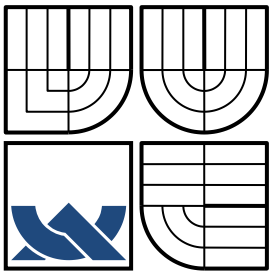
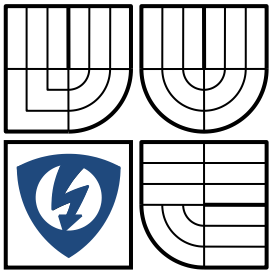


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV RADIOELEKTRONIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF RADIO ELECTRONICS

RFID PRÍSTUPOVÝ SYSTÉM V MIESTNOSTI

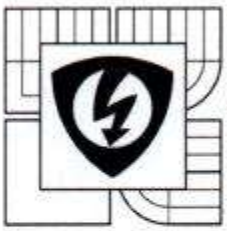
RFID BASED ACCESS SYSTEM IN ROOMS

DIPLOMOVÁ PRÁCA
MASTER'S THESIS

AUTOR PRÁCE Bc. Roman Mego
AUTHOR

VEDÚCI PRÁCE doc. Ing. Tomáš Frýza, Ph.D.
SUPERVISOR

BRNO, 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav radioelektroniky

Diplomová práce

magisterský navazující studijní obor
Elektronika a sdělovací technika

Student: Bc. Roman Mego ***ID:*** 106630
Ročník: 2 ***Akademický rok:*** 2011/12

NÁZEV TÉMATU:

RFID přístupový systém v místnosti

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s činností systémů RFID a analyzujte rizika spojené s jejich užívání . Vytvořte blokové schéma přístupového systému a také blokové zapojení v něm použitých prvků . Vyberte obvody ze kterých se bude skládat celý systém.

Navrhněte a realizujte obvodové zapojení prvků celého systému . Vytvořte potřebné knihovny budoucího softwaru pro demonstraci správné funkce jednotlivých prvků .

Vytvořte software systému , který bude obsahovat funkce pro snížení případného rizika . Proveďte detailní testování celého přístupového systému .

DOPORUČENÁ LITERATURA:

[1] FINKENZELLER, K. RFID handbook: fundamentals and application in contactless smart cards and identification, 2nd ed. Chichester: Wiley & Sons, 2003.

[2] LEHTONEN, M. et al. Securing RFID systems by detecting tag cloning [online]. 2010. [cit.: 17. prosince 2010]. Dostupné na www: http://www.springerlink.com/content/qvq80qj184k40416/fulltext.pdf.

Termín zadání: 6.2.2012 ***Termín odevzdání:*** 18.5.2012

Vedoucí práce: doc. Ing. Tomáš Frýza, Ph.D.
Konzultanti diplomové práce:

prof. Dr. Ing. Zbyněk Raida
předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob , zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č . 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé , hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Výzkum realizovaný v rámci této diplomové práce byl finančně podpořen projektem
CZ.1.07/2.3.00/20.0007 **Wireless Communication Teams**
operačního programu **Vzdělávání pro konkurenceschopnost**.

Finanční podpora byla poskytnuta Evropským sociálním fondem
a státním rozpočtem České republiky.

Abstrakt

Cieľom diplomovej práce je navrhnúť prístupový systém využívajúci technológiu RFID. Tento systém by mal znižovať bezpečnostné riziká spojené s jeho používaním. Počas riešenia boli vytvorené dve zariadenia. Prvý je prístupový terminál pracujúci na frekvencií 13,56 MHz a druhá je RFID čítačka k PC pracujúca na frekvencií 125 kHz. K nim bolo vytvorené programové vybavenie a tiež riadiaca aplikácia systému pre PC. Práca obsahuje prehľad o princípe RFID a možnosti realizácie prístupového systému. V ďalšej časti je podrobne opísaný postup návrhu obvodového zapojenia pre prvky systému. Záverečná časť opisuje vytvorený software pre prístupový terminál, v ňom použité knižnice a riadiacu aplikáciu systému pre PC.

Kľúčové slová

RFID, prístupový systém, bezpečnostné riziko, MiFare, MFRC530, EM4095, Ethernet

Abstract

The master's thesis aims to design an access control system using the RFID technology. The system should reduce security risks associated with its use. While working on project two devices were created. First is the access terminal operating on frequency of 13.56 MHz and second is the RFID reader for PC operating at frequency 125 kHz. Software for devices was created as well as system control application for PC. The document contains an overview of the RFID principles and possibility of implementation access control system. Next part of the project describes in detail step by step the process of designing electrical circuit for system parts. Last part talks about realized software, libraries which are used and the system control application for PC.

Keywords

RFID, access control, security risk, MiFare, MFRC530, EM4095, Ethernet

Bc. Mego, Roman. *RFID prístupový systém v miestnosti*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2012. 52 s. Vedúci diplomovej práce doc. Ing. Tomáš Frýza, Ph.D.

Prehlásenie

Prehlasujem, že svoju diplomovú prácu na tému RFID prístupový systém v miestnosti som vypracoval samostatne pod vedením vedúceho diplomovej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomý následkov porušenia ustanovení § 11 a nasledujúcich autorský zákona č. 121/2000 Zb., vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovení § 152 trestného zákona č. 140/1961 Zb.

