VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV MIKROELEKTRONIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF MICROELECTRONICS

ZABEZPECOVACÍ SYSTÉM PRO RODINNÝ DUM

SECURITY SYSTEM FOR FAMILY HOUSE

DIPLOMOVÁ PRÁCE

MASTER´S THESIS

AUTOR PRÁCE — Bc. Martin Sohr

AUTHOR

VEDOUCÍ PRÁCE — ING. DAVID JAROŠ

SUPERVISOR

BRNO 2011

Abstrakt:

Práce se zaobírá kompletním teoretickým návrhem bezpečnostního sytému pro rodinný dům od výběrů technologií, zabezpečovacích principů a výběru prvků, teoretický návrh jejich umístění až po praktickou realizaci.

V této práci je navrhnuto zabezpečení vstupních bodů, jako jsou okna a dveře, pomocí magnetických kontaktních čidel a oken pomocí senzorů rozbití skla a zabezpečením prostoru pomocí pohybových senzorů. Dále je v této práci vysvětlen funkční princip použití optických závor jakožto druhotného zabezpečení vnitřního prostoru.

Navržený zabezpečovací systém obsahuje centrální ovládací jednotku, která je schopna předat informace o stavu všech bezpečnostních prvků nadřazenému systému. Pro komunikaci mezi jednotlivými zařízeními bezpečnostního systému je využito bezdrátové komunikační technologie IQRF pracující v bez licenčním pásmu. Pro komunikaci mezi bezpečnostním systémem je využito GSM modulu SIM900.

Klíčová slova:

Rodinný dům, zabezpečovací systém, bezdrátová komunikace, IQRF, centrální řídicí jednotka, SPI, I2C, čidla tříštění skla, pohybové senzory, magnetické kontaktní čidla, grafický dotykový displej, LCD displej, mikrokontroler, SIM900, PIC24FJ256GB106, EA DOGM106, eDIPTFT43-A.

Abstract:

This thesis deals with complete theoretical design of security system for a family house, from the selection of technologies, security principles and selection of elements, theoretical suggestions of their placement to practical realization. I this thesis, securing of entry points, such as doors and windows, is done by magnetic contact sensors. Windows are secured also against breaking of glass. Inner space is secured using motion sensors. Further, the function principle of optical latches as secondary securing element of inner space is explained. The designed security system implements a central control unit, which is able to provide status information on all security elements to the host system. IQRF wireless communication operationg in licence-free is used for communication among elements of the security system. GSM SIM9000 module is used for communication with the security system.

Key Words:

Family house, security system, wireless communication, IQRF, central control unit, SPI, I2C, glass break sensors, motion sensors, magnetic contact sensors, graphic displey, LCD displey, microcontroler, SIM900, 24FJ256GB106, EA DOGM106, eDIPTFT43-A.

Bibliografická citace mé práce:

SOHR, M. *Zabezpečovací systém pro rodinný dům.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 63 s. Vedoucí semestrální práce Ing. David Jaroš.

Prohlášení autora o původnosti díla:

Prohlašuji, že jsem tuto vysokoškolskou kvalifikační práci vypracoval samostatně pod vedením vedoucího diplomové práce, s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury. 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 26. 5. 2011

…….

Bc. Martin Sohr

Poděkování:

Děkuji vedoucímu diplomové práce Ing. Davidu Jarošovi za metodické a cíleně orientované vedení při plnění úkolů realizovaných v návaznosti na diplomovou práci.

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Cílem diplomové práce je vytvořit návrh zabezpečovacího systému rodinného domu a realizovat zabezpečovací systém pro tento dům.

Každý zabezpečovací systém se skládá z řídicí jednotky, která předává informace o stavu připojených bezpečnostních prvků autorizované osobě, na PCO (pult centralizované ochrany) nebo obecnému nadřazenému systému a z bezpečnostních prvků, které kontrolují zabezpečený prostor.

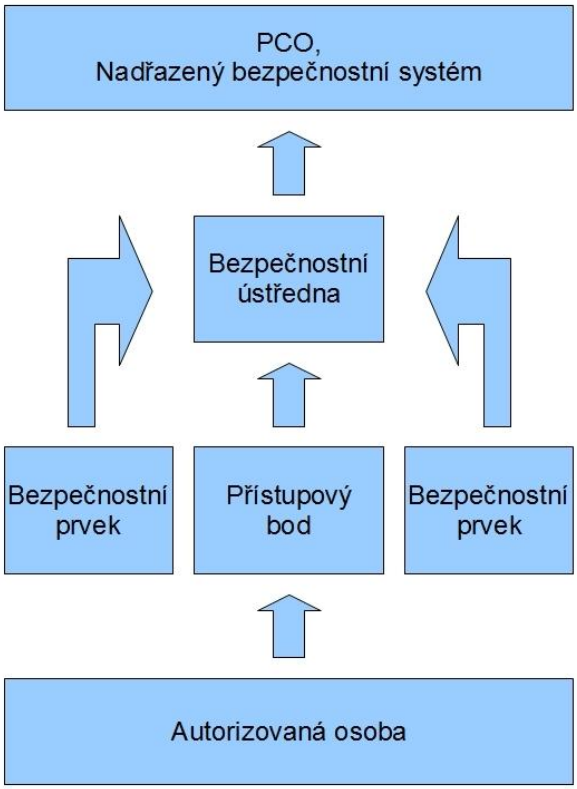
V dnešní době se mezi nejpoužívanější zabezpečovací prvky řadí detektory pohybu, detektory tříštění skla a magnetické kontaktní spínače. Jako podružné zabezpečovací prvky je možno použít mechanická, otřesová a zvuková čidla, optické závory a další. Všechny bezpečnostní prvky bývají k bezpečnostní ústředně připojeny pomocí metalického vedení nebo bezdrátové technologie. Pro bezdrátovou komunikaci bývá výrobcem, v technické dokumentaci výrobku, uveden typ a verze použitého komunikačního protokolu.

V realizované práci získává řídicí jednotka informace o stavu zabezpečení z magnetických kontaktních čidel, detektorů rozbití skla a pohybových senzor které jsou využity pro zabezpečení oken a dveří, detektorů pohybu využitých pro zajištění vnitřního prostoru rodinného domu a dalších možných instalovaných bezpečnostních prvků jako například optických závor. Ke vzájemné komunikaci mezi bezpečnostními prvky a řídicí jednotkou je využito bezdrátové technologie IQRF (Intelligence Quotient Radio Frequency).

2. Teoretický rozbor bezpečnostního systému

Zabezpečovací systém pro rodinný dům by se neměl skládat jen z hlásičů, které reagují až po úspěšném vniknutí do střeženého prostoru. Velmi důležité je u rodinného domu zabezpečení i vnějšího obvodu domu. To znamená, že by se měl poplach spustit již při pokusu o vniknutí.

Bezpečnostní systém by měl reagovat na každého potenciálního pachatele blížícího se k domu a spustit například osvětlení vstupních dveří, aby bylo jasné, že systém na potenciálního pachatele zareagoval, což může mít za následek odrazení pachatele od úmyslu vniknout do objektu. Blokové schéma obecného bezpečnostního systému je zobrazeno na obrázku 1.

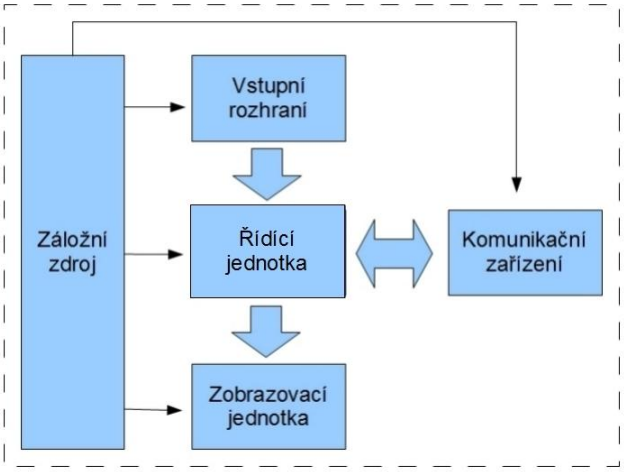


Obr. 1: Blokové schéma obecného bezpečnostního systému

2.1 Řídicí jednotka

Všechny prvky bezpečnostního systému jsou připojeny k centrální řídicí jednotce (CRJ), která vyhodnocuje signály z těchto prvků. Prvky bývají připojeny metalickým nebo bezdrátovým vedením. Řídicí jednotka signalizuje poplach, umožňuje nastavení systému, spouštění a vypínání zabezpečení a umožňuje jeho případnou aktuální kontrolu. Blokové schéma obecné bezpečnostní ústředny je zobrazeno na obrázku 2.

Při signalizaci poplachu dochází ke spuštění akustických a optických zařízení pro upozornění okolí na nestandardní situaci, popřípadě pro přivolání náhodné pomoci, informování autorizované osoby a přivolání bezpečnostních složek.



Obr. 2: Blokové schéma obecné bezpečnostní ústředny

Každá řídicí jednotka obsahuje:

- řídicí jednotku pro ovládání systému,
- zobrazovací jednotku pro kontrolu systému jako například:
  - displej,
  - LED (Light Emitting Diode),
  - obecný zobrazovací prvek,
- vstupní rozhraní pro nastavení systému bývá nejčastěji:
  - klávesnice,
  - dotykový displej,
- komunikační zařízení:
  - GSM (Global System for Mobil Communication),
  - Wi-fi (Wireless Fidelity),
  - Bluetooth,

        - komunikační rozhraní počítačové sítě a další,
    - záložní zdroj pro případ nouzového napájení.

Jakékoli zařízení, které má být řízeno vnějšími signály, musí obsahovat ovládací blok, který tyto signály interpretuje pomocí svého obvodového nebo softwarového vybavení.

Jako řídicí jednotky jsou nejčastěji používány různé typy mikrokontrolérů. Mikrokontrolér je programovatelná polovodičová součástka založena převážně na harvardské architektuře, to znamená, že paměť dat a programu je vzájemně oddělena. Mikrokontrolér přijímá data od připojených zařízení (periférií), zpracovává je podle naprogramovaného softwaru a vzhledem k přijatým datům celý systém ovládá.

2.1.1 Vstupní rozhraní

Vstupní rozhraní poskytuje autorizované osobě kromě možnosti vypnutí a zapnutí bezpečnostního systému i možnost jeho nastavení. U většiny bezpečnostních systémů je možno nastavit:

- heslo k identifikaci autorizované osoby,
- detailnější nastavení komunikačního zařízení,
- časové nastavení jako:
    - automatické kontroly systému,
    - doby preventivního informování autorizované osoby,
    - zpoždění vyhlášení poplachu čidlem zajišťujícím prostor kolem přístupového bodu.

Zpoždění vyhlášení poplachu je nutno nastavit pro minimalizaci planých poplachů z důvodu vypínání a spouštění zabezpečovacího systému.

2.1.2 Komunikační zařízení

Jako komunikační zařízení je použito modulu SIM900 sloužícího jak GSM brána mezi zabezpečovacím systémem a mobilní sítí.

GSM brána je oboustranný převodník pro volání mezi pevnou linkou a mobilním zařízením obsahující modul GSM. Umožňuje připojení digitálního nebo analogového telefonu, telefonní ústředny pomocí přímého spojení nebo sítě LAN (Local Area Network), odeslání a příjem SMS zpráv (Short message service) a zprostředkovává volání.

Připojením GSM modulu je možno velice efektivním způsobem doplnit zabezpečovací systém. Existence GSM modulu připojeného k ústředně umožňuje odposlech hlídaných

prostor a jako doplňkovou službu dálkové ovládání systému zabezpečení například pomocí SMS zpráv nebo pomocí elektronické pošty.[1]

2.2 Přístupový bod

Přístupový bod do systému bývá oddělen od bezpečnostní ústředny a bývá umístěn u vstupu do objektu. Oddělení těchto dvou částí se provádí z důvodu omezení přístupu k ústředně za účelem její ochrany, jako k řídicímu prvku celého zabezpečovacího systému. Přístupový bod bývá tvořen:

- rozhraním pro autentizaci heslem,
- zobrazovacím prvkem pro ověření správnosti hesla, spuštění a vypnutí systému,
- záložním zdrojem pro napájení při výpadku primárního zdroje.

2.3 Bezpečnostní prvky

V dnešní době se nejčastěji pro zajištění prostoru, soukromého vlastnictví a vlastní ochrany využívají tři druhy bezpečnostních čidel:

- detektory pohybu,
- detektory rozbití skla (též označované jako detektory tříštění skla),
- magnetická čidla pro detekci otevření oken nebo dveří.

Výhodou těchto zařízení je jejich

- nízká cena,
- dobrá spolehlivost,
- jednoduchá instalace,
- velká dostupnost.

Společnou nevýhodou detektorů rozbití skla a detektorů pohybu je nutnost napájení napětí těchto čidel. K napájení je možno podle typu čidla využít baterie nebo elektrické rozvodné sítě. U bateriově napájených čidel je nutno brát na zřetel umístění baterie:

- interní
    - jsou součást čidla,
    - používají pouze výrobcem schválené typy a velikosti baterií.
- externí
    - je nutné je připojit pomocí metalického vedení,
    - umožňuje používat libovolný typ a velikost baterií s požadovaným napětím.

Přehled některých snadno dostupných čidel a jejich parametrů je v tabulce 1.

Tab. 1: Přehled některých čidel a jejich parametrů

Název		F-G1010 [14]	MERGE JQ-L [15]	JA-80W [7]
Typ čidla			Infračervené	Mikrovlnné
Typ připojení			Metalické	Bezdrátové
Napájení		230V AC	230V AC	3.6 V DC
Max. zátěž		1200W	300W	
Detekční vzdálenost		12m	7m	12m
Výška instalace			0,75 ÷ 3,00m	2,5m
Úhel detekce	Horizontální	180°	120°	120°
	Vertikální	180°	60°	120°
Aktivační doba	Max		6min	

2.3.1 Detektory pohybu

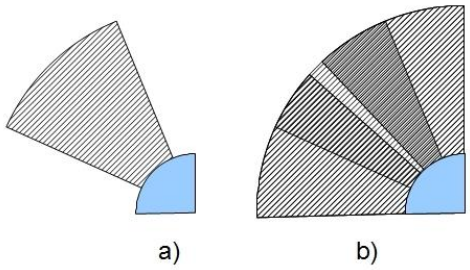
Snímače pohybu jsou určeny k prostorové ochraně objektu formou detekce pohybu osob v zorném poli snímače. Vysoká odolnost proti falešným poplachům je zajištěna digitální analýzou signálu, automatickou kalibrací vůči změnám prostředí a autotestem umožňujícím automatickou detekci poruch hardwaru. Na trhu jsou k dostání jak čidla pro:

- nástěnnou montáž,
- rohovou montáž,
- stropovou montáž.

Tato čidla můžeme dále rozdělit podle typu použité snímací technologie:

- infračervené,
- ultrazvukové,
- mikrovlnné.

