, nastává stejná situace jako v případě třikrát špatně zadaného kódu ve stavu Kódování (tj. vyžádání čísla VK).

Zadá-li uživatel správný starý kód, na displeji se zobrazí text:

ZADEJTE NOVY
KOD [ ]

Nyní může uživatel zadat nový kód, který chce využívat pro zastřežení a odstřežení objektu. Po zadání kódu je uživatel vyzván k zopakování kódu. Tím je systém schopen ověřit, zda se uživatel při zadání nového kódu nespletl. Je totiž málo pravděpodobné, že by uživatel provedl neúmyslně dvakrát stejnou chybu. Na displeji se objeví text:

OPAKUJTE NOVY
KOD [ ]

Pokud se oba kódy shodují, pak je nový kód uložen do paměti EEPROM, o čemž informuje displej textem:

NOVY KOD
ULOZEN

Po uložení nového kódu systém přechází do stavu Odkódováno. Pokud se ovšem nový kód s kontrolním kódem neshoduje, displej upozorní textem:

KODY
NESOUHLASI

Poté je uživatel znovu vyzván k zadání nového a kontrolního kódu.

Pokud je systém nečinný po dobu 1 minuty (není stisknuta žádná klávesa), přechází automaticky do stavu Odkódováno.

11.1.5 Stav Nastavení

Tento stav obsluhuje pouze menu nastavení systému. Svítí zelená LED dioda a podsvícení displeje je zapnuto. Aktivními klávesami jsou pouze klávesy A a B, které slouží k výběru položek v menu nastavení, a klávesa D, jejímž stiskem systém přechází zpět do stavu Odkódováno. Pokud je systém nečinný po dobu 1 minuty (není stisknuta žádná klávesa), přechází automaticky do stavu Odkódováno. V tomto stavu je na displeji zobrazen text:

[A] DALKOVE OVL.
[B] TEL. CISLA

Stiskem klávesy A se systém dostává do stavu Dálkové ovládání, stiskem klávesy B se systém dostává do stavu Tel. čísla.

11.1.6 Stav Dálkové ovládání

Tento stav slouží k vypnutí nebo zapnutí dálkového ovládání zabezpečovacího systému. Svítí zelená LED dioda a displej je osvětlen. Aktivními klávesami je klávesa A, která zapíná nebo vypíná dálkové ovládání, a klávesa D, která vrací systém o krok zpět, tedy do stavu Nastavení. Pokud je systém nečinný po dobu 1 minuty (není stisknuta žádná klávesa), přechází automaticky do stavu Odkódováno. Na displeji je zobrazen stav dálkového ovládání a aktivní klávesa. Pokud je možnost dálkového ovládání vypnuta, na displeji je zobrazen text:

STAV: VYPNUTO
[A] ZAPNOUT

V případě, že je dálkové ovládání zapnuto, je na displeji zobrazen text:

STAV: ZAPNUTO
[A] VYPNOUT

Stiskem klávesy A lze změnit stav dálkového ovládání. Po stisku klávesy A je na displeji krátce zobrazen aktuální (nový) stav dálkového ovládání. V případě, že došlo stiskem klávesy A k zapnutí dálkového ovládání, na displeji se objeví text:

STAV: ZAPNUTO

V opačném případě došlo-li stiskem klávesy A k vypnutí dálkového ovládání, displej zobrazí text:

STAV: VYPNUTO

Nový stav dálkového nastavení je uložen do EEPROM paměti mikrokontroléru. Poté systém přechází zpět do stavu Nastavení.

11.1.7 Stav Tel. čísla

Tento stav slouží pro správu oprávněných telefonních čísel (vložení, editace, odstranění). Svítí zelená LED dioda a displej je osvětlen. Pokud je systém nečinný po dobu 1 minuty (není stisknuta žádná klávesa), přechází automaticky do stavu Odkódováno. Proces správy telefonních čísel prochází třemi body:

1) výběr množiny čísel (čísla pro poplach nebo čísla pro dálkové ovládání)
2) prohlížení seznamu čísel
3) editace čísel

Stiskem klávesy D systém přechází mezi body nazpět, tedy z bodu 3 přechází do bodu 2, z bodu 2 do bodu 1 a z bodu 1 systém přechází zpět do stavu Nastavení.