V Brne dňa 18. mája 2012 .....

podpis autora

Poďakovanie

Ďakujem vedúcemu diplomovej práce doc. Ing. Tomášovi Frýzovi, Ph.D. za účinnú metodickú, pedagogickú a odbornú pomoc a ďalšie cenné rady pri spracovaní mojej diplomovej práce.

V Brne dňa 18. mája 2012 .....

podpis autora

Obsah

Úvod ... 1
1 Technológia RFID ... 2
1.1 Rozdelenie systémov RFID ... 2
1.1.1 Napájanie RFID transpondérov ... 2
1.1.2 Frekvencie používané v RFID ... 3
1.1.3 Druh pamäte ... 3
1.1.4 Zabezpečenie komunikácie ... 3
1.2 Možné riziká použitia RFID ... 4
1.2.1 Znemožnenie čítania transpondéru ... 4
1.2.2 Neoprávnené použitie transpondéru ... 5
1.2.3 Kopírovanie transpondérov ... 5
1.2.4 Sledovanie komunikácie terminál - server ... 6
1.2.5 Mechanické poškodenie terminálu ... 6
1.3 Ochrana pred možnými rizikami ... 6
2 Návrh prístupového systému ... 7
2.1 Topológia systému ... 7
2.1.1 Vytvorenie autonómnych terminálov ... 7
2.1.2 Prepojenie pomocou sériovej linky ... 7
2.1.3 Využitie už vybudovanej komunikačnej siete ... 8
2.2 Výber protokolu RFID ... 8
2.2.1 Pracovná frekvencia 125 kHz ... 8
2.2.2 Pracovná frekvencia 13,56 MHz ... 9
2.3 Časti systému ... 10
2.3.1 RFID čítačka k PC ... 10
2.3.2 Prístupový terminál ... 12
3 Návrh zapojenia ... 18
3.1 Čítačka RFID tagov k PC ... 18
3.1.1 Obvod EM4095 ... 18
3.1.2 Prevodník USB/UART ... 21
3.1.3 Mikrokontrolér ... 22
3.2 Prístupový terminál ... 22
3.2.1 Obvod MFRC530 ... 23
3.2.2 Obvod ENC424J600 ... 25
3.2.3 LCD displej ... 26
3.2.4 Klávesnica ... 27
3.2.5 Prevodník RS232/UART ... 27
3.2.6 Pamäť flash ... 27
3.2.7 Ovládanie zámku dverí ... 28
3.2.8 Detekcia poškodenia ... 28

3.2.9 Napájanie ... 28
3.2.10 Mikrokontrolér ... 31
4 Softwarová obsluha periférií ... 32
4.1 Ovládanie EM4095 ... 32
4.1.1 Inicializácia ... 32
4.1.2 Prijímanie demodulovaného signálu ... 32
4.1.3 Formát prijímaných dát ... 33
4.2 Ovládanie MFRC530 ... 33
4.2.1 Inicializácia ... 33
4.2.2 Práca s registrami ... 33
4.2.3 Zásobník FIFO ... 34
4.2.4 Spúšťanie príkazov ... 34
4.2.5 Prenos medzi MFRC530 a tagom ... 34
4.2.6 Komunikácia s tagmi MiFare ... 35
4.3 Ovládanie ENC424J600 ... 35
4.3.1 Inicializácia ... 36
4.3.2 Odoslanie paketu ... 37
4.3.3 Prijatie paketu ... 37
4.4 Ovládanie LCD ... 39
4.5 Ovládanie klávesnice ... 39
4.6 Flash pamäť ... 39
5 Program terminálu ... 40
5.1 Program ako celok ... 40
5.2 Stavový automat ... 41
5.3 Komunikácia pomocou TCP/IP ... 42
5.3.1 Aplikačná vrstva TCP/IP ... 43
5.3.2 Zabezpečenie prenosu ... 44
5.4 Servisný port ... 45
6 Aplikácia pre server ... 47
6.1 Databáza ... 47
6.2 Komunikácia s terminálmi ... 48
6.3 Spracovanie požiadavky ... 48
6.4 Užívateľské prostredie ... 50
7 Záver ... 51
Použitá literatúra ... 53
Zoznam príloh ... 56