Jednotlivé druhy a typy čidel se od sebe liší svými tvary charakteristik (akční rádius). Čidla pro rohovou a nástěnnou montáž mívají většinou charakteristiky ve tvaru velkého symetrického vějíře s úhlem vyzařování podle nastavení vnitřních DPS (desek plošných spojů). Pro nastavení větší zajištěné plochy čidlem se využívá nastavení nesymetrických tvarů charakteristik pomocí částečné rotace tohoto čidla, jak je zobrazeno na obrázku 3. [2]



Obr. 3: Rotace čidel: a) bez rotace b) částečná rotace čidla

Ultrazvukové detektory pohybu

Ultrazvukové detektory pohybu se skládají z ultrazvukového vysílače a přijímače pracujících na stejné frekvenci. Vysílač vysílá zvukové vlny na frekvenci vyšší jak 20kHz a odražená vlna je přijímána přijímačem. Z rozdílu doby mezi časem vyslání a přijetím vlny a ze známé rychlosti šíření vlny v prostoru je vypočtena vzdálenost tělesa, které způsobilo odraz vlny (rychlost šíření vln odpovídá přibližně rychlosti světla, což je zhruba 300 000 km/s). Pokud je v dosahu detektoru detekována změna vzdálenosti, je spuštěn poplach. Výhodou je, že tento druh alarmu je velice rychlý a spolehlivý. [2]

Infračervené detektory pohyb

Záření v infračervené oblasti je emitováno každým objektem, jehož teplota je nad teplotou absolutní nuly (0 K = -273,15 °C). Ke snímání infračerveného záření se využívá dvou druhů detektorů, které pro převod na elektrický signál využívají dvou rozdílných fyzikálních principů. Jsou to:

- **Tepelné detektory (Thermal Detectors)**
  - využívají změny některé vlastnosti materiálu na základě absorpce záření
- **Kvantové detektory (Quantum Detectors)**
  - využívají přímé přeměny dopadajícího záření na náboj, resp. elektrický proud

Nejběžnější typ infračerveného detektoru využívá pyroelektrického efektu, kde absorbované infračervené záření mění teplotu detektoru, která se pyroelektrickým efektem převádí na náboj na elektrodách. Tyto typy detektorů jsou jednoduché, velmi levné a nevyžadují žádné chlazení.[5]

Mikrovlnné detektory pohybu

Mikrovlnné detektory pracují v pásmu od 1 do 10GHz. Detektor vysílá vysokofrekvenční elektromagnetické vlny a přijímá jejich odezvu. Pokud dojde ke změně odezvy je vyhlášen poplach. Kromě spuštění poplachu lze pomocí tohoto čidla také určit rychlost postupu pachatele, což můžeme zahrnout k vyhodnocování planých poplachů. Nevýhodou mikrovlnných detektorů je, že mikrovlny pronikají například sklem, tenkými stěnami a podobně, čímž může dojít při nevhodné montáži k vyhlášení poplachu způsobeného pohybem mimo střežený prostor. Pokud je v jednom střeženém prostoru použito více mikrovlnných detektorů, musí být detektory vzájemně synchronizovány, nebo pracovat na různých frekvencích.[9]

2.3.2 Detektory rozbití skla

Detektor rozbití skla vyhodnocuje akustické změny, zvuky a změny tlaku v hlídaném prostoru. Musí být odolný proti různým rušivým signálům, které jsou podobné zvukům tříštěného skla. Mezi tyto signály můžeme zahrnout zazvonění domovního zvonku, vibrace různých předmětů a další. Každý moderní detektor rozbití skla je opatřen výstupem pro připojení k systému, ochranným krytem, pamětí a možností nastavení citlivosti pro daný hlídaný prostor. Paměť je zde využitá pro uložení vzorníku zvuku, se kterým se porovnávají zvuky tříštěného skla. Přehled některých detektorů rozbití skla a jejich parametrů je uveden v tabulce 2.

Tab. 2: Přehled některých detektorů rozbití skla a jejich parametrů [11, 12, 13, 14]

Název	GBS-210 [11]	JA-85B [12]	DL 500 [13]	JS – 25 [14]
Napájení	12V DC	3.6V DC	10 ÷ 14V DC	12V DC
Připojení	metalické	bezdrátové	metalické	Metalické
Max. odběr	10mA		28mA	35mA
Max. detekční vzdálenost	9m	9m	6.5m	9m
Min. plocha okenní výplně	0.6 x 0.6m	0.6 x 0.6m	0.3 x 0.3m	0.6 x 0.6m
Max. aktivační doba	60s			60s
Rozsah pracovních teplot	-10 ÷ 40°C	-10 ÷ 40°C	-10 ÷ 40°C	-10 ÷ 55°C

2.3.3 Kontaktní magnetická čidla

Tato čidla se skládají ze dvou částí, kde v jedné je umístěn permanentní magnet a v druhé je kontakt jazýčkového relé (dva feromagnetické plíšky). Pokud se obě tyto části vyskytují v dostatečně blízké vzdálenosti od sebe, je relé sepnuto (rozepnuto). Dojde-li ovšem k mechanickému oddálení částí, například při otevření okna nebo dveří, neboť jedna část čidla je umístěna na rámu (obvykle jazýčkové relé) a druhá (magnet) na křídle zabezpečeného vstupu do objektu, dojde k rozpojení (sepnutí) kontaktu jazýčkového relé a tím k aktivaci

poplachu. Obě části zařízení je možno k zajišťovanému objektu snadno upevnit, například přilepit nebo přišroubovat.

2.3.4 Optické závory

Optická závora je paprsek, který je v jednom bodě emitován a ve druhém detekován. Pokud dojde k narušení přenosu paprsku, je vyhlášen poplach. Optické závory mohou pracovat ve spektru:

- viditelného červeného světla,
- infračerveného světla
    - odolnější vůči rušení vnějšími světelnými vlivy,
- laseru
    - vhodný pro detekci malých objektů.

Světelné závory existují ve 3 variantách:

- světelná závora s přijímačem na protější straně vysílače,
- retro reflexní senzor s vysílačem a přijímačem v jednom zařízení
    - dochází k odrazu paprsku od odrazky nebo reflexní vrstvy,
- difúzní senzor s odrazem paprsku od detekovaného objektu.

Difúzní senzory mohou být dále v provedení s potlačeným pozadím, aby nedocházelo k nežádoucí detekci objektů na pozadí. [8]

Princip potlačeného pozadí

Princip potlačeného pozadí je založen na protínání dráhy paprsku vysílače a přijímače u difúzních senzorů. Toto protínání má za následek rozdělení viditelného pole na aktivní oblast a pozadí.

Dále je určena aktuální poloha objektu, pomocí snímání objektu ze dvou úhlů a výpočtu polohy objektu prostřednictvím geometrického uspořádání - triangulace. Tímto je docíleno spolehlivého rozlišení objektu a pozadí. [10]

3. Použité komunikační technologie a principy

V této části práce je popsána komunikační technologie IQRF a komunikace po rozhraní SPI (Serial Peripheral Interface) a pomocí sériového komunikačního rozhraní I^2C (Inter Integrated Circuit).

3.1 IQRF

Platforma IQRF byla vyvinutá společností MICRORISC s.r.o. z Jičína. Jedná se o bezdrátový modul formátu SIM (Subscriber Identity Module) karty o rozměrech 25 x 14,9 mm tzv. transceive, který obsahuje řídicí mikrokontrolér typu PIC16F88. V mikrokontroléru je naprogramovaný operační systém, obsluhující veškerou komunikaci jak bezdrátovou, tak metalickou mezi modulem a připojeným hardwarem. Tento modul je zobrazen na obrázku 4:

Obr. 4: Transceiver IQRF [21]

Veškeré příkazy a funkce pro obsluhu, komunikaci a zajištění funkčnosti jsou již naprogramovány výrobcem v mikrokontroléru modulu, čímž je zajištěna snadná realizace komunikace. To umožňuje velmi jednoduchou tvorbu aplikací i uživatelům, kteří jsou velmi zběžně seznámeni s problematikou elektroniky, VF (vysokofrekvenční) techniky, programováním a mikrokontroléry.

Operační systém v modulu se skládá z před programovaných funkcí a procedur, které se samy starají o kompletní běh aplikace. Programátorovi aplikace se tedy stačí obeznámit se syntaxí

volání procedur a funkcí, jejich parametry, vlastnostmi a funkcí. Programátor se například u bezdrátové komunikace nemusí zaobírat o problémy s:

- potvrzováním doručení paketů,
- kontrolními součty,
- adresací cílových zařízení a podobnými problémy,

které provází navázání bezdrátové komunikace pomocí zařízení bez operačního systému. Samotná komunikace mezi modulem a připojeným hardwarem je zajištěna komunikační sběrnice I^2C (Inter Integrated Circuit) a SPI (Serial Peripheral Interface).

Moduly IQRF pracují ve frekvenčním pásu, které nevyžaduje žádnou licenci pro komunikaci na těchto frekvencích. Pro USA se používá frekvence 916 MHz a pro Evropu 868 MHz. [3]

3.1.1 Topologie sítí

Modul IQRF umožňuje snadnou tvorbu rozsáhlých sítí, které lze strukturovat do menších podsítí s různými topologiemi, přičemž koordinátory podsítí jsou současně uzly páteřní sítě. Mezi topologie realizované moduly IQRF patří:

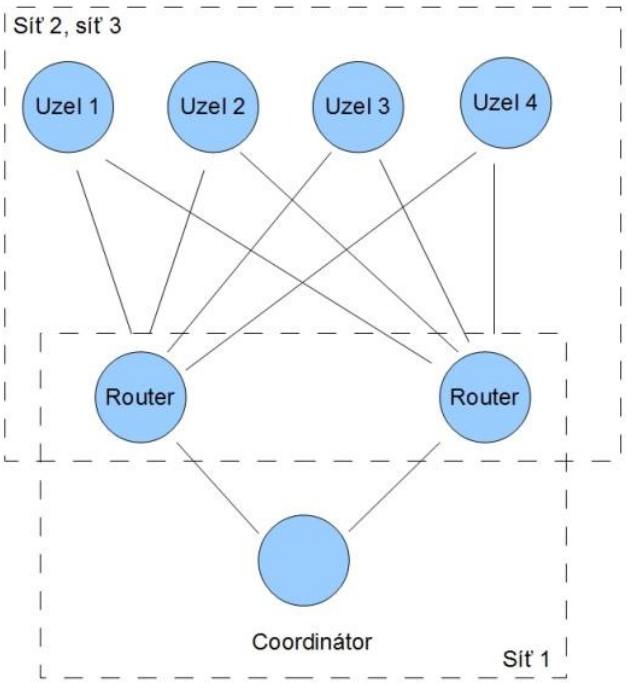
- hvězda (Star),
- rozšířená hvězda (Extended Star),
- mesh.

Mesh sítě

Mesh sítě jsou nejkomplikovanější typy sítí. Skládají se z jednoho koordinátoru a několika uzlů, které můžou mezi sebou navzájem komunikovat. Pokud není možná přímá komunikace mezi uzly nebo koordinátorem a uzlem, je možné routování této sítě. Routování znamená, že komunikace mezi žádanými prvky probíhá přes ostatní, které tyto data pouze přeposílají a nedochází k jejich zpracování. Tímto způsobem se též vytváří tzv. samo opravy, kdy při selhání preferované cesty jsou data přeposlána cestou alternativní pomocí principu mesh sítí.

3.1.2 IQMesh

Mesh sítě realizované pomocí platformy IQRF, tzv. IQMesh sítě, jsou postaveny na faktu, že jedno fyzické zařízení může být současně komunikačním bodem několika různých sítí. Routování v IQMesh sítích vyžaduje speciálně vyčleněné uzly, které zde plní funkci routeru. Koordinátor v IQMesh síti tvoří společně s vyčleněnými routery první podsíť. Každý router společně s cílovými uzly (nody) tvoří další podsítě. Schéma IQMesh je zobrazeno na obrázku 5.



Obr. 5: Schéma topologie IQMesh sítě

Přenos dat od koordinátoru k cílovému uzlu je v první podsíti řešen všesměrovým vysíláním (broadcast), kdy mezi vysílaná data je vložen identifikátor dat a adresa cílového uzlu. V routeru je tato adresa načtena a data jsou následně poslány na cílový uzel. Po přijetí dat cílovým uzlem jsou data zpracována. Po přijetí dalších dat jsou navzájem porovnány jejich identifikátory. Při shodě dojde k zahození paketu, čímž se zamezí opětovnému zpracování již přijatých dat poslaných pouze jiným routerem.

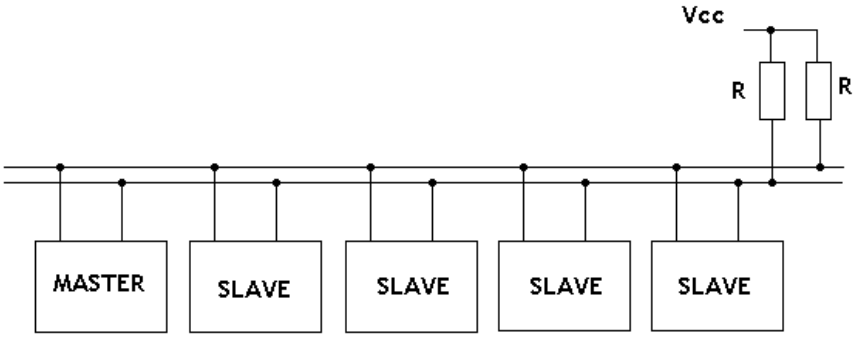
3.2 I^2C

Sériové komunikační rozhraní I^2C je ideální řešení pro komunikaci mezi mikrokontroléry. Je to dvouvodičová datová sběrnice propojující jeden nebo několik řídicích mikrokontrolérů označených jako „MASTER“ a periferní zařízení značené jako „SLAVE“.

Celkem k této sběrnici může být připojeno až 128 zařízení. Tento počet je dán strukturou komunikačního protokolu. Sběrnice I^2C je dvouvodičová, přičemž jeden vodič slouží pro přenos dat (vodič SDA) a druhý k přenosu hodinového signálu (vodič SCK), kterým bývá veškerá komunikace synchronizována. Oba vodiče je možno používat jako obousměrné, čímž je zajištěna obousměrná komunikace (half duplex).

Každý tento vodič je vybaven zvyšovacím rezistorem (PULL UP rezistor) a může být libovolným zařízením stažen na nízkou úroveň výstupem s otevřeným kolektorem nebo

drainem. Velikost těchto rezistorů není stálá, ale je dána frekvencí hodinového signálu vodiče SCK. Obecně se velikost těchto rezistorů pohybuje kolem hodnoty 10kΩ. Princip připojení zařízení a zvyšovacích rezistorů je zobrazen na obrázku 6.

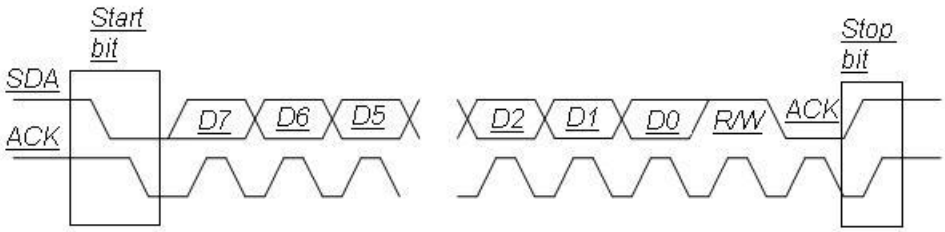


Obr. 6: Připojení zařízení a zvyšovacích odporů ke sběrnici

3.2.1 Definované stavy

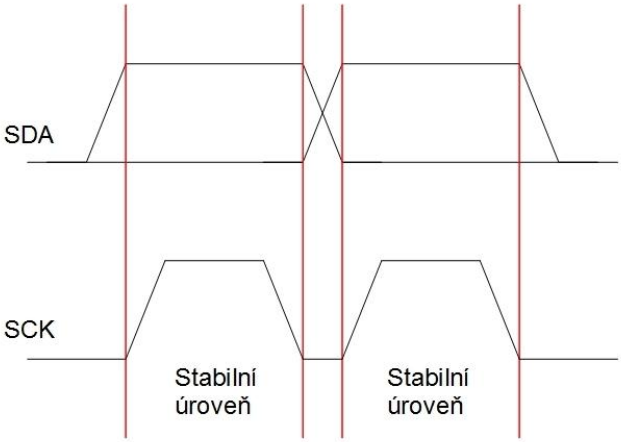
Rychlost komunikace je dána frekvencí vodiče SCK. Při komunikaci se rozeznávají přesně definované logické úrovně, které jsou zobrazeny na obrázku 7.