Bezprostředně po vstupu do stavu Tel. čísla je na displeji zobrazen text:

[A] POPLACH
[B] DALKOVE OVL.

Stiskem klávesy A je vybrána množina poplachových telefonních čísel k zobrazení. Stiskem klávesy B je vybrána množina telefonních čísel pro dálkové

ovládání. Po stisku klávesy A nebo B přechází stav Tel. čísla do bodu 2 a na displeji jsou zobrazena čísla konkrétní množiny, např.:

TEL1: 777123456
[A] ZMENIT [B] ↓

Stiskem klávesy B lze zobrazovat následující telefonní čísla uložená v paměti (v množině poplachových telefonních čísel mohou být uložena maximálně 3 čísla, v množině telefonních čísel pro dálkové ovládání může být uloženo až 9 telefonních čísel). V prohlížení telefonních čísel je zajištěna kruhová rotace zobrazení. Je-li zobrazeno poslední telefonní číslo v množině, stisk klávesy B zobrazí opět první číslo v množině.

Zobrazuje-li například displej telefonní číslo uložené na první pozici v paměti, pak po dvou stiscích klávesy B je na displeji zobrazeno třetí číslo v paměti:

TEL3: 737556677
[A] ZMENIT [B] ↓

Pokud není na konkrétní pozici uloženo číslo, displej zobrazuje:

TEL3: NEZADANO
[A] ZMENIT [B] ↓

Stiskem klávesy A přechází stav Tel. čísla do bodu 3. V tomto bodu je možné čísla zadat, smazat nebo editovat. Je-li na displeji zobrazeno telefonní číslo uložené na první pozici v paměti, pak stiskem klávesy A systém přechází k jeho editaci. Na displeji je zobrazeno:

TEL1: _
[A] ULOZIT

Stiskem klávesy A je provedeno uložení „prázdného čísla“, tedy původní číslo je smazáno a na jeho pozici se objeví text NEZADANO. Pokud uživatel nechce

číslo smazat, ale editovat, zadává číslo přímo z číselné klávesnice. Po zadání např. tří čísel displej zobrazuje:

TEL1: 732_

[B] ←

Klávesou B lze provést korektury zadávaného čísla, tedy smazat konkrétní pozice čísla při jejich špatném zadání a zadat je znovu správně. Po zadání devíti čísel je na displeji zobrazeno:

TEL1: 732717828

[A] ULOZIT [B] ←

Stiskem klávesy A lze nové telefonní číslo uložit. Systém poté přechází do bodu 2 (prohlížení množiny čísel). Čísla se při ukládání automaticky řadí na nejnižší volnou pozici v paměti. Je-li například číslo zadáváno na 8. pozici v paměti, ovšem nejnižší volná pozice v paměti je pozice 5, pak je zadávané číslo automaticky uloženo na 5. pozici v paměti. Také v případě mazání telefonních čísel je využito automatického řazení. Je-li například smazáno číslo na 2. pozici, pak se automaticky čísla z vyšších pozic přesouvají o pozici níže, aby nevznikla mezera v paměti po vymazání čísla z 2. pozice.

11.1.8 Stav Poplach

Ihned po přechodu do tohoto stavu se rozezvučí siréna a vyšle se log. 1 na výstup sloužící pro napojení přídavného výstupního zařízení. Svítí červená LED dioda. Systém odpočítává maximální dobu poplachu (5 minut), po kterou je siréna v provozu, nedojde-li k deaktivaci poplachu prostřednictvím klávesnice. S periodou 30 sekund jsou odesílány poplachové SMS na telefonní čísla v paměti EEPROM mikrokontroléru. Zároveň je prohledávána paměť SMS zpráv v telefonu. V případě nalezení nové nepřečtené SMS zprávy je zpráva vyhodnocena a vyřízena. Pokud je na mobilní telefon přijata zpráva ve tvaru OK (potvrzovací SMS), která byla odeslána z telefonního čísla, na které byla zaslána poplachová SMS, je odesílání

dalších poplachových SMS ukončeno. Pokud ovšem po třech odeslaných poplachových SMS nepřijde na mobilní telefon EZS do 30 sekund potvrzovací zpráva ve tvaru OK, systém vytáčí telefonní číslo uložené na první pozici v paměti EEPROM.