Zoznam obrázkov

Obr. 1.1: Napájanie pasívneho RFID tagu 3
Obr. 1.2: Rozdelenie systémov podľa funkčnosti (prevzaté z [2]) 4
Obr. 1.3: RFID transpondér v prevedení ISO karty s vyznačením sériového čísla 6
Obr. 2.1: Rozloženie systému s použitím RS-485 7
Obr. 2.2: Prístupový systém využívajúci LAN 8
Obr. 2.3: Bloková schéma čítačky k PC 10
Obr. 2.4: Modul firmy Parallax (Foto: Parallax) 10
Obr. 2.5: Modul ID-12 (Foto: ID Innovations) 11
Obr. 2.6: Bloková schéma RFID terminálu 12
Obr. 2.7: Modul MM-U57D (Foto: Netronix) 13
Obr. 2.8: Modul Nano SocketLAN (Foto: ConnectOne) 14
Obr. 2.9: Modul EG-SR-7100A (Foto: WIZnet) 14
Obr. 2.10: Modul XPort (Foto: Lantronix) 15
Obr. 3.1: Odporúčané zapojenie EM4095 (prevzaté z [19]) 18
Obr. 3.2: Význam označenia rozmerov cievky 19
Obr. 3.3: Zapojenie prevodníku USB/UART (prevzaté z [22]) 22
Obr. 3.4: Typické zapojenie MFRC530 (prevzaté z [23]) 23
Obr. 3.5: Rozloženie cievky pre anténu 24
Obr. 3.6: Pripojenie oddeľovacieho transformátora k ENC424J600 (prevzaté z [25]) ... 26
Obr. 3.7: Zapojenie MAX3232 (prevzaté z [26]) 27
Obr. 3.8: Zapojenie tranzistorového spínača 28
Obr. 3.9: Typické zapojenie TPS23750 (prevzaté z [27]) 29
Obr. 3.10: Náhradná schéma TL431 (prevzaté z [28]) 30
Obr. 3.11: Získanie napájacieho napätia 30
Obr. 4.1: Princíp dekódovania Manchestru 32
Obr. 4.2: Formát výstupných dát (prevzaté z [30]) 33
Obr. 4.3: Byte udávajúci adresu registra MFRC530 33
Obr. 4.4: Formát odosielaného obsahu s automatickým dopĺňaním 37
Obr. 4.5: Rozloženie prijatého paketu v pamäti (prevzaté z [25]) 38
Obr. 5.1: Vývojový diagram hlavného behu programu 41
Obr. 5.2: Stavový diagram automatu v termináli 42
Obr. 5.3: Zobrazované informácie pomocou HTTP 43
Obr. 5.4: Komunikácia pri kontrole stavu 43
Obr. 5.5: Komunikácia počas prístupu užívateľa 44
Obr. 5.6: Zachytená komunikácia medzi terminálom a serverom 45
Obr. 5.7: Komunikácia pomocou servisného portu 46
Obr. 6.1: Algoritmus vyhodnocovania prístupu užívateľa 49
Obr. 6.2: Užívateľské prostredie správy terminálov 50
Obr. 6.3: Užívateľské prostredie správy užívateľov 50

Zoznam tabuliek

Tabuľka 2.1: Mikrokontroléry vhodné na použitie 11
Tabuľka 2.2: Porovnanie integrovaných obvodov rady MFRC 13
Tabuľka 2.3: Prehľad Ethernetových modulov 14
Tabuľka 2.4: Ethernetové radiče firmy Microchip 15
Tabuľka 2.5: Vzorka lacných 32-bitových mikrokontrolérov 17
Tabuľka 3.1: Pripojenie portov mikrokontroléra PIC 22
Tabuľka 3.2: Zapojenie MFRC530 pre SPI 24
Tabuľka 3.3: Voľba triedy zariadenia 29
Tabuľka 3.4: Pripojenie portov mikrokontroléra STM32 31
Tabuľka 5.1: Uložené nastavenia v pamäti flash 40
Tabuľka 6.1: Štruktúra tabuľky obsahujúcej zoznam terminálov 47
Tabuľka 6.2: Štruktúra tabuľky obsahujúcej zoznam užívateľov 47
Tabuľka 6.3: Štruktúra tabuľky priradenia užívateľa s terminálom 47
Tabuľka 6.4: Štruktúra tabuľky záznamu akcií 48

Úvod

Skratka RFID pochádza z anglického výrazu Radio-Frequency Identification, ktorá ako z názvu vyplýva označuje technológiu pre rádiovú identifikáciu. V posledných rokoch sa tento druh identifikácie dostal do rôznych oblastí ako napríklad správa majetku, logistika, prístupové systémy alebo aj bezhotovostné platby.

Cieľom práce je navrhnúť prístupový systém, ktorý bude túto technológiu využívať a tiež vytvoriť prvky v ňom používané. Tento systém by mal byť navrhnutý tak, aby bolo možné znížiť bezpečnostné riziká spojené s jeho využívaním.

Počas riešenia projektu budú navrhnuté a realizované obvodové zapojenia prístupového terminálu a jednoduchej RFID čítačky k PC. K nim bude vytvorený firmware pre použité mikrokontroléry. Tiež sa vytvorí aplikácia pre PC, pomocou ktorej sa budú spravovať prístupové body v systéme a aj jeho užívateľov.

Prvá časť práce sa zaoberá princípom činnosti technológie RFID. Tiež sú tu spomenuté možné riziká spojené s jej používaním, ako aj možnosti ako tieto riziká obmedziť. V druhej časti je pohľad na prístupový systém ako na celok. Spomínajú sa v nej možné riešenia systému a vlastnosti prvkov z ktorých sa skladajú. Pri návrhu prvkov je uvedený postup pre dve možné varianty RFID. Druhá polovica práce sa zaoberá tvorbou programového vybavenia. V časti opisujúcej tvorbu firmwaru sú spomenuté princípy pre komunikáciu s pripojenými periférami. Je tiež opísaný použitý protokol pre komunikáciu terminálu po sieti. Na záver sú ukázané možnosti vytvorenej riadiacej aplikácie.

1 Technológia RFID

Pri RFID systémoch dochádza k identifikácií objektov obsahujúcich transpondér bez potreby priameho kontaktu. Ich výhodou je že nie je potrebná ich presná poloha ako napríklad pri identifikácií pomocou čiarových kódov. Stačí aby bol transpondér v dosahu čítačky. Ten sa môže pohybovať v rozsahu jednotiek centimetrov po jednotky metrov.