- klidový stav:
  - SDA i SCK na vysoké úrovni (HIGH).
- zahájení komunikace - „START BIT“ ,
  - SDA na nízké úrovni (LOW),
  - SCK na vysoké úrovni (HIGH).
- ukončení komunikace – „STOP BIT“
  - SDA i SCK na HIGH.
- přenos dat:
  - Data zabírají osm bitů, které jsou potvrzeny impulsy na SCK.
  - Přenos začíná bitem s nejvyšší váhou.
- potvrzení (acknowledge) – „ACK“:
  - SDA na LOW
  - SCK na HIGH
  - uvozuje vysílání datových bitů.



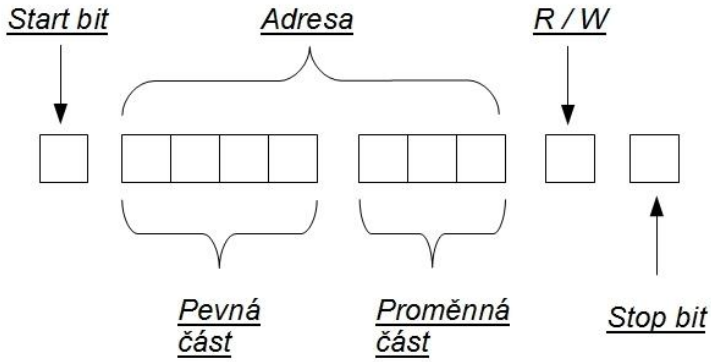
Obr. 7: Přenos dat po sběrnici I^2C

Každý bit, vyslaný na vodič SDA, musí mít stálou logickou úroveň po celou dobu trvání jednoho pulsu hodinového signálu vyslaného na SCK. Tato situace je zobrazena na obrázku 8.



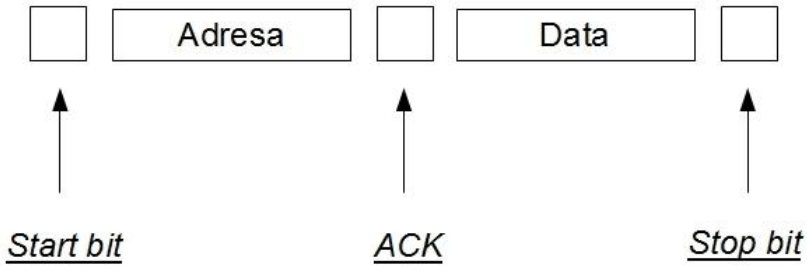
Obr. 8: Stabilita logické úrovně

Každé zařízení připojené na sběrnici je identifikováno pomocí unikátní adresy. Tato adresa je zaslána jako první část komunikace po START BITU. Celá adresa zaujímá sedm bitů, které jsou znázorněny na obrázku 9.



Obr. 9: Adresový bajt

První čtyři bity jsou napevno dány typem zařízení, následující tři jsou proměnné a osmý bit (R/W) rozhoduje o čtení nebo zápisu dat. Mají-li se číst data od zařízení SLAVE, musí se adresa přenést s bitem R/W nastaveným na HIGH. Master vždy vydá osm hodinových impulsů a dostane osm datových bitů. Po těchto bitech následuje bit ACK pro potvrzení příjmu a případné data. Celá komunikace je ukončena STOP BITEM. Grafické zobrazení adresy a komunikačního rámce je zobrazeno na obrázku 10:



Obr. 10: Datový přenos

3.3 SPI

Komunikační rozhraní SPI je sériová externí sběrnice sloužící pro vzájemnou komunikaci dvou nebo více uzlů, přičemž pouze jeden uzel vystupuje v roli řadiče sběrnice (MASTER) a ostatní uzly jako podřízení (SLAVE).

Sběrnice SPI se kvůli své hardwarové jednoduchosti používá například pro komunikaci s pamětí, textovými i grafickými LCD (Liquid Crystal Display) panely, DA a AD převodníky a obvody reálného času - RTC (Real-Time Clock).

3.3.1 Vlastnosti sběrnice SPI

MASTER obsahuje generátor hodinového signálu, který je společný všem uzlům, čímž je zajištěn zcela synchronní obousměrný přenos dat (full duplex). Hodinový signál je rozváděn vodičem SCK. Kromě tohoto vodiče jsou uzly propojeny vodiči označovaných jako MISO (Master In, Slave Out) nebo MOSI (Master Out, Slave In) určených pro přenos dat a vodičem SSEL (Slave Select), jenž slouží k výběru zařízení SLAVE.

3.3.2 Přednosti a zápory sběrnice SPI

Sběrnice SPI je kompatibilní s technologií TTL (Transistor-transistor logic) a tím pádem i s technologií CMOS (Complementary Metal-Oxide-Semiconductor). Sběrnice SPI je v podstatě několik vzájemně propojených posuvných registrů, které jsou řízeny jednotným hodinovým signálem. Obousměrná komunikace probíhá po samostatných vodičích, takže není problém mezi vysíláním a příjmem dat.

Mezi nevýhody:

- Existence pouze jednoho zařízení, které může pracovat v režimu MASTER.
- Nutnost přenášet data pouze na kratší vzdálenosti, což je dáno nutností synchronizace SCK a přenášených dat.
- Neexistence signálu typu ACK pro řízení příjmu a přenosu dat.
- Nutnost použití pro full duplexní komunikaci čtyř vodičů.
- Neexistence jednotného způsobů synchronizace dat:
  - hodinovým signálem (lze použít obě logické úrovně,
  - náběžnou hranou signálu SCK,
  - sestupnou hranou signálu SCK.

Mnoho zařízení v dnešní době obsahuje konfigurační registry kvůli volbě způsobu synchronizace dat signálem ACK. K vysílání i příjmu dat dochází vždy až po ustálení obou datových vodičů, tedy uprostřed bitového intervalu.

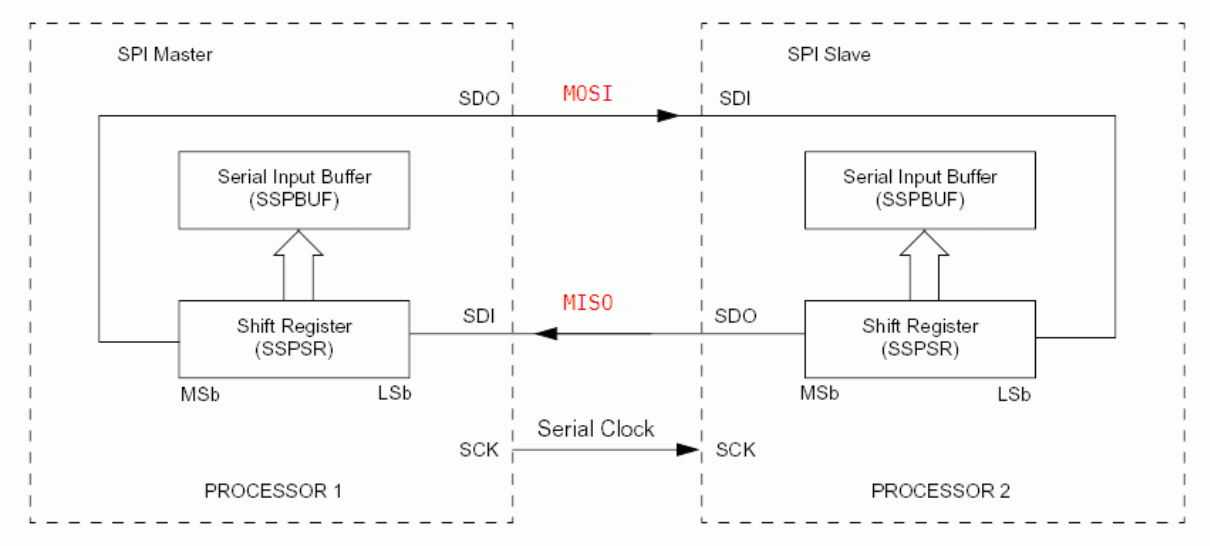
Mezi výhody patří:

- Možnost full duplexního přenosu dat,
- Neexistence datového rámce s adresačním bajtem.
- Jednoduchá komunikace a výběr aktivního zařízení SLAVE

3.3.3 Princip komunikace po sběrnici SPI

Princip propojení dvou uzlů pomocí sběrnice SPI, přičemž jeden má funkci MASTER a druhý SLAVE je zobrazen na obrázku 11. Oba uzly obsahují v tom nejjednodušším případě dva registry:

- Datový záchytný registr - Serial Input Buffer – SSPBUF,
- Posuvný registr - Shift Register – SSPSR.



Obr. 11: Princip propojení dvou uzlů pomocí sběrnice SPI [15]

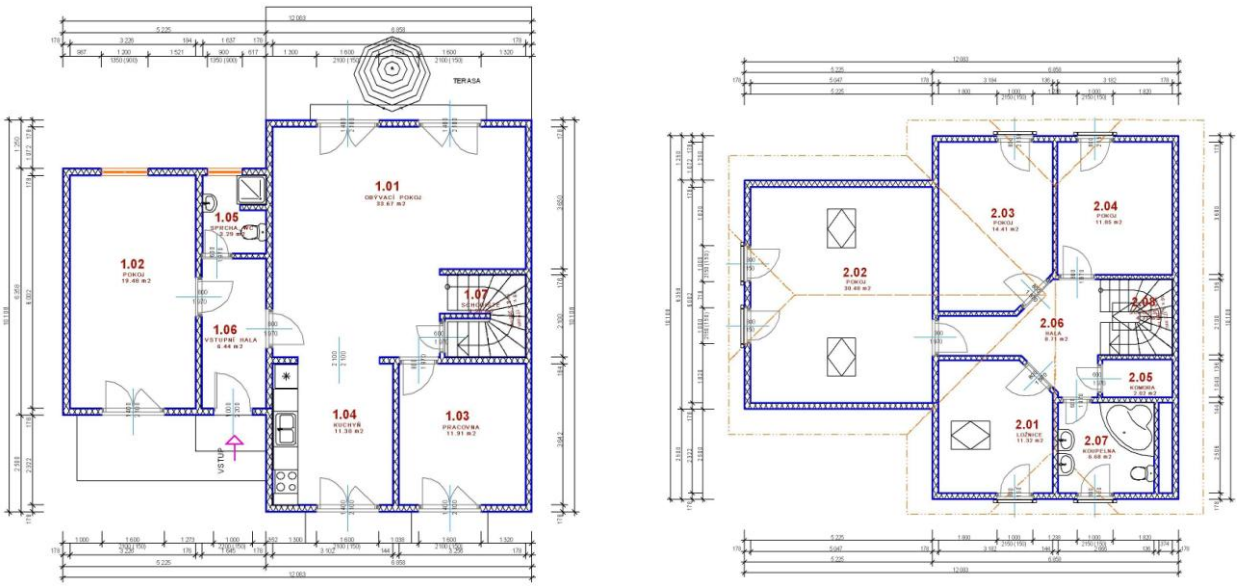
Do registru SSPSR je zapsán korektně přijatý bajt, který čeká na zpracování. Tento registr je tedy jednoprvková fronta zabezpečující korektní příjem a vysílání celého bajtu. Při každé změně signálu SCK dojde k rotování bajt doprava a bit na nejnižším místě je vyslán nebo přijat.

4. Praktický návrh

V dnešní době pro zabezpečení rodinného domu nelze použít pouze zabezpečení vstupních bodů, jako jsou okna a dveře. Musí se zajistit i prostor za těmito vstupy pro případ selhání jejich zabezpečení.

4.1 Parametry hlídaného prostoru

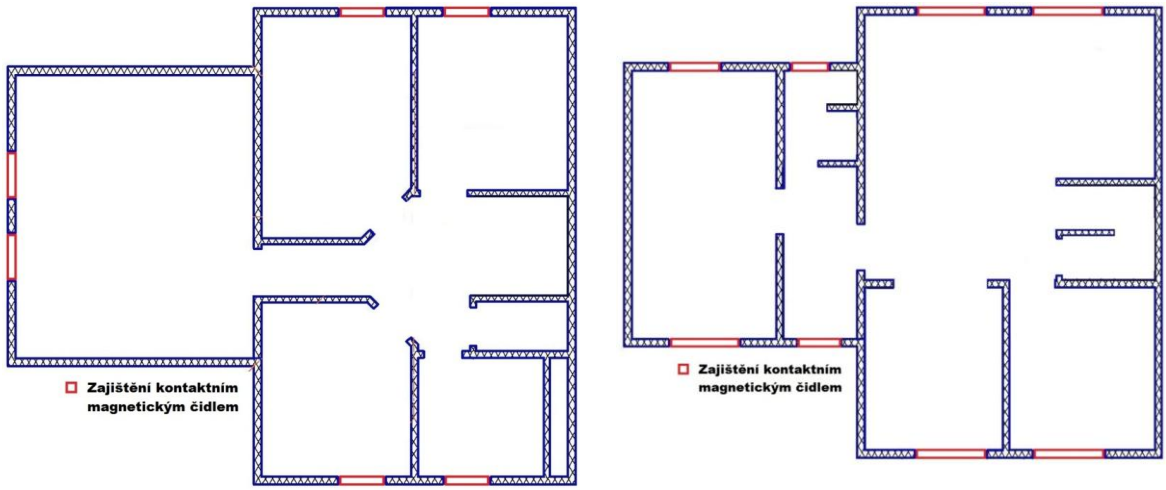
Pro funkční zajištění hlídaných prostor je nutná správná prostorová instalace zabezpečovacích prvků. Tato instalace je zcela závislá na parametrech zajišťovaných prostor. Tyto parametry jsou zobrazeny na obrázku 12.



Obr. 12: Půdorys přízemí a prvního patra rodinného domu [4]

4.2 Zabezpečení oken a dveří

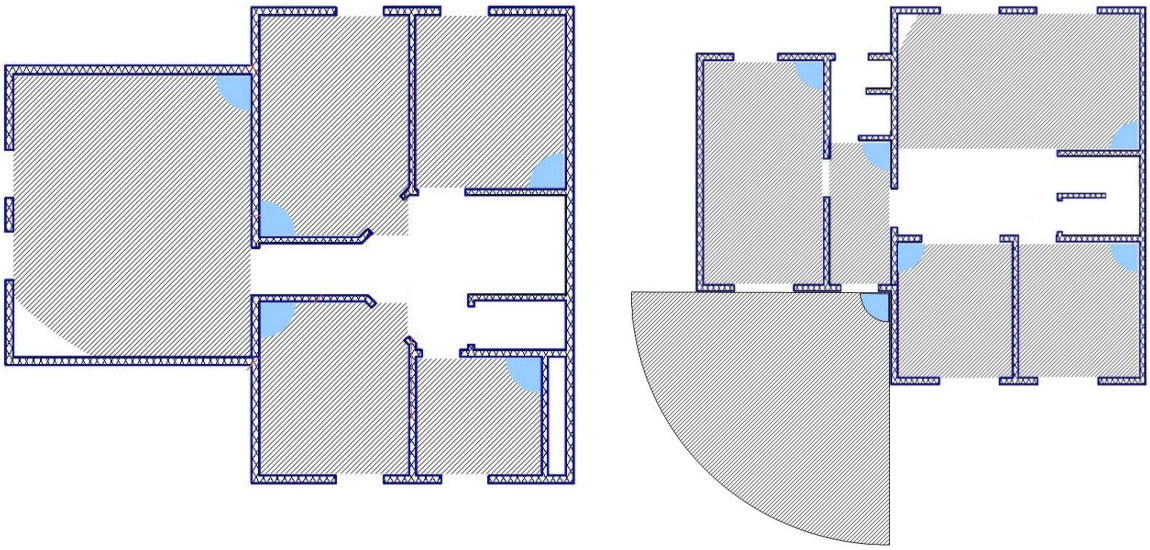
Pro zabezpečení oknem a dveří se používají magnetická bezpečnostní čidla, která se na tyto prvky montují. Těchto čidel je v dnešní době na trhu několik druhů. Liší se pouze velikostí, barvou a tvarem. Dalo by se říci, že jsou modifikací jediného typu a tím pádem je výběr čidla pro použití naprosto jednoduchý. Zabezpečení prostor pomocí magnetických čidel je zobrazen na obrázku 13.