V tomto stavu jsou aktivní pouze číselné klávesy. Uživatel může poplach deaktivovat zadáním čísla VK, k čemuž jej vyzývá text na displeji:

ZADEJTE CISLO VK
[ ]

Pro zadání čísla VK má uživatel neomezený počet pokusů. Po správném zadání VK je poplach deaktivován a systém přechází do stavu Odkódováno. Je-li zadáno špatné číslo VK, displej uživatele upozorní textem:

NESPRAVNE
CISLO VK

Poté je uživatel znovu vyzván k zadání čísla VK. Nepodaří-li se uživateli VK zadat do 5 minut, siréna se automaticky deaktivuje, ovšem systém i nadále požaduje zadání čísla VK. Až po správném zadání VK se systém dostává do stavu Odkódováno.

Je-li siréna deaktivována vypršením maximální doby (5 minut), uživatel, který přijde do objektu později, musí být informován, že k poplachu došlo. Tuto informaci může uživatel odvodit z faktu, že systém po něm požaduje číslo VK místo uživatelského kódu. Systém však upozorní uživatele také prostřednictvím LCD displeje. Displej informuje o deaktivované siréně poté, co uživatel zadá číslo VK a systém přejde do stavu Odkódováno. Těsně po přechodu do tohoto stavu displej bliká a zobrazuje text:

SYSTEM BYL
V POPLACHU

Informaci o poplachu lze z displeje smazat libovolnou klávesou, systém pak pokračuje v činnosti odpovídající stavu Odkódováno.

12. ZÁVĚR

Problematika elektronických zabezpečovacích systémů je dnes široce rozvíjející se perspektivní obor. Stále se projektují nové metody zabezpečení a vyvíjejí se nové zabezpečovací prvky. O zabezpečení elektronickým zabezpečovacím systémem je stále větší exponenciálně rostoucí zájem.

V předložené práci je proveden návrh mikroprocesorového systému včetně příslušného softwarového vybavení, který slouží jako řidící jednotka elektronického zabezpečovacího systému, kterým lze zabezpečit menší objekt proti neoprávněnému vniknutí osob. Řidící jednotka byla realizována na navržené desce plošného spoje, oživena a prakticky odzkoušena s příslušnými čidly. Byla ověřena funkčnost softwarového vybavení.

Navržený systém elektronického zabezpečení dokáže zabezpečit průměrně veliký byt s jedním vchodem. Systém lze ovládat prostřednictvím 16 tlačítkové klávesnice a pro vizuální kontrolu chování systému slouží podsvícený LCD displej. K rychlé orientaci ve stavech systému a pro poskytování zpětné vazby uživateli je systém vybaven světelnou a zvukovou signalizací v podobě červené a zelené LED diody a bzučáku. Detekci neoprávněného vniknutí do objektu zjišťuje infračervený detektor pohybu PIR, který snímá střežený prostor v okolí hlavního vchodu do objektu. Poplach je hlášen interiérovou sirénou v rámci vnitřního prostoru objektu. Jejím úkolem je znepříjemnit pachateli pobyt uvnitř objektu. Efektivnější hlášení poplachu zajišťuje mobilní telefon připojený k ústředně zabezpečovacího systému, který hlásí poplach na dálku zasíláním poplachových SMS zpráv majiteli, případně dalším osobám. Majitel (popřípadě jiné informované osoby) se mohou postarat o zajištění objektu např. povoláním orgánu bezpečnosti nebo osobně. Mobilní telefon je kromě hlášení poplachu využit také k dálkovému odstřežení systému nebo zjištění aktuálního stavu systému (zakódováno/odkódováno). Komunikace mezi uživatelem a zabezpečovacím systémem probíhá prostřednictvím krátkých textových zpráv SMS.