V tejto kapitole bude bližšie uvedený princíp na akom systémy RFID pracujú, ich rozdelenie podľa funkcie a tiež ich výhody, prípadne nevýhody.

1.1 Rozdelenie systémov RFID

Systémy RFID je možné deliť podľa nasledujúcich kritérií:

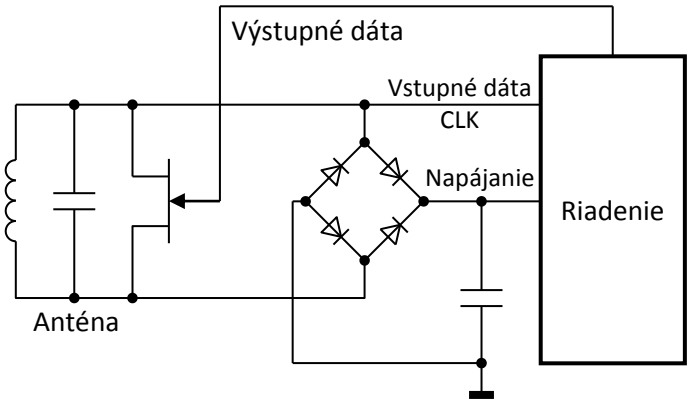
- spôsob získavania energie pre vlastnú činnosť
- pracovná frekvencia
- druh pamäte
- zabezpečenie komunikácie

1.1.1 Napájanie RFID transpondérov

Základom RFID transpondéru je integrovaný obvod kombinovaný s anténou, ktorý prenáša požadované informácie do čítačky. Podľa toho ako získavajú potrebnú energiu je ich možné deliť na aktívne a pasívne.

Pri aktívnych transpondéroch je napájanie riešené klasicky, ako pri väčšine elektronických obvodov. Sú buď batériovo napájané alebo využívajú iný napájací adaptér. Príkladom môže byť jednotka umiestnená v automobiloch slúžiaca pre mýtny systém.

Pasívne RFID transpondéry nemajú vlastný zdroj, ani možnosť sa k nemu pripojiť. Namiesto toho získavajú energiu zo svojho okolia. Tá je pochopiteľne najväčšia v elektromagnetickom poli v okolí čítačky. Takéto transpondéry sa často vyskytujú vo forme kariet alebo príveskov na kľúče. Princíp napájania je zobrazený na obr. 1.1.



Obr. 1.1: Napájanie pasívneho RFID tagu

1.1.2 Frekvencie používané v RFID

Pre technológiu RFID platia rôzne štandardy a podľa nich sa mení aj pracovná frekvencia. Od nej závisí rýchlosť prenosu dát, ale aj vzdialenosť na akú je možné komunikovať. Medzi používané frekvencie podľa [1] patria:

- 125 kHz / 134 kHz (ISO 18000-2)
- 13,56 MHz (ISO 18000-3)
- 2,45 GHz (ISO 18000-4)
- 5,8 GHz (ISO 18000-5)
- 860 MHz – 930 MHz (ISO 18000-6)
- 433,92 MHz (ISO 18000-7)

1.1.3 Druh pamäte

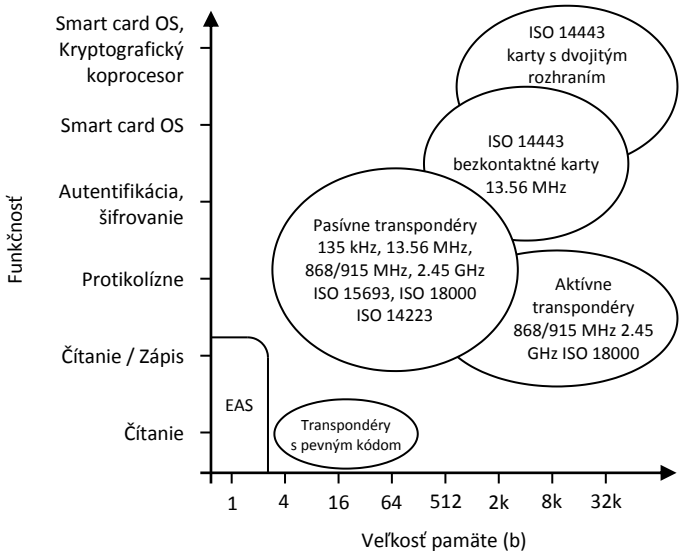
Pamäť RFID transpondéru môže určená len na čítanie, alebo je možné aj do nej zapisovať. Špeciálnym prípadom môžu byť obvody ktoré obsahujú senzory a na základe ich stavu upravujú odosielané informácie (napr. informácia o teplote). Transpondéry na ktoré je možné informácie aj zapisovať majú väčšinou časť pamäte pevnú s predprogramovaným sériovým číslom, aby bolo možné obvod jednoznačne identifikovať.

1.1.4 Zabezpečenie komunikácie

Pri najjednoduchších systémoch začne transpondér vysielať dáta hneď ako sa dostane do blízkosti čítačky. V prípade že by sa ich v tomto priestore nachádzalo viac, došlo by ku kolízii. Zložitejšie systémy obsahujú antikolízne protokoly vďaka ktorým je možné čítať aj z transpondérov ktoré sú blízko pri sebe.