Obr. 13: Zabezpečení přízemí pomocí magnetických čidel

4.3 Umístění čidel pohybu

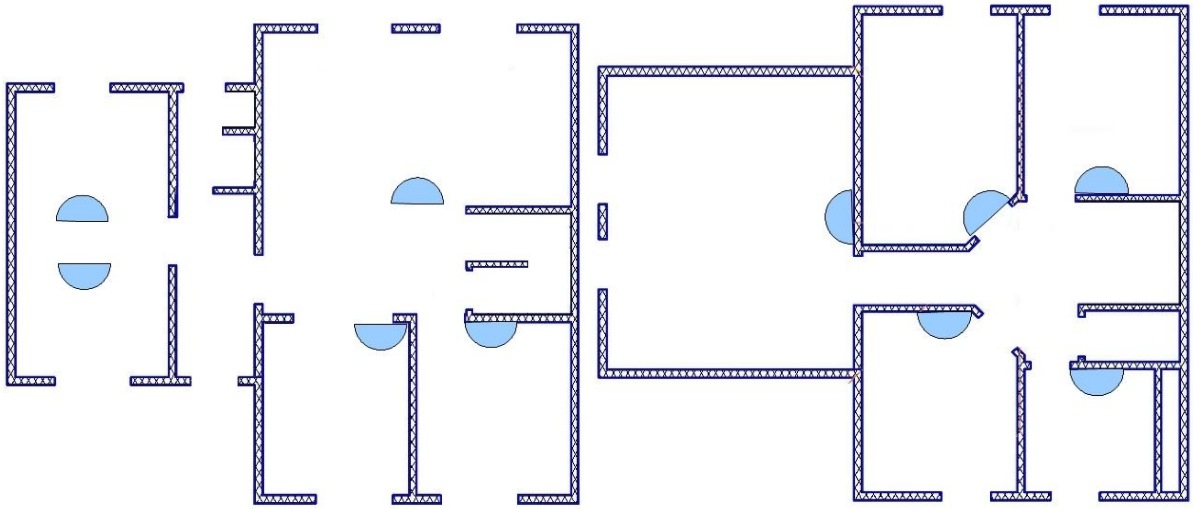
Výběr pohybového čidla pro zajištění vnitřního prostoru je vázán na parametry zajišťovaného prostoru. Je závislý na výšce stropu z důvodu minimální výšky instalace čidla, rozměrech zajišťovaného prostoru, samotné volbě mezi čidly (čidla pro nástěnnou, stropní nebo rohovou montáž) v důsledku prostorových charakteristik. Umístění čidel pohybu je znázorněno na obrázku 14. Pro zabezpečení byly použity parametry čidla pohybu MERGE JQ-L.



Obr. 14: Umístění detektorů pohybu

4.4 Umístění detektorů rozbití skla

U detektorů rozbití skla se navíc k parametrům místnosti musí brát v úvahu rozměry zaskleněné plochy a maximální vzdálenost čidla od skla pro správné nastavení citlivosti a minimalizace falešných poplachů. Umístění detektorů DL 500 je zobrazeno na obrázku 15.



Obr. 15: Umístění detektorů rozbití skla

5. Praktická realizace bezpečnostního systému

5.1 Realizace řídicí jednotky

Řídicí jednotka je hlavní část bezpečnostního systému a bývá bezpečně umístěna v zabezpečeném prostoru. Skládá se z:

- grafického dotykového displeje EA eDIPTFT43A, který slouží jako uživatelské rozhraní,
- GSM modulu SIM900 pro informování oprávněné osoby pomocí zprávy SMS při narušení zabezpečeného prostoru nebo při nestandardní situaci,
- obvodu reálního času kvůli možnosti časového managementu. Tento obvod je integrován do použitého procesoru řídicí jednotky.
- modulu IQRF pro zajištění komunikace mezi jednotlivými základními částmi,
- 16ti bitovým řídicím procesorem značky PIC s označením 24FJ256GB106 pro programovou obsluhu všech připojených zařízení, vyjma displeje, který je obsluhován vlastním integrovaným procesorem. Dále tento procesor zabezpečuje správu a ovládání celého bezpečnostního sytému.
- MINI USB konektoru umožňujícím po připojení FLASH disku nahrání reportu o stavu a historie užití systému.
- EEPROM paměti sloužící pro uklání reportu o činnosti systému,
- napájecího systému:
    - stabilizace 230V AC na 15V DC pomocí externího transformátoru a následné usměrnění na potřebné napájecí napětí jednotlivých součástí a zařízení,
    - záložní napájecí systém pro případ výpadku primárního napájení.

Řídicí jednotka umožňuje nastavení parametrů poplašného systému pro správnou funkčnost. Lze nastavit:

- zpoždění při spouštění poplachu,
- telefonní číslo pro GSM modul,
- hesla pro deaktivování systému,
- hesla pro vstup do řídicí jednotky,
- heslo pro práci s reportem,
- obecné nastavení času,
- časové nastavení intervalů kontroly připojení bezpečnostních prvků,
- definice připojených prvků a úrovně zabezpečení pro přístup uživatelů,
- telefonní kontakt pro GSM modul,
- definice zabezpečovacích profilů.

5.1.1 Displej EA eDIPTFT43

Jedná se o grafický dotykový displej s vlastním interním procesorem spravujícím ovládání a komunikaci mezi hardwarem a samotným displejem. Displej slouží jako uživatelské rozhraní pro zadávání přístupového hesla do nastavovací části a pro samotné nastavení zabezpečovacího sytému a jeho parametrů. [16] Elektrické specifikace jsou uvedeny v tabulce 3.

Tab. 3: Parametry displeje EA eDIPTFT43[16]

Parametr		MIN	MAX
Napájení		4.9 V	5.1 V
Pracovní teplota		-20 °C	70 °C
Proudový odběr	100% podsvícení	180 mA	
	Bez podsvícení	80 mA	
Vstupní napětí	**LOG 1**	3 V	5.6 V
	LOG 0	-0.5 V	1.5 V
Výstupní napění	**LOG 1**	4.2 V	
	LOG 0		0.7 V
Výstupní proud			20 mA
Rozměry	Výška	3.0 mm	
	Délka	25 mm	
	Šířka	14.9 mm	

5.1.2 Obvod reálného času a čítání času

Obvod reálného času je integrován do procesoru řídicí jednotky. Tento obvod disponuje pamětí, ve které je možno uchovávat aktuální čas (sekundy, minuty, hodiny) a datum (dny v týdnu, den v měsíci, měsíc, rok) a umožňuje tyto parametry jak číst, tak je do paměti i zapisovat. Pro přesné čítání času v sekundách je nutné připojit k procesoru přesný krystal o frekvenci 32,768 kHz. Samotné čítání času bude prováděno samotným řídicím procesorem pomocí časového přerušení nastaveného co nejpřesněji na 1s. V pravidelných časových intervalech bude docházet ke korekci reálného času načtením dat z RTC.

5.1.3 SIM 900

Jedná se o GSM / GPRS (General Packet Radio Service) modul navržený pro SMT (surface mount technology) technologii s integrovaným procesorem AMR926EJ. Umožňuje:

- hlasová volání,
- SMS,
- MMS (*Media Marketing Servies*),

- FAX,
- datovou komunikaci.

Základní elektrické a funkční specifikace jsou uvedeny v tabulce 4.

Tab. 4: Parametry obvodu SIM900

Parametr		**MIN**	**MAX**
Napájení		3.1V	4.8V
Pracovní teplota		-40°C	85°C
Proudový odběr		1.5 mA	
Pracovní pásma		850 / 900 / 1800 / 1900 MHz	
Rozměry	výška	24 mm	
	délka	24 mm	
	šířka	3 mm	
Datová komunikace		GPRS	
		PBCCH	
		CSD	
		USSD	
Podporované datové protokoly		MUX	
		TCP/UDP	
		FTP/HTTP	
		FOTA	
		MMS	
		AT	
Datové rozhraní		SIM 3V / 1.8V	
		Audio vstup	
		RTC	
		SPI	
		I2C	
		GPIO	
		PWM	
		ADC	

5.2 Realizace přístupového bodu

Přístupový bod slouží pouze k identifikaci uživatele pomocí hesla a předávání potřebných informací řídící jednotce. přístupový bod je kromě procesoru a napájecí části sestaven z:

- LCD displeje,
- 16-ti klávesové maticové klávesnice,
- IQRF modulu.

5.3 Realizace bezpečnostního prvku

Bezpečnostní prvek je kromě samotného bezpečnostního čidla zcela založena na modulu IQRF, ke kterému je přidána napájecí část v podobě dvou baterií pro napájení jak samotného modulu tak případně pro napájení bezpečnostního čidla v případě čidla s externím bateriovým napájením.

6. Obvodový návrh

Kompletní obvodový návrh je rozdělen do částí:

- více napěťový zdroj,
- obvod centrální řídicí jednotky s grafickým dotykovým displejem,
- obvod pro realizaci přístupového bodu s LCD displejem,
- komunikační obvod s modulem SIM900,
- obvod pro připojení bezpečnostního prvku.

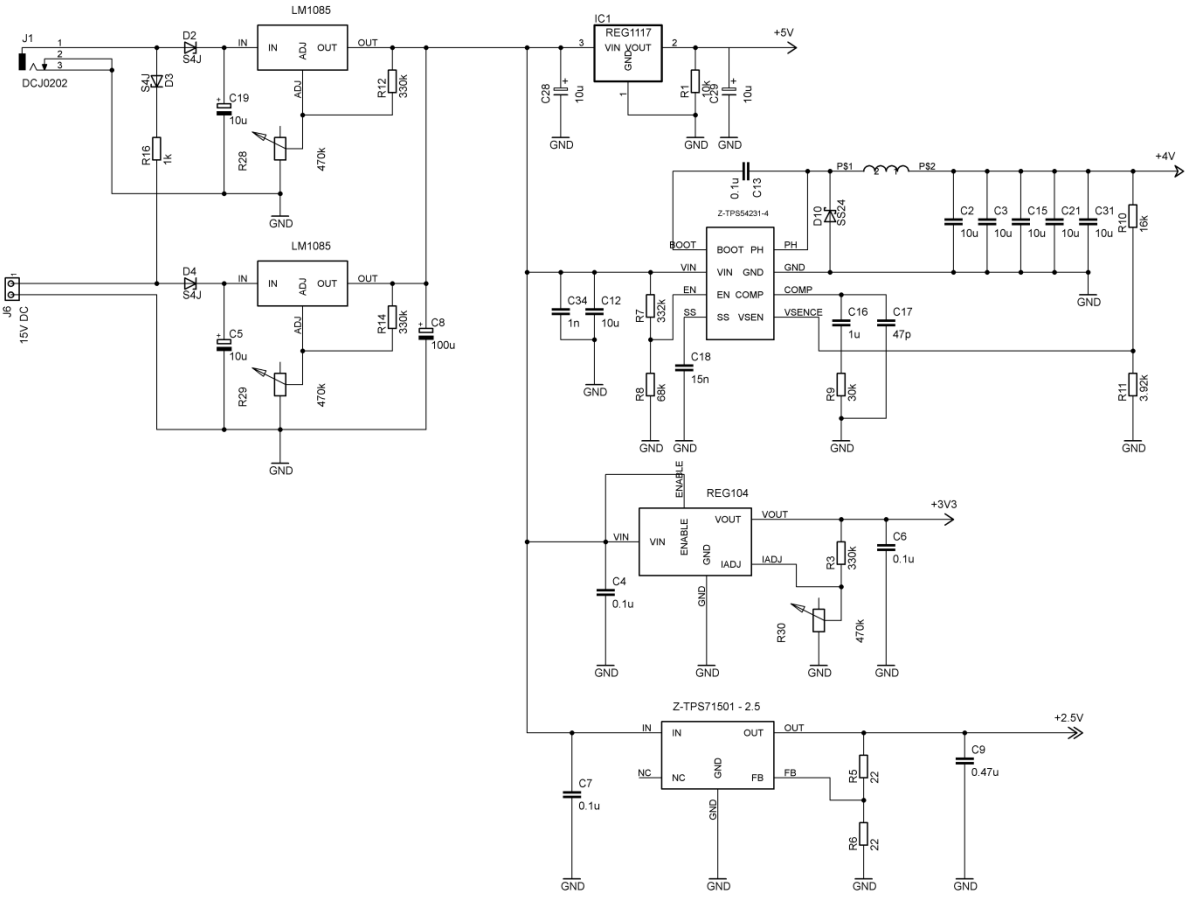
Všechny tyto části, kromě více napěťového zdroje, jsou dále opatřeny moduly IQFR pro jejich vzájemnou komunikaci.

6.1 Více napěťový zdroj

Navržený více napěťový zdroj je implementován jak v obvodu centrální jednotky, tak v obvodu přístupového bodu. V každém tomto návrhu jsou u zdroje navrženy pouze napětí použitelné pro toto zapojení, na rozdíl od zobrazeného návrhu zdroje (viz. obr.34), kde jsou navržena všechny použitá napětí. Pro získání potřebného napětí jsou použity jak stabilizátory, tak spínané zdroje.

Návrh zdroje je rozdělen do 5 základních částí definovaných svými napětími:

- před stabilizace,
- napájení grafického displeje,
- napájení GSM modulu SIM900,
- primární napájení procesoru,
- napájení jádra procesoru.



Obr. 16: Více napěťový zdroj - návrh všech použitých napětí

6.1.1 Spínaný zdroj

Rozdíl mezi spínaným a lineárním zdrojem je hlavně ve způsobu používání výkonového regulačního členu. Ve spínaných zdrojích je výkonový člen zatěžován impulsně. Je střídavě spínán a rozpínán. Využívají se výhody impulsního režimu daného prvku. V impulsním režimu může být odebíraný impulsní výkon podstatně větší, než jaký je možné odebírat v lineárním režimu s použitím stejného výkonového prvku.[20]

Spínaný vs. lineární zdroj

Výhody:

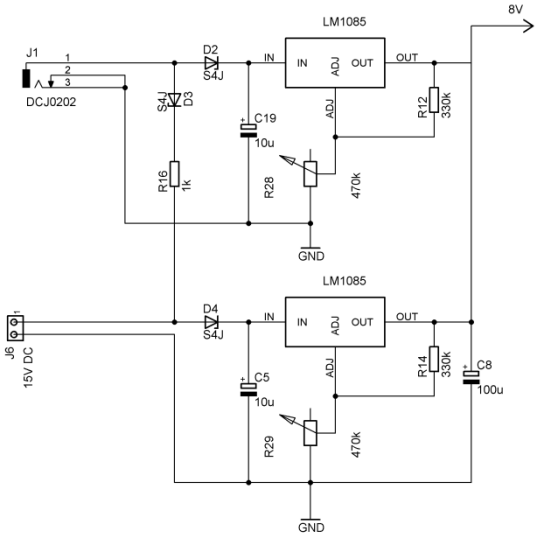
- vyšší účinnost;
- malé rozměry;
- ekonomická výhodnost.

Nevýhody:

- pomalá reakce výstupního napětí na změnu zatěžovacího proudu;
- zdroj rušivých signálů.