Výhodou předloženého modelu elektronického zabezpečovacího systému je jednoduchost jeho struktury a zapojení. I méně zkušený elektrotechnik by byl schopen s přiloženým návodem, deskou plošných spojů a součástkami, mezi kterými

by nechyběl naprogramovaný mikrokontrolér, model sestavit. Zkušenější elektrotechnik může využít programování mikrokontroléru přímo v aplikaci a může si tímto dotvořit řídící program dle svých představ. Celková cena všech součástí modelu by neměla převýšit částku 2000,- Kč.

Potenciál mobilní komunikace je stále více využíván například v oblasti moderního řízení inteligentních budov, kde je dálková komunikace využita např. k přímému nastavení vytápění, k odemčení vstupních vrat a k jiným přípravám objektu před vstupem uživatele. Menšími úpravami SW a HW stávajícího modelu zabezpečovacího systému a rozšířením o větší řídící jednotku by ústředna modelu byla také schopna dálkově řídit některé technické prvky budovy. Již by se ovšem nejednalo o ústřednu zabezpečovacího systému, ale o komplexní řídící jednotku objektu.

13. POUŽITÁ LITERATURA

[1] ULBRICH, J. *Zabezpečovací systém s mikrokontrolérem řady ATmega*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2007. 67 s. Vedoucí bakalářské práce Ing. Tomáš Macho, Ph.D.

[2] FLAJZAR, T. *GSM alarm – přenos poplachu na mobilní telefon*. Praha: BEN – technická literatura, 2005. 84 s. ISBN 80-7300-183-7.

[3] KREJČIŘÍK, A. *SMS – Střežení a ovládání objektů pomocí mobilu a SMS*. Praha: BEN – technická literatura, 2004. 304 s. ISBN 80-7300-082-2.

[4] VÁŇA,V. *Mikrokontroléry Atmel AVR – popis procesorů a instrukční soubor*. Praha: BEN – technická literatura, 2003. 335 s. ISBN 80-7300-083-0.

[5] KUCHAŘ, Jan. *Ochranu objektu je třeba svěřit odborné firmě! – Diskrétní a účinná ochrana majetku* [online]. 2003. Dostupné z: ⟨http://si.vega.cz/clanky/elektroinstalace/ochranu-objektu-je-treba-sverit-odborne-firme-dis/⟩.

[6] *Systém EZS – Elektronické zabezpečovací systémy* [online]. Elektronis, 2004. Dostupné z: ⟨http://www.elektronis.cz/system-ezs.html⟩.

[7] *Elektronické zabezpečení budov* [online]. Elreko, 2006. Dostupné z: ⟨http://www.elreko.cz/index.php?pg=sub&co=4⟩.

[8] *Zabezpečovací systémy – EZS* [online]. Šveva, s r.o., 2006. Dostupné z: ⟨http://www.sveva.znojemsko.com/?cap=4573⟩.

[9] *Zabezpečovací systémy* [online]. Elektro Vilímec, 2006. Dostupné z: ⟨http://www.vilimec.cz/index.php?action=menu&menu_id=27⟩.

[10] *Komponenty EZS systémy* [online]. Inels. Dostupné z: ⟨http://www.inels.cz/index.php?sekce=produkty&akce=show&id=88⟩.

[11] *EZS – elektrická zabezpečovací signalizace* [online]. Genova, 2007. Dostupné z: ⟨http://www.genova.cz/ezs-elektricka-zabezpecovaci-signalizace/⟩.

[12] *Poradna* [online]. Acces. Dostupné z: ⟨http://www.acces.cz/acces/poradna/⟩.

[13] *Bezpečně bezpečný dům* [online]. Časopis Mozaika, 2002. Dostupné z: ⟨http://www.cmss.cz/_templ/bydleni/mozaika/02_2/36.htm⟩.

[14] VOJÁČEK, Antonín. *Detektory kouře – princip & IO Freescale* [online]. 2006. Dostupné z: ⟨http://automatizace.hw.cz/mereni-a-regulace/ART274-detektory-koure--princip-%2526-io-freescale.html⟩.

[15] *Znakové LCD displeje – procesory PIC* [online]. Doveda Boys, 2006. Dostupné z: ⟨http://www.cmail.cz/doveda/lcd/⟩.