Ďalšie možné zabezpečenie s ktorým je možné sa stretnúť je ochrana heslom. To je obsiahnuté v transpondéroch na ktoré je možné zapisovať. Heslo je vyžadované pri čítaní alebo zapisovaní podľa použitého systému. Pri systémoch s vysokou požiadavkou na bezpečnosť sú prenášané dáta navyše šifrované.

Na obrázku (obr. 1.2) je znázornené rozdelenie RFID systémov podľa vyššie uvedených vlastností.



Obr. 1.2: Rozdelenie systémov podľa funkčnosti (prevzaté z [2])

1.2 Možné riziká použitia RFID

Napriek tomu že RFID systémy majú svoje výhody, je potrebné počítať aj s možnými rizikami pri ich používaní. Tie bývajú prevažne spojené s úmyselným napadnutím systému za účelom jeho obídenia alebo znefunkčnenia. Touto problematikou sa podrobnejšie zaoberá [3] a preto budú riziká spojené s ich užívaním spomenuté len okrajovo. Riziká sú nasledujúce:

- Znemožnenie čítania transpondéru
- Neoprávnené použitie transpondéru
- Kopírovanie transpondéru
- Sledovanie komunikácie terminál – server
- Mechanické poškodenie terminálu

1.2.1 Znemožnenie čítania transpondéru

Znemožnenie čítania transpondéru je možné dvoma spôsobmi. Buď nie je možné čítať z neho dáta trvalo alebo len dočasne. V prvom prípade dochádza k trvalému poškodeniu riadiaceho čipu alebo antény. To sa dá ľahko zariadiť jeho mechanickým poškodením. Transpondér je tiež možné poškodiť bez známok fyzického poškodenia silným energetickým impulzom ktorý zničí vnútornú štruktúru integrovaného obvodu [4]. Niektoré transpondéry je tiež možné znehodnotiť odoslaním príkazu KILL.

Pre dočasné znefunkčnenie je možné transpondér obaliť vodivým materiálom a tak vytvoriť Faradayovu klietku. Druhá možnosť je rušenie komunikácie vytvorením signálu ktorý bude interferovať so signálom medzi čítačkou a transpondérom. To sa

môže stať aj neúmyselne ak sa v blízkosti čítačky nachádza zariadenie pracujúce na blízkej frekvencií ako RFID systém.

Tieto metódy majú dopad na bezpečnosť v systémoch ktoré sú využívané v obchodoch pri strážení tovaru. Na ostatné majú skôr vplyv na ich spoľahlivosť.

1.2.2 Neoprávnené použitie transpondéru

Táto udalosť by mohla nastať v prípade krádeže alebo straty transpondéru. Vtedy by neoprávnená osoba mohla bez vynaloženia námahy obísť systém pomocou cudzej identity.

1.2.3 Kopírovanie transpondérov

Prípad kopírovania je podobný predchádzajúcemu bodu. Rozdiel je v tom, že je potrebné dostatočné technické vybavenie. Niektorá literatúra uvádza, že jednou z výhod RFID systémov je nemožnosť kopírovania transpondérov, pretože obsahujú sériové číslo v časti pamäti ktorú nie je možné prepísať. Tým pádom je nemožné vytvoriť dva rovnaké transpondéry ich modifikáciou. Túto skutočnosť udáva aj [2]. Z toho by sa dalo usudzovať, že sú z tohto hľadiska RFID systémy bezpečné. Je tu však možnosť ako vytvoriť kópiu transpondéru a to jeho emuláciou. Na internete je možné nájsť mnoho zapojení ktoré majú túto funkciu. Ako príklad je uvedený jednoduchý projekt „Unique (EM4001) RFID Emulator“ [5].

Pri použití emulátora je ešte potrebné poznať údaje ktoré sú do čítačky prenášané. Ako príklad sa použije emulátor spomenutý v [5]. Transpondéry využívajúce protokol EM4001 pracujú na frekvencií f = 125 kHz. Podľa druhu obvodu je jeden bit odoslaný v časoch $64/f$, $32/f$ alebo $16/f$. Najčastejšie je možné stretnúť sa s obvodmi ktoré odošlú jeden bit v čase $64/f$ = 512 µs. Celá odosielaná sekvencia je dlhá 64 bitov, takže sa odošle za čas $64 \cdot 64/f$ = 32,768 ms.

Z celkovej dĺžky odosielanej sekvencie je 10 bitov pevných ktoré udávajú jej začiatok a koniec, 14 bitov redundantných pre identifikáciu správnosti prenosu a zvyšných 40 bitov je nezávislých a udáva sériové číslo karty. Ak by sa použila metóda brute-force, tak by sa všetkých 2^{40} možností odoslalo za $2^{40} \cdot 64 \cdot 64/f \approx 1142$ rokov. V tomto prípade je malá pravdepodobnosť úspešnosti útoku.

Po zakúpení RFID kariet z tej istej série bolo zistené, že prvé 3 bajty ich sériových čísel boli rovnaké. Ak by mal útočník informáciu o sérií z ktorej sú karty v systéme registrované, stačilo by mu vyskúšať 2^{16} možností. V takomto prípade by testovanie možných kombinácií prešlo za necelých 36 minút.

Posledná možnosť je priame zistenie kódu transpondéra. To je možné pomocou ručnej čítačky aj bez vedomia užívateľa, prípadne pohľadom na transpondér ktorý má na sebe uvedené sériové číslo.