6.1.2 Před stabilizace

Navržený zdroj je opatřen obvodem pro předstabilizaci, kde vstupní napětí (napětí záložní baterie nebo síťové napětí usměrněné externím stabilizátorem) je stabilizováno na 8V. Pro každý vstupní zdroj je použito stabilizátoru LM1085 s mírně rozdílnými poměry děličů ve zpětných vazbách těchto stabilizátorů. Viz. Obr. 17.

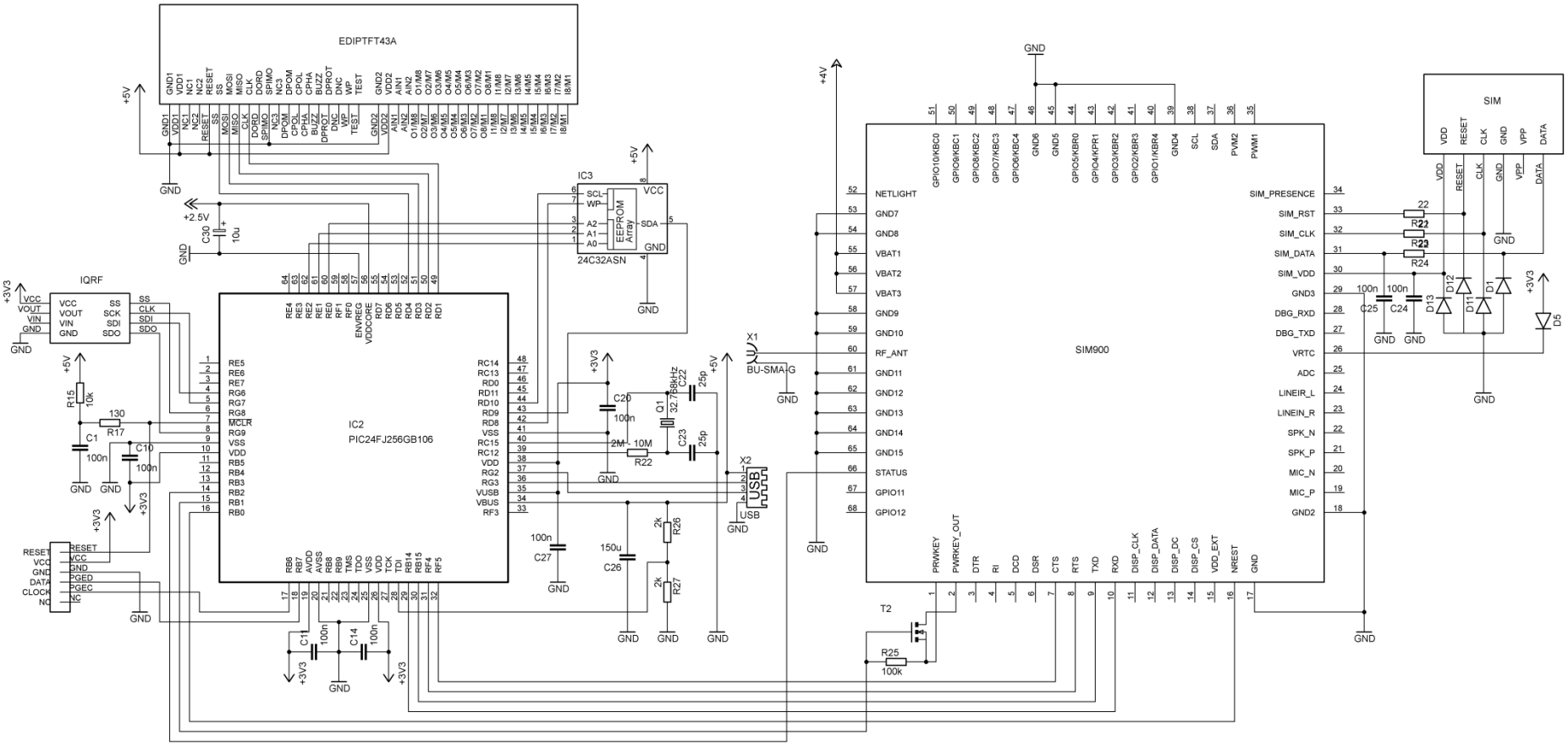


Obr. 17: Před stabilizace

Vstupy stabilizátoru jsou odděleny výkonovými diodami kvůli možnosti nabíjení záložní baterie bez nutnosti odpojení baterie z obvodu a jako ochrana před přepólováním.

6.2 Obvod centrální řídicí jednotky

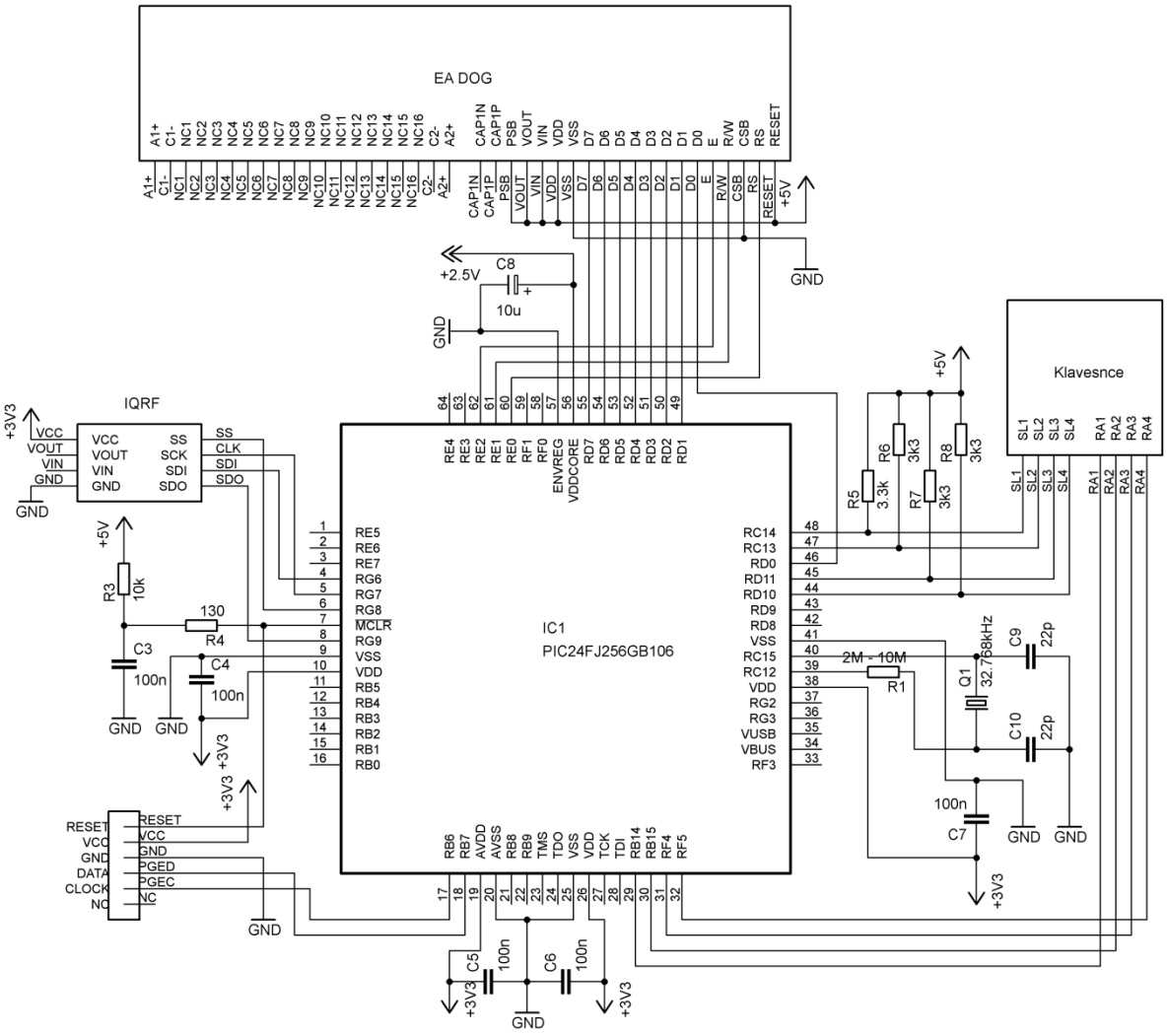
Hlavní součástí je procesor PIC24FJ256GB106, který obsluhuje celý bezpečnostní systém. K tomuto procesoru je připojen GMS modul Sim900 od firmy SimCom a barevný grafický dotykový displej eDIPTFT43-A od firmy Electronic Assembly. Pro komunikaci mezi procesorem a GSM modulem je využit UART s napěťovými úrovněmi 3,3V a pro komunikaci procesoru a displeje sběrnice SPI. Dále je zde pro bezdrátovou komunikaci mezi jednotlivými zařízeními bezpečnostního systému připojen bezdrátový modul IQRF firmy MICRORISC s.r.o. Tento modul je k řídicímu procesoru připojen sběrnicí SPI. Zapojení řídící jednotky bez napájení části je uvedeno na obrázku 18.



Obr. 18: Schéma řídicí jednotky

6.3 Obvod pro realizaci přístupového bodu

Přístupový bod je realizován procesor PIC24FJ256GB106, který obsluhuje třířádkový LCD displej DOGM106 od firmy Electronic Assembly a šestnáctiznakovou klávesnici. Pro komunikaci mezi procesorem a displejem je využito 8-bitové komunikační sběrnice s napěťovou úrovní 5V. Dále je zde pro bezdrátovou komunikaci mezi jednotlivými zařízeními bezpečnostního systému připojen bezdrátový modul IQRF. Zapojení přístupového bodu bez zdrojové části je uvedeno na obrázku 19.



Obr. 19: Schéma přístupového bodu

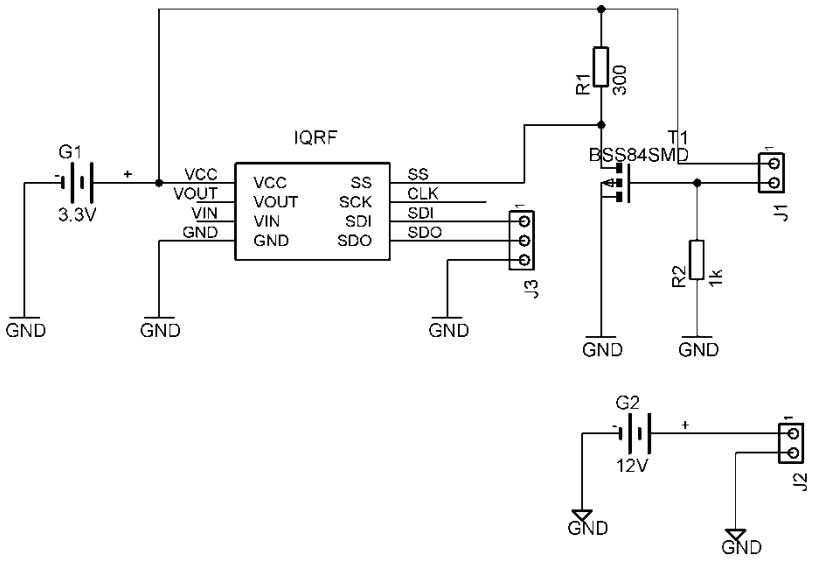
6.4 Obvod pro připojení bezpečnostního prvku

Jako bezpečnostní prvky jsou v návrhu použity:

- magnetická čidla,
- detektory pohybu,
- čidla tříštění skla.

Pro již realizovaný rodinný dům jsou veškerá čidla vyžadující napájení napájena z baterií. U domů ve stádiu realizace nebo plánování můžeme použít napájení pomocí sítě 230V se záložním bateriovým napájením.

Celý obvod se skládá z modulu IQRF, který zde zastupuje kromě komunikačního prvku taky prvek rozhodovací. Dále jsou zde dvě baterie, jedna pro napájení modulu IQRF a druhá jako napájení pro bezpečnostní čidlo. Tato baterie může být a nemusí být použita ve vztahu k typu použitého čidla. Kvůli možnosti rozhodování u magnetického čidla je obvod opatřen MOS tranzistorem plnící funkci změny logické úrovně na pinu SS modulu IQRF při rozpojení (spojení) magnetického kontaktu magnetického čidla. Schéma obvodu pro připojení bezpečnostního prvku je na obrázku 20.



Obr. 20: Schéma připojení bezpečnostního prvku

7. Programový návrh

V této kapitole se seznámíte s programovým návrhem nejdůležitějších částí bezpečnostního systému jako je:

- dotykový displej,
- IQRF,
- řídicí procesor CRJ,
- SIM900.

7.1 Program řídicího mikrokontroléru CRJ

Mikrokontrolér CRJ je zařízení řídící celý bezpečnostní systém. Přijímá data od svých periferií a tyto informace zpracovává. Podle typu přijatých správ obsluhuje celý systém. Všechny důležité informace k ovládání systému se zpracovávají zde a o výsledku jejich zpracování jsou periferie pouze informována.

Největší datová komunikace probíhá mezi procesorem a modulem IQRF připojeným pomocí sběrnice SPI, která předává informace od bezpečnostních čidel a přístupových bodu viz. kapitola 7.4.

Dalším podstatným bodem je komunikace mezi mikrokontrolerem a dotykovým displejem EA eDIPTFT43 - A připojeným sběrnicí SPI. Tento displej slouží jako přístupové rozhraní do systému pro nastavování parametrů bezpečnostního systému.

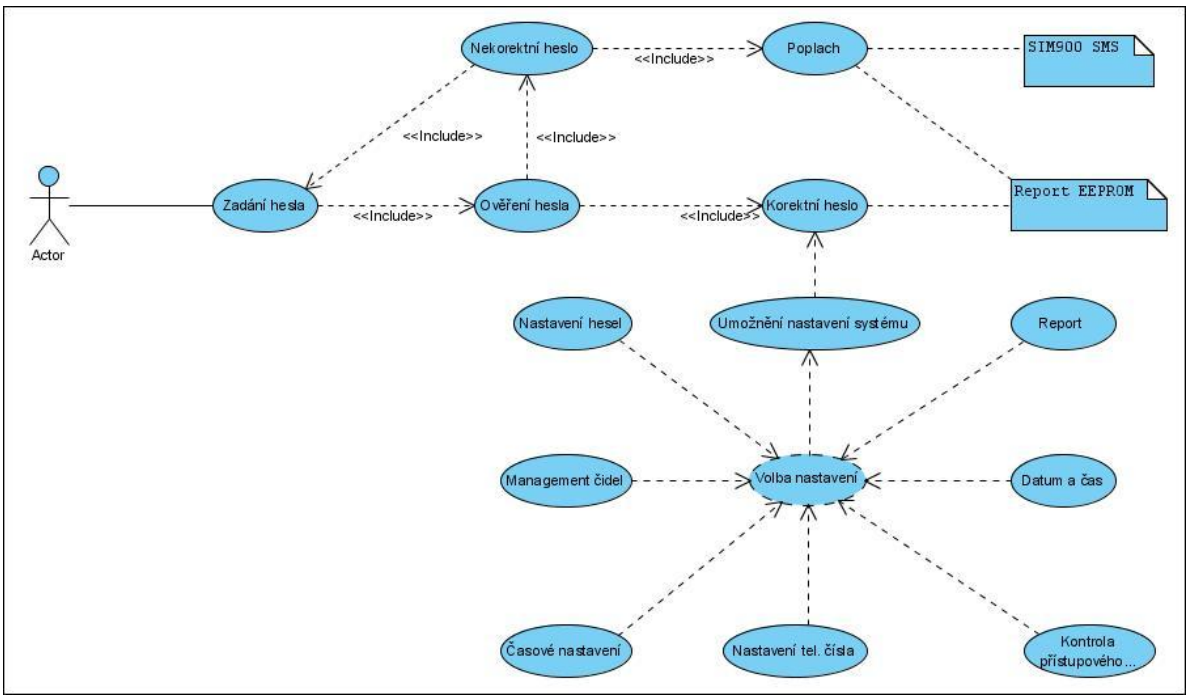
7.2 Obsluha řídicí jednotka

Systém řídicí jednotky můžeme rozdělit na několik subsystému, které se vztahují k volbám nastavení poplašného systémů. Tyto subsystémy jsou:

- nastavení času a data,
- nastavení telefonního čísla,
- management čidel,
- kontrola systému,
- časové nastavení,
- report,
- hesla.