[16] *Ultrazvukový detektor pohybu CA-530 (zboží)* [online]. Dobrý-obchod.cz. Dostupné z: ⟨http://www.dobry-obchod.cz/produkt/detail/autoalarmy/34-prislusenstvi-pro-autoalarmy/ca530ja-ultrazvukovy-detektor-pohybu-ca-530/⟩.

[17] *Mikrovlnný senzor vnitřní/vnější (zboží)* [online]. 9000 - senzory. Dostupné z: ⟨http://www.9000.cz/senzory/mikrovlnny-senzor-vnitrni-vnejsi⟩.

[18] *Telefon Siemens C35 (zboží)* [online]. DH servis. Dostupné z: ⟨http://obchod.dhservis.cz/index.php?main_page=product_info&cPath=82&products_id=339⟩.

[19] *GSM komunikátor SIP300 modul* [online]. Flajzar, s.r.o. Dostupné z: ⟨http://www.flajzar.cz/detail.php?zbozi=2547&cat=500&open=&z=galerie⟩.

[20] *GPRS net module* [online]. Beijer electronics. Dostupné z: ⟨http://www.brodersen.se/products/modem/gprs/gprs.htm⟩.

[21] *F-KV16KEY maticová klávesnice (zboží)* [online]. GM electronic. Dostupné z: ⟨http://www.gme.cz/cz/index.php?product=637-091⟩.

[22] *F-PDS-901A PIR detektor (zboží)* [online]. GM electronic. Dostupné z: ⟨http://www.gme.cz/cz/index.php?product=754-183⟩.

[23] *KPE-1500 siréna (zboží)* [online]. GM electronic. Dostupné z: ⟨http://www.gme.cz/cz/index.php?product=640-060⟩.

[24] *Siemens C35, Siemens mobile phone system* [online]. AMK Goldnet. Dostupné z: ⟨http://www.amkgoldnet.com.my/prodsc.asp?prodid=123⟩.

[25] BURDA, Pavel. *Komunikace s mobilem přes sériový port pomocí AT příkazů* [online]. P.E.S. consulting, s.r.o., PC Svět. 2002. Dostupné z: ⟨http://www.pcsvet.cz/art/article.php?id=2291⟩.

[26] Hankovec, David. *Alarm s přenosem poplachu po síti GSM* [online]. DH servis. Dostupné z: ⟨http://www.dhservis.cz/dalsi/alarm.htm⟩.

[27] Hankovec, David. *AT příkazy mobilních telefonů* [online]. DH servis. Dostupné z: ⟨http://www.dhservis.cz/dalsi/at_prikazy.htm#sms⟩.

[28] Strolený, J. *AT příkazy telefonu Siemens C 25* [online]. Doveda Boys, 2002. Dostupné z: ⟨ http://www.cmail.cz/doveda/gsm/at_c25.htm ⟩.

[29] Admíra, M. *Mobilní telefony – rady programátorům* [online]. 2006. Dostupné z: ⟨http://www.adamira.cz/radypgmmobil/⟩.

[30] Matuška, J. *Jak na SMS v PERLu* [online]. 2008. Dostupné z: ⟨http://walda.starhill.org/pocitace-perl2sms.html⟩.

[31] Klaška, L. (hlavní redaktor). *Svět sítí – slovníček pojmů a zkratek - P* [online]. Infinity a.s. Dostupné z: ⟨http://www.svetsiti.cz/slovnik.asp?Chr=P⟩.

[32] Strolený, J. *PDU protokol* [online]. Doveda Boys, 2004. Dostupné z: ⟨http://www.cmail.cz/doveda/gsm/pdu_sms.htm#type_adress⟩.

[33] Nezval, M. *SMS a PDU formát (Protocol Description Unit)* [online]. BraMo, 2003. Dostupné z: ⟨http://bramo.ic.cz/sms.htm⟩.

[34] Hankovec, D. *Vytvoření PDU formátu SMS zprávy jednočipem a odeslání mobilním telefonem* [online]. DH servis. Dostupné z: ⟨http://www.dhservis.cz/dalsi/construction_pdu.htm⟩.