Obr. 1.3: RFID transpondér v prevedení ISO karty s vyznačením sériového čísla

Kopírovanie transpondérov v poslednej dobe nie je len záležitosťou lacnejších systémov. Začínajú sa objavovať metódy akým obchádzať systémy používané v aplikáciách, ktoré vyžadujú vysoký stupeň zabezpečenia. Príkladom je projekt „OpenPCD“ [6] emulujúci ISO 14443, ISO 15693 alebo protokol MiFare. Niektoré štáty používajú tieto štandardy napríklad v elektronických pasoch.

1.2.4 Sledovanie komunikácie terminál - server

RFID systémy bývajú často prepojené s databázou, podľa ktorej vyhodnocujú dáta načítané z tagov. V prípade že by táto komunikácia prebiehala pomocou prístupného média (počítačová sieť, bezdrôtové pripojenie), dala by sa táto komunikácia odpočúvať, analyzovať a zistené informácie využiť v prospech útočníka.

1.2.5 Mechanické poškodenie terminálu

Ako posledný uvedený prípad je mechanické poškodenie terminálu. Ten je významný pri prístupových systémoch. Ak terminál v sebe obsahuje napríklad relé ktoré ovláda zámok dverí, dá sa po odstránení krytu premostiť vodičom a tak zámok odomknúť.

1.3 Ochrana pred možnými rizikami

Zabezpečenie systému závisí hlavne od jeho využívania a požiadavky na jeho bezpečnosť. Medzi spôsoby ako by bolo možné znížiť riziká spomenuté vyššie patrí:

- fyzická kontrola na strategických miestach
- dodatočné overenie pomocou iného parametra
- detekcia skopírovania transpondéra
- obmedzenie čítania po priložení neregistrovaného transpondéra
- používanie šifrovanej komunikácie
- zvýšenie mechanickej odolnosti / detekcia poškodenia terminálu

2 Návrh prístupového systému

Nasledujúca kapitola sa bude zaoberať návrhom prístupového systému ktorý bude využívať technológiu RFID pre overenie osoby ktorá chce vstúpiť do miestnosti. V návrhu by sa mali zohľadniť skutočnosti vďaka ktorým by mohla neoprávnená osoba tento systém obísť.

2.1 Topológia systému

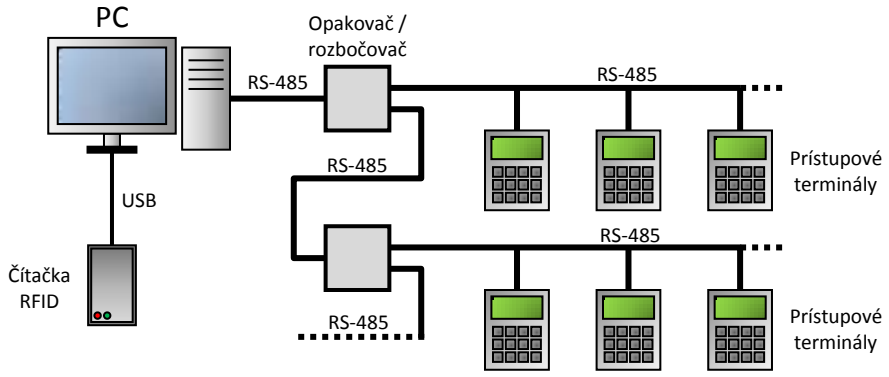
Aby bolo možné navrhnúť prvky systému, musí sa určiť ako bude tento systém fungovať ako celok.

2.1.1 Vytvorenie autonómnych terminálov

Prvou možnosťou je, že by bol pri každej zabezpečenej miestnosti autonómny terminál. Jeho funkcia by spočívala v načítaní kódu a jeho porovnaní s kódmi uloženými v jeho pamäti. Toto riešenie by bolo jednoduché. Problém by nastal, ak by sa v budove nachádzalo viac terminálov a bolo by potrebné často meniť prístupové práva. V tom prípade by sa muselo ku každému terminálu pristúpiť osobne a zmeniť ich obsah pamäte. Ďalšou veľkou nevýhodou je tá, že by nebolo možné vytvoriť funkcie pre vyššiu bezpečnosť systému. Toto riešenie je v rozpore zo zadaním.

2.1.2 Prepojenie pomocou sériovej linky

Keď bude mať terminál možnosť pripojenia pomocou sériovej linky, bude možná jeho vzdialená správa pomocou PC. Ak by sa navyše použilo rozhranie RS-485, môže byť na ňom použitých 32 zariadení. Podľa [7] pri zvýšení vstupnej impedancie prijímačov, prípadne po použití opakovačov počet zariadení môže stúpnuť na 128.