Pro volbu nastavení je uživatel nucen identifikovat se jedinečným přístupovým heslem odlišným od hesla pro deaktivaci poplašného systému. Po korektním zadání hesla je uživateli

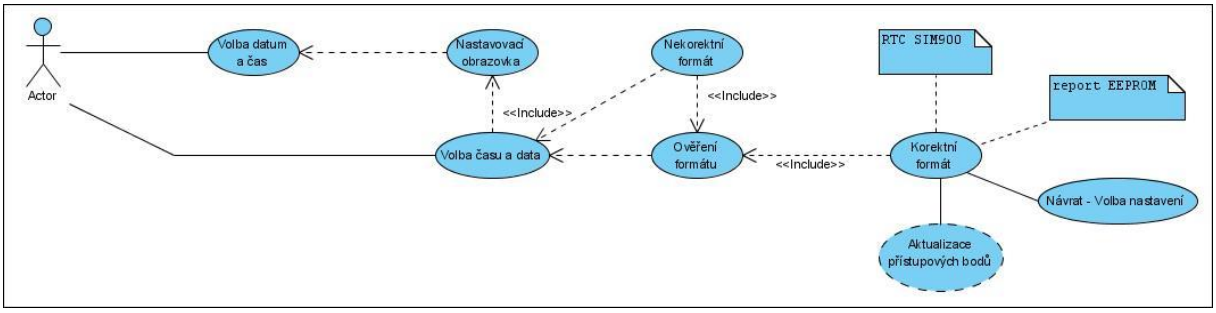
dovoleno samotné nastavení celého systému. Při nekorektním pokusu o přístup je uživateli umožněno dvou následných opakování zadání hesla, bez oznámení pokusů o přístup oprávněné osobě pomocí SMS zprávy automaticky zaslané modulem SIM900. Korektní i třetí nekorektní přístup v řadě je automaticky zaznamenán do reportu a uložen do EEPROM paměti umístěné na DPS řídicí jednotky. Principiální schéma pro volbu nastavení je zobrazeno na obrázku 21.



Obr. 21: Volba nastavení systému

7.2.1 Nastavení času a data

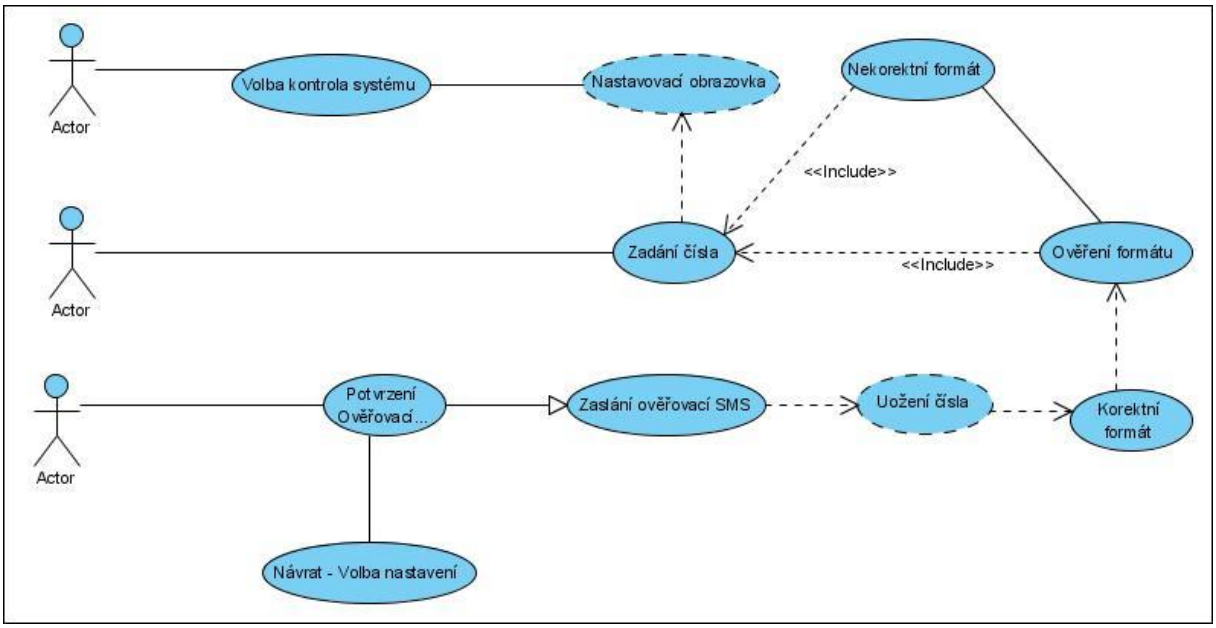
Po této volbě je nejprve načten aktuální čas z RTC, což umožňuje uživateli lepší orientaci při časovém nastavení. Po změně některého parametru a jejím potvrzení uživatelem je provedena kontrola zadaného formátu dat. Při nalezení chyby je uživatel na tuto chybu upozorněn a je nucen ji opravit. Po bezchybné kontrole je o změně času informován GSM modul, změna uložena do reportu a aktualizovány veškeré přístupové body. Princip změny časového nastavení je na obrázku 22.



Obr. 22: Princip nastavení času a data

7.2.2 Nastavení telefonního čísla

Užitím této volby je možno změnit nastavení telefonního čísla pro informování o bezpečnostním narušení systému. Po zadání nového telefonního čísla a jeho potvrzení dochází ke kontrole formátu čísla. O nekorektní kontrole je uživatel informován a nucen opravit tuto chybu. Po korektní kontrole je číslo uloženo do GSM modulu a na toto číslo zaslána ověřovací SMS zpráva. Touto zprávou je uživatel vyzván o vytočení čísla SIM karty v GSM modulu bezpečnostního systému a tím dojde k aktivaci nového telefonního čísla. Princip změny telefonního čísla je na obrázku 23.



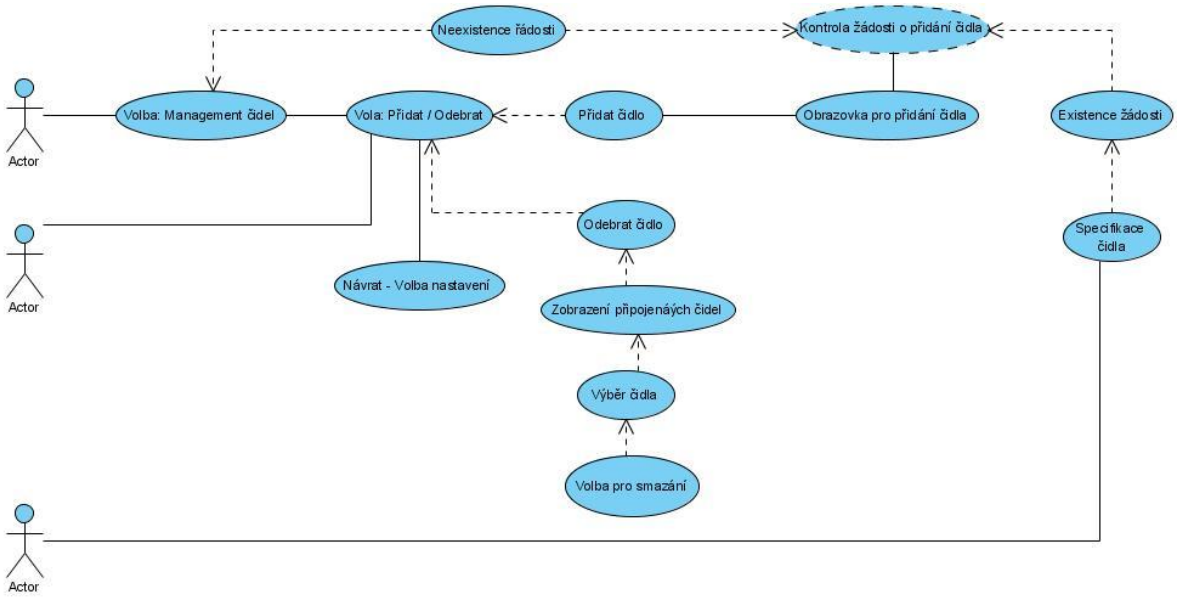
Obr. 23: Princip natavení telefonního čísla

7.2.3 Management čidel

V této volbě je uživateli umožněno přidávat o odebírat čidla do bezdrátové sítě. Po zvolení volby "Přidat" musí uživatel definovat umístění přidávaného čidla a jeho umístění odpovídá

patru kde se čidlo má nacházet a typ zabezpečovacího prvku. Tyto parametry jsou velmi důležité pro možné budoucí kontroly založené na těchto parametrech. Poté je čidlo žádající o připojení do sítě připojeno. Připojení čidlo přidáno mezi připojené čidla a potřebná data pro budoucí komunikaci uložena do paměti řídící jednotky.

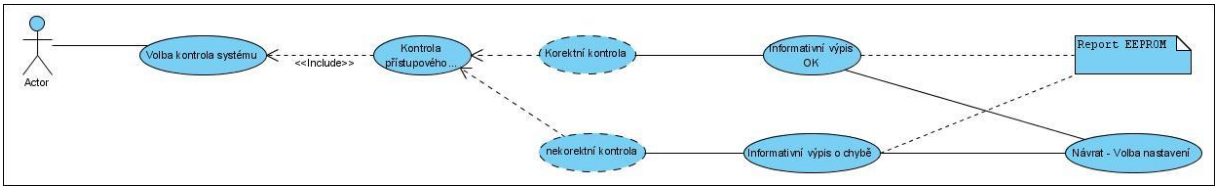
Pokud je zvolena uživatelem volba "Odebrat" je uživatel nucen specifikovat čidlo na odebrání. Specifikace probíhá pomocí jeho umístění, ID uzlu získaného z paměti bezpečnostního systému a případně i pomocí typu bezpečnostního prvku. Typ prvku je u odebírání čidla velice důležitý neboť specifikuje a umožňuje odebrat skupinu uzlů. Princip managementu je zobrazen na obrázku 24.



Obr. 24: Princip managementu čidel

7.2.4 Kontrola systému

Touto volbou je na předem definovanou dobu aktivován celý bezpečnostní systém. Je zkontrolována komunikace mezi všemi bezpečnostními čidly, zkontrolovány magnetická čidla a zkontrolován veškerý hlídaný prostor kromě prostoru s CRJ. Po kompletní kontrole je uživateli vypsán stav systému na displej a případně spuštěn poplach. Následně je stav systému zanesen do reportu. Princip kontroly zabezpečení je zobrazen na obrázku 25.



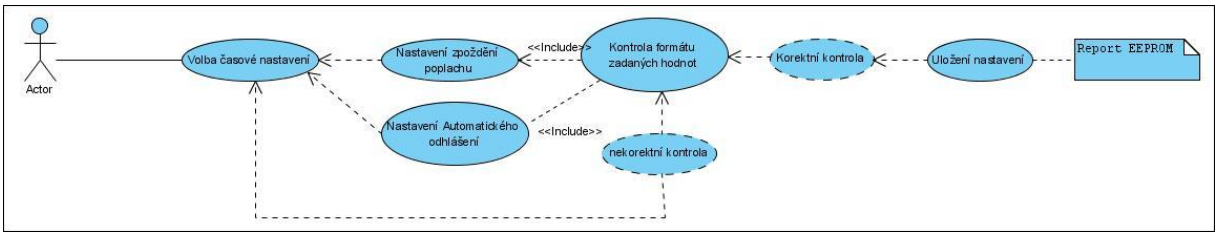
Obr. 25: Princip kontroly systému

7.2.5 Časové nastavení systému

V této volbě je možno nastavit dvě základní věci:

1. nastavení zpoždění poplachu u přístupových bodu,
2. nastavení časového odhlášení z řídicí jednotky při neaktivitě uživatele.

Při této volbě jsou uživateli oba tyto časy zobrazeny v sekundách pro lepší časovou orientaci při jejich úpravě. Po zadání a jejich potvrzení dochází ke kontrole zadaných hodnot. Po nekorektní kontrole, zadáním například nulové hodnoty, je uživatel o tomto stavu informován a zažádán o nápravu chyby. Po korektní kontrole je nové natavení uloženo a vytvořen zápis v reportu o změně nastavení. Blokové schéma je zobrazeno na obrázku 26.



Obr. 26: Princip časového nastavení systému

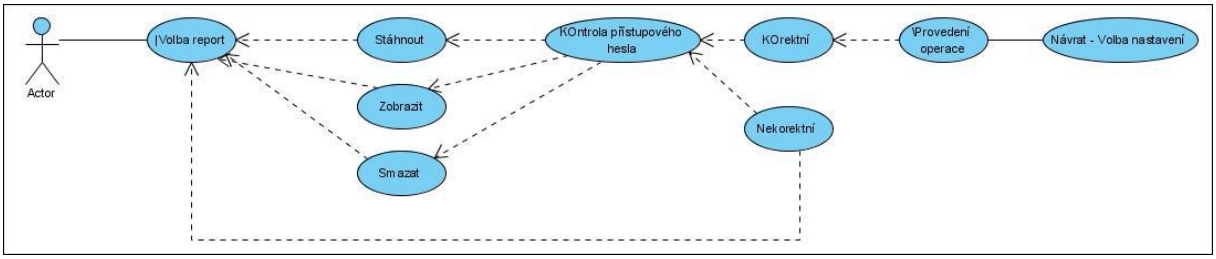
7.2.6 Princip práce s reportem

Report slouží k ukládání záznamů o stavu bezpečnostního systému a jeho změnách. Reporty v systému můžeme:

- stáhnout na flash disk,
- zobrazit na displeji,
- smazat z paměti.

Po každé z těchto voleb je uživatel zažádán o zadání přístupového hesla. Po korektním hesle je tato volba provedena, při nekorektním je zažádán o opakování zadání hesla. Při třetím po sobě jdoucím chybném zadání je uživatel odhlášen z řídicí jednotky a vytvořen záznam o

pokusu o vniku do záznamů reportu. Blokové schéma přístupu do reportu je zobrazeno na obrázku 27.



Obr. 27: Princip práce s reporty

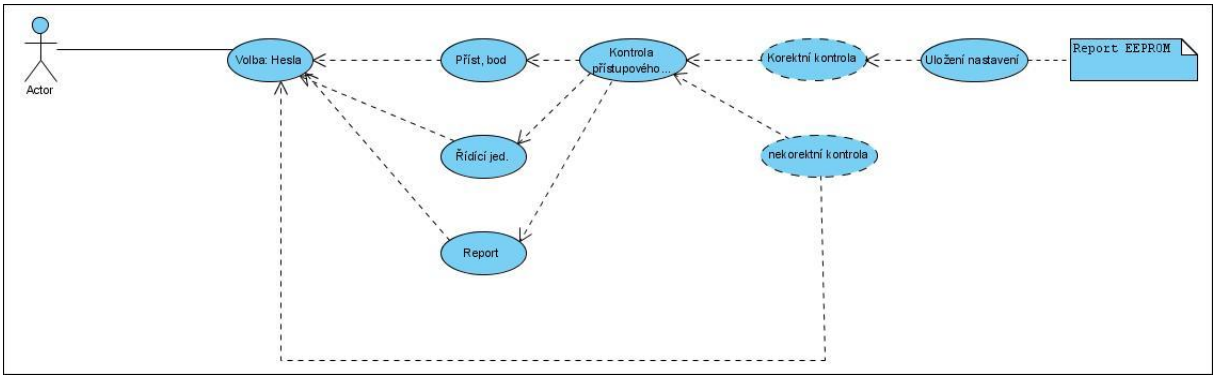
7.2.7 Hesla

Tato volba nastavení umožňuje nastavit hesla pro všechny zabezpečené oblasti systému. Jedná se o hesla pro:

- samotný přístup do řídicí jednotky,
- vypnutí bezpečnostního systému,
- administraci reportu.