[35] *What is a Zener Diode* [online]. ERT – Electronics + Radio Today. Dostupné z: ⟨http://www.electronics-radio.com/articles/electronic_components/diode/zener-diode.php⟩.

[36] *Data sheets Atmel AVR ATtiny2313* [online]. Atmel Corporation, 2006. Dostupné z: ⟨http://www.atmel.com/dyn/resources/prod_documents/2543S.pdf⟩.

[37] *Data sheets Atmel AVR ATmega8* [online]. Atmel Corporation, 2006. Dostupné z: ⟨http://www.atmel.com/dyn/resources/prod_documents/2486S.pdf⟩.

[38] *Data sheets Atmel AVR ATmega16* [online]. Atmel Corporation, 2006. Dostupné z: ⟨http://www.atmel.com/dyn/resources/prod_documents/doc2466.pdf⟩.

[39] *Data sheets Atmel AVR ATmega64* [online]. Atmel Corporation, 2006. Dostupné z: ⟨http://www.atmel.com/dyn/resources/prod_documents/2490S.pdf⟩.

[40] *Data sheets KA78XX/KA78XXA 3-Terminal 1A Positive Voltage Regulator* [online]. Fairchild Semiconductor. Dostupné z: ⟨*http://www.tranzistoare.ro/datasheets/228/390068_DS.pdf*⟩.

[41] *Data sheets Low Signal Relay G5V-1* [online]. Omron. Dostupné z: ⟨*http://www.omron.com/ecb/products/pdf/en-g5v1.pdf*⟩.

[42] *Data sheets LCD display MC1602E-SYL/H* [online]. Dostupné z: ⟨*http://postdownload.filefront.com/12506869//6613056241e396d59733ce8d0a13187b014a5217fea6819c3b46ab75088baa60ae0bf2b2b4cc2505*⟩.

[43] *Součástky pro elektroniku 2004.* GM electronic, s r.o., 2004. 537 s.

14. SEZNAM ZKRATEK

AL1	Alarm pin1
AL2	Alarm pin2
ALU	Arithmetic and Logic Unit
ASCII	American Standard Code for Information Interchange
AT	Attention
AVR	Automatic Voltage Regulator
CD	Compact Disc
CGRAM	Character Generator Random Access Memory
CLK	Clock
DIP	Dual Inline Package
DPS	Deska Plošných Spojů
EEPROM	Electrically Erasable Programable Read Only Memory
EZS	Eektronické Zabezpečovací Systémy
GND	Ground
GSM	Global System for Mobile communications
GPRS	General Packet Radio Service
HW	Hardware
JTAG	Joint Test Action Group
kap.	Kapitola
LCD	Liquid Crystal Display
LED	Light Emitting Diode
log.	Logická/Logical
MOSI	Master Outpus, Slave Input
MISO	Master Input, Slave Output
MSB	Most Significant Bit
MT	Mobilní Telefon
OVL.	Ovládání
PCO	Pult Centralizované Ochrany
PDIP	Plastic Dual In-line Package

PDU	Protocol Description Unit
PID	Protocol Identifier
PIR	Passive Infrared
RAM	Random Access Memory
ROM	Read Only Memory
RST	Reset
RxD	Recieve Data
SCK	Serial Clock
SIM	Subscriber Identity Module
SMS	Short Message Systems
SRAM	Static RAM
SW	Software
TA1	Tamper pin1
TA2	Tamper pin2
tel.	Telefonní/telefonního
TxD	Transmit Data
VCC	Common-Collector Voltage
VK	Výrobní Kód

15. OBSAH PŘILOŽENÉHO CD

Na CD se nacházejí tyto adresáře obsahující:

Data sheets	Katalogové listy použitých obvodů (ve formátech pdf)
Dokumentace	Diplomová práce (ve formátu pdf)
DPS	Návrhy desek plošných spojů pro výrobu (vytvořeno v programu Eagle 4.11 ve formátu brd)
Zdrojový kód C	Kód řidícího programu (ve formátech c)
Zdrojový kód HEX	Kód řidícího programu ve formátu pro mikrokontrolér (ve formátu hex)