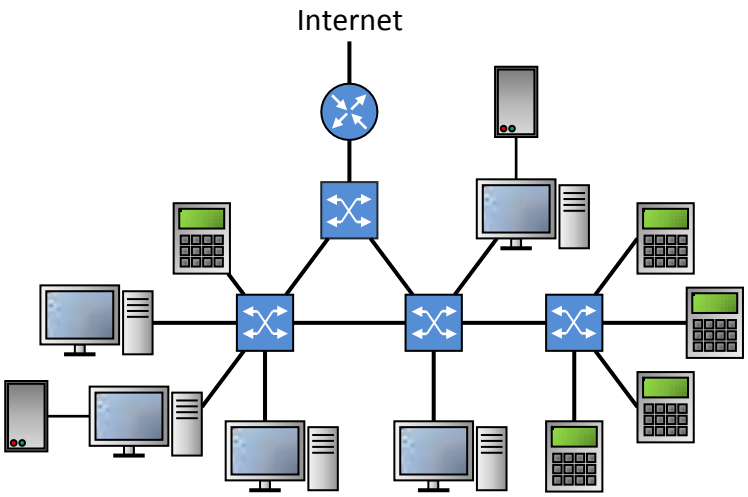


Obr. 2.1: Rozloženie systému s použitím RS-485

Nevýhodou tohto riešenia je potreba natiahnutia novej kabeláže v budove. Výhoda z hľadiska bezpečnosti spočíva v oddelenom prenosovom médiu použitom pre komunikáciu. Ak bude fyzicky ťažko dostupné, bude aj monitorovanie komunikácie tiež sťažené.

2.1.3 Využitie už vybudovanej komunikačnej siete

Väčšina budov vyžadujúcich rozsiahly prístupový systém obsahuje vybudovanú počítačová sieť. Tieto siete sú založené na technológií Ethernet. Takáto sieť by sa dala doplniť o potrebné prvky a nebolo by potrebné budovať všetko od základov.



Obr. 2.2: Prístupový systém využívajúci LAN

V takomto riešení je možné použiť prakticky neobmedzený počet terminálov. Takisto tu nie je obmedzenie maximálnej vzdialenosti na akú je možné systém použiť. Ak je využitá technológia Ethernet, je tiež možné využiť možnosť napájania pomocou kabeláže po ktorej sa prenášajú dáta.

Takéto riešenie prináša univerzálnosť. Je potrebné počítať s tým, že systém bude viditeľný pre ostatných užívateľov siete a tak sa to musí zohľadniť pri vytváraní softwarovej časti.

2.2 Výber protokolu RFID

Pred samotným návrhom zapojenia je potrebné zvoliť protokol na akom bude RFID systém založený. Pre podobné identifikačné systémy sa využívajú štandardy pracujúce na frekvencií 125 kHz alebo 13,56 MHz.

2.2.1 Pracovná frekvencia 125 kHz

Pre túto frekvenciu je na trhu dostupných niekoľko možných štandardov. Tie sú väčšinou označované podľa názvu obvodu ktorý je použitý pri konštrukcií tagu. Medzi ne patria napríklad:

- EM4001, EM4002, EM4100, EM4102, GK4001...
- EM4450 [8]
- T5557 [9]
- Hitag 2 [10]

Obvody EM4001 a s nimi kompatibilné patria medzi najjednoduchšie. Obsahujú 64b pamäte z ktorej sa dá len čítať. Tá obsahuje jedinečné číslo karty. Transpondéry sa vyrábajú v rôznych prevedeniach. V jeho prospech hrá ľahká dostupnosť na trhu ako obvodov potrebných pre konštrukciu čítačky, tak aj dostupnosť samotných transpondérov. Výhodná je tiež ich cena vďaka ich rozšírenému používaniu. Na trhu sa začínajú objavovať aj obvody s dvojnásobnou pamäťou (EM4200).

Obvody EM4450 majú pamäť 1kb do ktorej je možné zapisovať. Čítanie a zápis môžu byť chránené heslom. V dnešnej dobe sú tieto obvody málo používané a tiež ich dostupnosť je horšia. Výhodou je, že pri vhodnom zapojení je možné čítačku pre EM4001 upraviť pre tieto obvody len zmenou programu.

T5557 má podobné vlastnosti ako EM4450. Rozdiel je v jeho menšej pamäti (330b). Navyše obsahuje ochranu proti kolízií.

Hitag sa často využíva v automobilovom priemysle. Transpondér je umiestnený v kľúči od vozidla a slúži na odblokovanie imobilizéru. Do jeho pamäte je možné zapisovať, zápis je chráneným heslom a dáta sú šifrované. V prípade Hitag2 sa využíva prúdová šifra využívajúca 48-bitový lineárny spätnoväzobný posuvný register. Presný šifrovací algoritmus nie je výrobcom zverejnený a preto je potrebné na konštrukciu čítačky zakúpiť špeciálny obvod.

2.2.2 Pracovná frekvencia 13,56 MHz

Na tejto frekvencií sú na trhu dostupné systémy s technológiou MiFare. Táto technológia sa využíva pre aplikácie s vyššími požiadavkami pre zabezpečenie. Obvody pre transpondéry sú vyhotovené v rôznych variantoch odlišujúcich sa veľkosťou pamäte. Pre MiFare Classic šifrovací algoritmus označovaný ako Crypto-1 nie je výrobcom zverejnený a preto sa musí pre konštrukciu čítačky zakúpiť špeciálny obvod. Viac o jednotlivých prevedeniach RFID tagov je možné nájsť na stránkach výrobcu [11].

Pre vytvorenie prístupového systému je zvolená technológia RFID s pracovnou frekvenciou 13,56 MHz. Pre jej výber hrala úloha hlavne vyššia miera zabezpečenia, pretože pre jej oklamanie je potrebné lepšie technické vybavenie. Tiež zatiaľ nie je na internete veľa dostupných postupov ako obísť takéto zabezpečenie. Vyššia bezpečnosť so sebou prináša aj vyššiu cenu.