Po změně libovolného hesla je uživatel zažádán o zadání přístupového hesla do řídicí jednotky, což slouží jako podružná kontrola o korektnosti změny autorizovaným uživatelem. Při změně hesla pro vstup do řídicí jednotky je tato změna potvrzena zadáním měněného přístupového hesla uživatelem. Při nekorektnosti hesla se postupuje principiálně stejně jako při přihlášení do systému řídicí jednotky, ale místo zpuštění poplachu je uživatel odhlášen z administrace řídicí jednotky bez uložení změny nastavení.

Po správně zadaném hesle jsou všechny hesla uložena a aktualizována. Tato změna je následně zapsána do reportu a uložena do EEPROM paměti. Principiální schéma celé změny hesel ze zobrazeno na obrázku 28.



Obr. 28: Nastavení hesel

7.3 Přístupový bod

Činnost přístupového bodu je rozdělen do tří subsystému specifikujících kompletní funkčnost přístupového bodu. Je to:

- vypnutí systému,
- volba aktivního profilu,
- zapnutí systému.

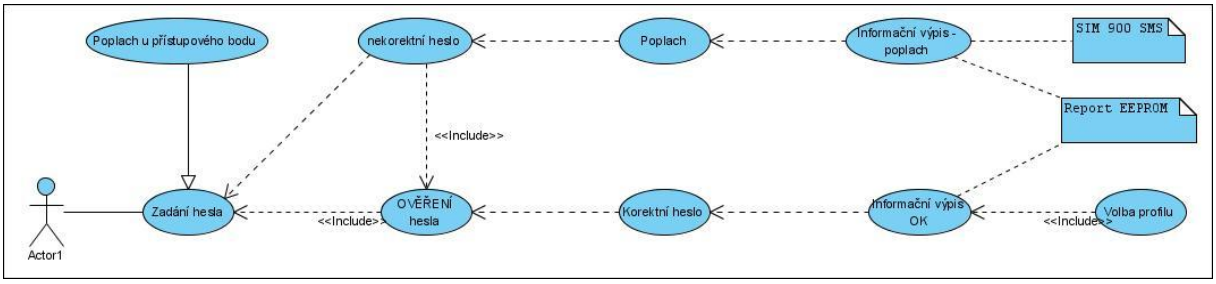
7.3.1 Vypnutí systému

Při vstupu osoby do hlídaného prostoru u přístupového bodu je toto narušení zaznamenáno bezpečnostními čidly. Vyhlášení poplachu je u těchto čidel zpožděno o definovaný čas nastavitelný v řídicí jednotce a který je defaultně určen na 15 sekund. Tento časový interval má uživatel k dispozici na deaktivaci poplašného systému.

Pro deaktivaci je potřeba zadat správné přístupové heslo. Toto heslo je pomocí modulu IQRF zasláno do řídicí jednotky, kde dojde k jeho vyhodnocení a informování přístupového bodu o korektnosti zadaného hesla.

Pokud je heslo nekorektní, má uživatel dva opětovné pokusy na jeho zadání. Po třech nekorektních pokusech po sobě je spuštěn poplach, je informována autorizovaná osoba pomocí SMS zprávy a poplach je zapsán do reportu a uložen do EEPROM paměti na DPS řídicí jednotky.

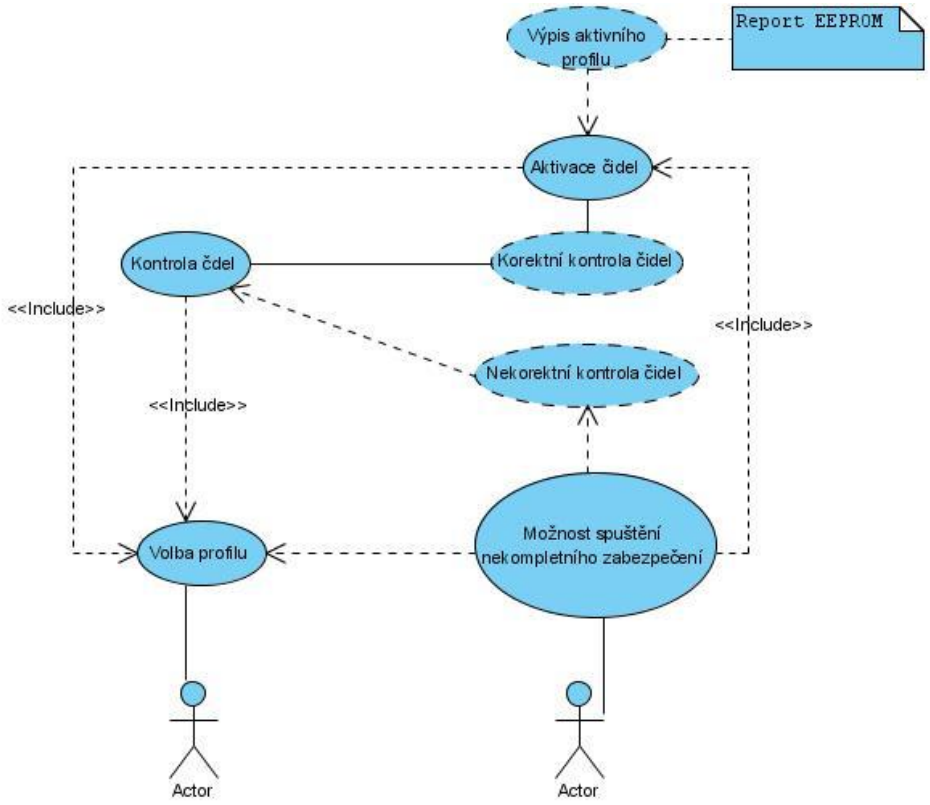
Při správném zadání hesla je bezpečnostní systém vypnut a na displeji je uživatel informován o tomto vypnutí a je mu umožněna volba aktivního profilu. Toto vypnutí systému je zaznamenáno a uloženo do reportu. Principiální schéma vypnutí bezpečnostního systému je zobrazeno na obrázku 29.



Obr. 29: Vypnutí systému

7.3.2 Volba aktivního profilu

Po volbě bezpečnostního profilu uživatelem je systémem provedena kontrola týkající se zabezpečené části hlídaného prostoru, která se vztahuje k nově aktivovanému profilu. Po kontrole je uživatel informován o výsledku této kontroly. Po bezchybné kontrole je automaticky spuštěn vybraný bezpečnostní profil. Pokud je při kontrole narušen zabezpečovaný prostor je uživatel, o tomto stavu společně s typem a umístěním čidla, informován. Poté je uživateli nabídnuta možnost pokračovat v zabezpečení bez kontroly tímto čidlem nebo aktivaci přerušit a provést patřičné kroky k nápravě.

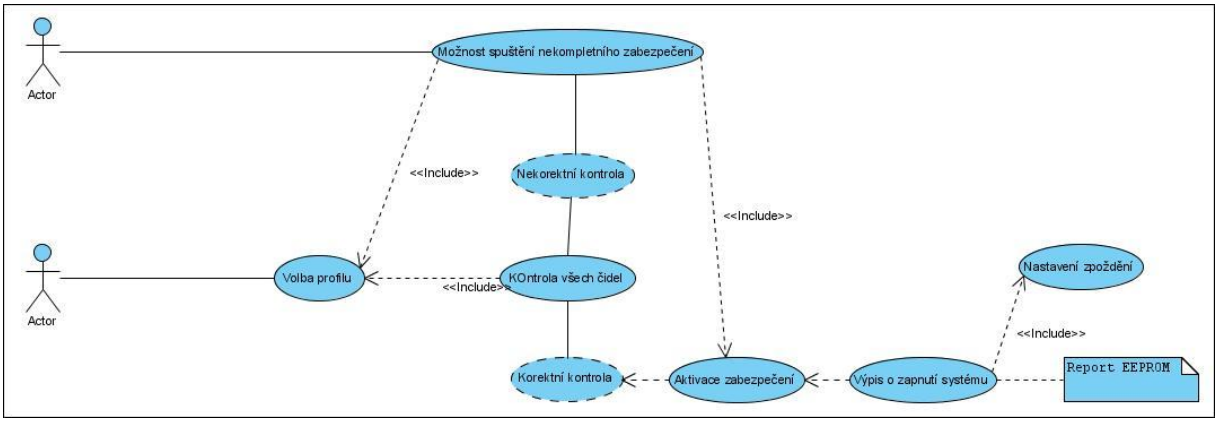


Obr. 30: Volba aktivního profilu

7.3.3 Zapnutí systému

Uživatel pomocí přístupového body zvolí profil OUT, o čemž je pomocí modulu IQRF informována řídicí jednotka. Řídicí jednotka zkontroluje připojení všech čidel a zkontroluje hlídaný prostor. Pokud je vše v pořádku je spuštěn systém bez čidla hlídajícího aktivní přístupový bod na dobu potřebnou k opuštění hlídaného prostoru. Spuštění systému je zaznamenáno do reportu a následně uloženo do paměti EEPROM.

Pokud je systémem identifikována chyba při kontrole (čidlo nekomunikuje, hlídaný prostor je narušen) je uživateli umožněno tytu chybu ignorovat a bezpečnostní systém spustit bez kompletní ochrany nebo spuštění systému přerušit a chybu odstranit. Principiální schéma zapnutí bezpečnostního systému je zobrazeno na obrázku 31.



Obr. 31: Zapnutí systému

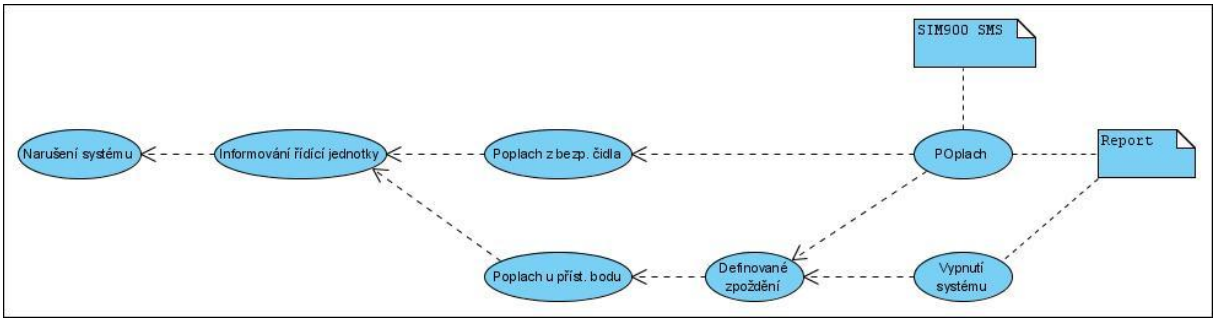
7.3.4 Funkční princip spuštění poplachu

Poplach může být zpuštěn ze dvou důvodu.

- Vniknutím osoby do střeženého prostoru mimo prostor s přístupovými body.
- Vniknutím osoby do střeženého prostoru s přístupovými body viz. Vypnutí systému.

Při detekování narušení v oblasti mimo oblast s přístupovým bodem je ihned pomocí modulu IQRF informována řídicí jednotka a je spuštěn poplach. Pomocí modulu SIM900 je informována pověřená osoba a poplach zaznamenán do reportu.

Při narušení oblasti s přístupovým bodem je poplach zpožděn o předdefinovaný čas pro ověření oprávněného přístupu, viz. Vypnutí systému. Principiální schéma zapnutí bezpečnostního systému je zobrazeno na obrázku 32.



Obr. 32: Vniknutí osoby do střeženého prostoru a vyhodnocení poplachu

7.4 Bezdrátová komunikace mezi zařízeními

Ke komunikaci mezi řídicí jednotkou a dalšími prvky systému je využívám bezdrátová platforma IQRF. Modul IQRF v centrální jednotce vykonává funkci hlavního koordinátoru (hierarchicky nejvýše postaveného komunikačního zařízení v realizované síti). Koordinátor centrální jednotky (KCJ) přímo spravuje tři typy uzlu:

- uzel přístupového bodu (PB),
- koordinátor patra (KP),
- zařízení pro připojení bezpečnostního prvku (BP).

Kvůli jednoduchosti komunikace, neexistence důvodu extremně velkého počtu uzlu a zaměření návrhu na implementaci do rodinného domu byl počet každého typu zařízení omezen počtem devíti a u zařízení pro připojení prvků k jednomu koordinátoru na 99. I přes toto omezení je při maximální možné výtěžnosti k centrální jednotce připojit až 881 bezpečnostních prvků viz. rovnice 1.

$$maximalní\ výtěžnost = maximální\ počet\ KP * počet\ čidel\ na\ jedn\ koordinátor \quad (1)$$

7.4.1 Modul přístupového bodu

Komunikace mezi přístupovým bodem a řídící jednotkou probíhá bez jakékoliv podpory dalších síťových uzlů, čímž se sníží na minimum doba mezi vysláním a příjem dat, doba odezvy a možnost vzniku chyb. Veškerá komunikace probíhá oběma směry - half duplex, vzájemná komunikace je vždy potvrzena zasláním identifikačního příznaku pro potvrzení příjmu komunikace cílovým uzlem nebo koordinátorem, nebo očekávanou odpovědí například na ověření přístupového hesla od centrální řídící jednotky.

Po vyvolání akce na přístupovém bodu nebo centrální řídicí jednotce například zadáním a potvrzením hesla uživatelem na přístupovém bodu je řídicí jednotce zaslán datový balík (paket) obsahující kromě povinných parametrů (adresa příjemce, adresa odesilatele, CRC) data obsahující identifikační příznak a zadané heslo. Identifikační příznak musí být jedinečný pro použitou technologii přenosu dat v aktuální síti, ale pro jinou technologii, síť, podsíť může uvozovat jinou akci. Řídicí jednotka vyhodnotí přijaté data (příznak) jako žádost o kontrolu hesla a zadané heslo, provede kontrolu a informuje přístupový bodu o výsledku kontroly.

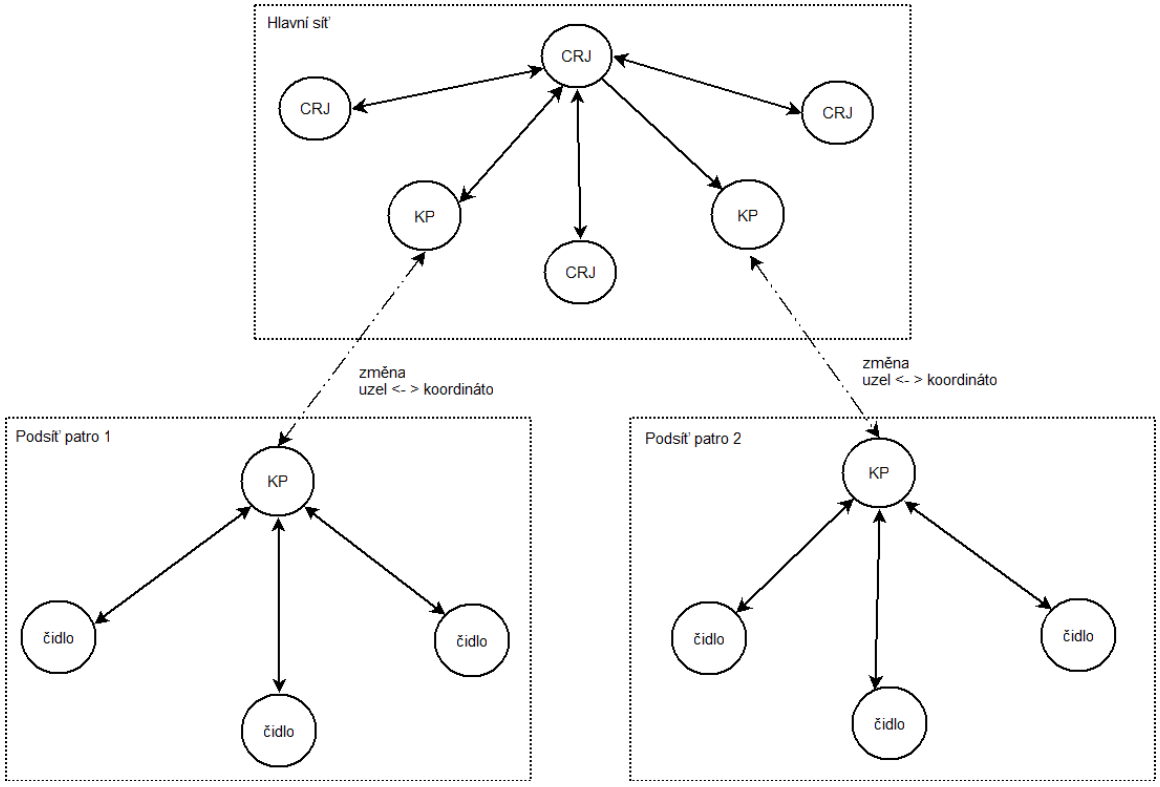
Mezi přístupovým bodem a řídící jednotkou může probíhat vzájemná komunikace jako reakce na různé akce. Všechny akce typické pouze pro přístupový bod jsou uvedeny v tabulce 5.

Tab. 5: Akce přípustné pouze pro přístupový bod (PB) vs. centrální řídicí jednotka (CRJ)

Akce	**Odesilatel**	**Příjemce**	
		Odpověď.	Potvrzení
Přidání PB	CRJ	ID	
Zadání hesla - vypnutí bezpečnostního systému	PB	Souhlasí / nesouhlasí	
Změna bezpečnostního profilu	PB		
Kontrola systému	CRJ	OK / Poplach	
Aktualizace - datum, čas	CRJ		Příznak
Oznámení o poplachu	CRJ		Příznak

7.4.2 Koordinátor patra a uzly podsítě

Koordinátor patra je jedním ze dvou možných typů uzlů patřící do sítě hlavního koordinátoru. Na rozdíl od uzlu přístupového bodu je současně součástí podsítě kde zastupuje roli koordinátoru. Pro příjem dat od řídící centrální jednotky je nutno nastavit uzel patřící do této sítě. Při detekci dat určených do podsítě se uzel přepne do podsítě kde je koordinátorem a data přepošle na cílový uzel (čidlo). Struktura sítě a podsítě je zobrazena na obrázku 33. Při komunikaci čidla a centrální řídicí jednotky je postup obrácený ale principiálně zcela obdobný.



Obr. 33: Struktura sítě a podsítě

Všechny akce typické pro komunikaci mezi CRJ a KP s čidly jsou uvedeny v tabulce 6.

Tab.6: Akce přípustné pouze pro PB a čidla vs. CRJ

Akce	**Odesilatel**	**Příjemce**	
		Odpověď.	Potvrzení
Přidat koordinátor patra	CRJ	ID	
Přidat uzel	CRJ	ID + ID	
Odebrat koordinátor patra	CRJ		Příznak
Odebrat uzel	CRJ		Příznak
Zkontrolovat podsíť	CRJ	OK / chyba ID	
Poplach	KP		
Kontrola zabezpečení - vše	CRJ	OK Chyba	
Odebrat vše	CRJ		Příznak

7.4.3 Struktura komunikačního protokolu

Pro komunikaci v bezdrátové síti je použito dvou komunikačních protokolu, lišících se jednou částí paketů. Jedná se o komunikaci typu:

- P2P (peer - to - peer),

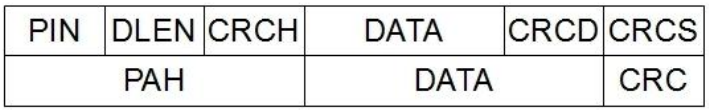
- IQMesh.

Rozdíly v těchto protokolech je v počtu a obsahu informačních bloků. Pakety pro P2P komunikaci se skládají z bloků s názvy:

- PAH (Paket Header),
- Data,
- CRC (Cyclic redundancy check).

K paketu pro IQMesh síť je navíc připojen blok NTWINFO (Networking information).

Každý blok je dále rozdělen podle bajtů, přičemž jeden bajt každého bloku je kontrolní mechanizmus, pro zajištění spolehlivosti přenosu. Struktury protokolů jsou zobrazeny na obrázcích 34 a35.



Obr. 34: Struktura protokolu pro P2P komunikaci

Obr. 35: Struktura protokolu pro IQMesh komunikaci

Komunikační protokol je zobrazen v tabulce 7.

Tab. 7: Komunikační protokol

Název paketu	adresa adresáta	typ odesílatele	adresa odesílatele	délka paketu	data	CRC
Přidat koordinátor patra	0x0X	0x01	0x01	2	Příznak, patro	
Přidat přístupový bod	0x1X	0x01	0x01	2	Příznak, příznak	
Přidat čidlo do patra	0x0X	0x01	0x01	3	Příznak, patro, typ	
Odebrat čidlo z patra	0x0X	0x01	0x01	4	Příznak, patro, ID	
Odebrat koordinátor patra	0x0X	0x01	0x01	2	Příznak, patro	
Odebrat přístupový bod	0x1X	0x01	0x01	3	Příznak,ID	
Potvrzení přidání koordinátoru	0x00	0x0X	0x0X	2	Příznak, ID	
Potvrzení přidání přístupového bodu	0x00	0x1X	0x1X	2	Příznak, ID	
Potvrzení přidání čidla	0x00	0x0X	0x0X	3	Příznak, patro, ID	
Potvrzení odebrání čidla z patra	0x00	0x0X	0x0X	3	Příznak, patro, ID	
Potvrzení odebrání koordinátoru	0x00	0x0X	0x0X	2	Příznak, patro	
Potvrzení odebrání přístupového bodu	0x00	0x1X	0x1X	2	Příznak, ID	
Kontrola vše	0xFF	0x00	0x00	2	Příznak, 0	
Kontrola na patře	0x0X	0x00	0x00	2	Přídla, patro	
Kontrola typu čidla	0xFF	0x00	0x00	3	Příznak, příznak, typ	
Kontrola typu čidla na patře	0x0X	0x00	0x00	3	Příznak, patro, typ	
Kontrola typu čidla všude	0xFF	0x00	0x00	3	Příznak, 0 , typ	
Odezvu čidla (kontrola)	0x00	0x0X	0x0X	6	Příznak, odkud, ID, OK	
Ověření hesla	0x00	0x1X	0x1X	6	Příznak, heslo	
Aktivace profilu	0x00	0x1X	0x1X	2	Příznak, profil	
Odpověd na kontrola hesla	0x1X	0x00	0x00	3	Příznak,OK	
Aktualizace času, data	0x1X	0x00	0x00	13	Příznak,čas,datum	
Poplach	0x1X	0x00	0x00	1	Příznak	

7.5 Program SIM900

SIM900 je GSM modul s vlastním operačním systémem. K řídícímu procesoru je připojen sběrnicí UART, který pomocí vysílání řídících příkazů ovládá GSM komunikaci. Řídicí příkazy jsou specifické funkce a procedury z operačního systému GSM modulu, které spouští výrobcem implementované programy v operačním systému modulu zabezpečující navázání, správu a bezchybný průběh komunikace s dalšími GSM zařízeními.

8. Závěr

Úkolem této práce bylo navrhnout a realizovat bezpečnostní systém pro rodinný dům s použitím bezdrátové technologie IQRF.

V této práci jsou uvedeny a diskutovány veškeré parametry potřebné k navržení funkčního bezpečnostního systému. Celé zařízení bylo teoreticky navrženo. Byly navrženy veškeré obvodové návrhy pro budoucí realizaci systému od řídicí jednotky, přes přístupový bod až po obvodový návrh připojení všech diskutovaných bezpečnostních čidel.

U řídicí jednotky bylo brána v potaz nutnost komunikace s nadřazeným bezpečnostním systémem, v tomto případě s autorizovanou osobou nebo přímým připojením na pult centrální ochrany. Tento požadavek byl vyřešen zahrnutím GSM modulu SIM900 do návrhu centrální řídicí jednotky.

Pro komunikaci mezi jednotlivými zařízeními systému byl zvolen bezdrátový komunikační modul IQRF. Byla navržena proměnná topologie sítě (o maximu dvou úrovní) kvůli rozsáhlosti zabezpečovaného prostoru, nutnost přesnější identifikace místa narušení a možnosti dynamického použití této sítě v závislosti na požadavcích majitele a parametrech zabezpečovaného prostoru. Primárně byla zvolena topologie IQMESH, kde primární síť zahrnuje modul řídicí jednotky jako koordinátor celé sítě, přístupové body a uzly, které současně slouží jako koordinátory pro pod sítě. Každá tako podsíť obsahuje kromě koordinátoru již pouze zařízení pro připojení bezpečnostního prvku.

Prakticky byla realizován kompletní DPS centrální řídicí jednotky s napěťovou částí, ovládací systém centrální řídicí jednotky pomocí dotykového grafického displeje a IQMESH síť. Ovládací program v displeji je realizován do míry omezené pouze na tento displej. Samotné nastavení systému by mělo být realizováno programem procesoru řídící jednotky, který do této doby nebyl realizován.

Z důvodu velké rozsáhlosti práce nebyla realizována DPS přístupového bodu a obslužný program pro procesory řídící jednotky a přístupového bodu.

Konkrétním výstupem této práce je tedy kompletní návrh bezpečnostního systému s diskuzí všech parametrů, použitých technologií a rozbor použitých hlavních součástek a zařízení navržených pro použití v realizovaném bezpečnostním systému. Systém je tedy ke dnešnímu dni za fází kompletního návrhu a zhruba v 60% realizace.

9. Seznam zkratek

AC	alternating current
AD	Analog/digital
CRC	Cyclic redundancy Check
CRJ	Centrální řídicí jednotka
CMOS	Complementary Metal-Oxide-Semiconductor
DA	Digital/analog
DC	Direct current
DPS	Deska plošných spojů
GSM	Global System for Mobil Communication
I^2C	Inter Integrated Circuit
IQRF	Intelligence Quotient Radio Frequency.
KP	Koordinátor patra
LAN	Local Area Network
LCD	Liquid crystal display
LED	Light Emitting Diode
MISO	Master In, Slave Out
MOSI	Master Out, Slave In
NTWINFO	Networking information
P2P	Peer – to – peer
PB	Přístupový bod
PAH	Paket Header
SIM	Dubscriber identity module

SMS	Short Message Service
SPI	Serial Peripheral Interface
TTL	Transistor-transistor logic
VF	Vysokofrekvenční
UART	Universal Asynchronous Receive Transmitter
Wifi	Wireless Fidelity

10. Použité zdroje

[1] KŘEJČIŘÍK, Alexandr. *SMS-Střežení a ovládání objektů pomocí mobilu a SMS*. 1. vyd. Praha : BEN - technická literatura, 2004. 304 s. ISBN 80-7300-082-2.

[2] DIEM, Walter. *Bezpečnostní zařízení*. Redaktorka Pavla Vokounová; přeložil Karel Kopička. 1. Auflage. Praha : Ikar, 2000. 111 s. ISBN 80-7202-604-6.

[3] I*QRF : simply way to smarter wireless solution* [online]. 2010, updated 2010-04-14 [cit. 2010-04-21]. Dostupné z WWW: <http://www.iqrf.com/weben/index.php>.

[4] *Montáže domů, stavby na klíč:RD : akce* [online]. 2009 [cit. 2010-04-21]. Magenta production s.r.o. Dostupné z WWW: <http://www.magenta.cz/akce/rd-akce.html>.

[5] VOJÁČEK, Antonín. *www.hw.cz : automatrizace* [online]. 11 Říjen, 2007 - 21:24 [cit. 2010-04-14]. Infračervené kvantové detektory a termokamery. Dostupné z WWW: <http://automatizace.hw.cz/infracervene-kvantove-detektory-termokamery-uvod>.

[6] *GM Electronic* [online]. 2010 [cit. 2010-04-21]. Dostupné z WWW: <http://www.gme.cz/cz/>.

[7] *Zabezpečovací systémy : GURU CZ* [online]. 1999 [cit. 2010-04-21]. Dostupné z WWW: <http://www.zabezpecovaci-system.eu/produkty/detektory/detektory-pohybu/ja-80p-bezdratovy-pir-detektor-pohybu-osob-29.htm>.

[8] *Produkty : Fotoelektrické senzory* [online]. 2009 [cit. 2010-04-18]. Schmachtl elektronika strojírenství. Dostupné z WWW: <http://www.schmachtl.cz/senzorika/binarni-fotosenzory/fotoelektricke-senzory/>.

[9] JAROŠ, Miroslav. *Základní informace o detektorech* [online]. 1999 [cit. 2010-04-21]. ACCES: poradna EZS. Dostupné z WWW: <http://www.acces.cz/acces/poradna/detektory-pohybu.asp>.

[10] *Optoelektrické snímače* [online]. 1999 [cit. 2010-04-22]. Balluff CZ s.r.o. Dostupné z WWW: <http://www.balluff.cz/bos_principy-definice.asp>.

[11] GBS 210, [cit. 2010-04-22]. Dostupné z WWW: <http://www.centrumbezpecnosti.cz/db/files/g35_GBS_210.pdf>.

[12] JA-85, [cit. 2010-04-22]. Dostupné z WWW: <Bhttp://www.jablotron.cz/oasis/docs/manualy/JA-85B_CZ_MHP52603.pdf>.

[13] DL 500, [cit. 2010-04-22]. Dostupné z WWW: <http://www.siemens.cz/siemjetstorage/files/49569_DL500cz2.pdf>.

[14] JS-25, [cit. 2010-04-22]. Dostupné z WWW: <http://cip.inshop.cz/inshop/files/js-25.pdf>.

[15] *Komunikace po sériové sběrnici I2C* [online]. Copyright © 1998 – 2010 [cit. 2010-04-22]. Root.cz. Dostupné z WWW: <http://www.root.cz/clanky/komunikace-po-seriove-sbernici-isup2supc>.

[16] EA eDIPTFT43, [2010-4-25]. Dostupné z WWW: <http://www.lcd-module.com/eng/pdf/grafik/ediptft43-ae.pdf>.

[17] 16F505, [2010-4-25]. Dostupné z WWW: <http://ww1.microchip.com/downloads/en/DeviceDoc/41236E.pdf>.

[18] CM160200SFAYAG-I4, [2010-4-25]. Dostupné z WWW: <http://www.gme.cz/_dokumentace/dokumenty/513/513-159/dsh.513-159.1.pdf>.

[19] IQRF OS v2.09 User's Guide, [cit. 2010-04-22]. Dostupné z WWW: <http://www.iqrf.com/weben/index.php?sekce=support&id=archive&kat=35&ids=84>.

[20] BABČANÍK, Jan. *Hw.cz* [online]. 2007 [cit. 2011-04-26]. Spínané zdroje. Dostupné z WWW: <http://hw.cz/Teorie-a-praxe/ART1876-Spinane-zdroje.html>.

[21] *Communication* [online]. 2004 [cit. 2011-05-25]. BZ-COM ltd communication & embeddedsolutions. Dostupné z WWW: <http://www.bz-com.com/knowledge_base_list.asp?id=342>.