Pre demonštračné účely je tiež možné vytvoriť jednoduchú čítačku pre RFID tagy s pracovnou frekvenciou 125 kHz. Tá bude slúžiť hlavne pre porovnanie náročnosti vytvorenia systémov založených na dvoch rôznych technológiách. Tiež sa môžu porovnať ich vlastnosti pri činnosti.

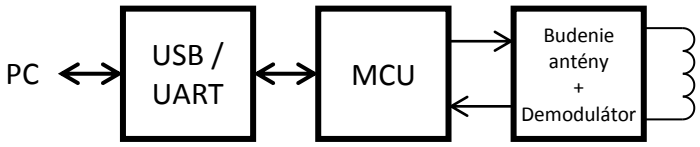
2.3 Časti systému

Bolo rozhodnuté, že systém bude využívať lokálnu sieť postavenej na technológií Ethernet. Z jeho rozloženia (obr. 2.2) je možné vidieť, že je potrebné navrhnúť dva prvky:

- RFID čítačka k PC
- Terminál riadiaci prístup do miestnosti

2.3.1 RFID čítačka k PC

Úlohou čítačky k PC bude načítavať čísla transpondérov a predávať ich aplikácií pre registráciu užívateľov. Keďže zariadenie bude vykonávať len túto jednu funkciu, nebude náročné na obvodové zapojenie ani na výpočtový výkon. Jeho bloková schéma je znázornená na obr. 2.3.



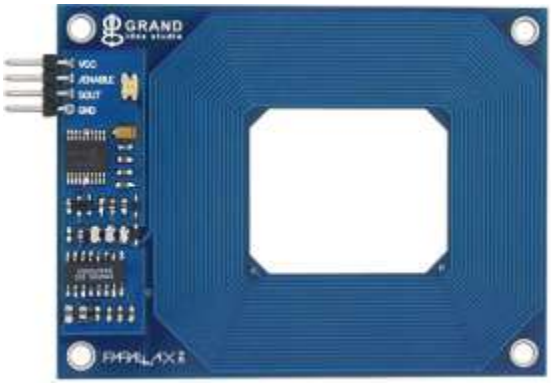
Obr. 2.3: Bloková schéma čítačky k PC

V tejto práci bude pre demonštračný účel použitá RFID technológia s frekvenciou 125 kHz.

2.3.1.1 RFID modul

Základom je modul ktorý sprostredkováva komunikáciu s transpondérom. Ten obsahuje budič antény s demodulátorom a samotnú anténu. V tomto kroku návrhu sa ponúkajú dve možnosti a to zakúpiť už hotový modul alebo ho vytvoriť.

Hodové moduly sa vyrábajú buď vo forme zapojenia realizovaného na plošnom spoji alebo ako zaliate obvody určené pre montáž plošného spoja. Tie už obsahujú aj mikrokontrolér, ktorý spracováva prijaté dáta a odosiela ich pomocou sériovej linky. Prvá varianta je nevýhodná z hľadiska svojich rozmerov a konštrukcie. Ako zástupca bol vybraný modul od firmy Parallax, ktorého rozmery sú 62,2mm x 82,5mm (obr. 2.4).



Obr. 2.4: Modul firmy Parallax (Foto: Parallax)

Zástupca z druhej skupiny je modul ID-12 od firmy ID-Innovations (obr. 2.5). Jeho rozmery sú 25mm x 26mm. Keďže je navrhnutý pre montáž do plošného spoja, nie je potrebné špeciálne riešiť jeho mechanické uchytenie.

Obr. 2.5: Modul ID-12 (Foto: ID Innovations)

Tieto moduly majú nevýhodu v tom, že sú určené len pre komunikáciu s transpondérmi EM4001 a s nimi kompatibilnými. V prípade potreby je nemožné zmeniť ich funkciu. Z tohto dôvodu je zvolená možnosť vytvorenia vlastného zapojenia.

Pre tento účel je možné zohnať integrované obvody navrhnuté priamo pre konštrukciu RFID čítačiek. Medzi najdostupnejšie patria EM4095 (dostupné v [12]) a U2270B (dostupné v [12] a [13]). Oba tieto obvody obsahujú výstupné budiče pre anténu a demodulátor signálu vytváraného transpondérom. Tiež je možné s oboma zapisovať do transpondérov ktoré to umožňujú.

Vzhľadom na to že s oboma obvodmi je možné realizovať tie isté funkcie s približne tým istým množstvom externých súčiastok rozhodujúca pre výber bude cena. Tá je pri obvode EM4095 mierne nižšia.

2.3.1.2 Mikrokontrolér

Účel mikrokontroléra bude riadenie RFID modulu, spracovanie prijatých dát a ich následné odoslanie pomocou sériovej linky. Impulzy v prijímanom signáli môžu mať minimálnu šírku od 64 µs do 256 µs v závislosti na použitom tagu. Ak by bolo potrebných 64 inštrukčných cyklov na spracovanie polovice bitu kódu Manchester, stačil by v najrýchlejšej variante tagu výpočtový výkon 1 MIPS. Pre tento účel postačí jednoduchý 8-bitový mikrokontrolér. Tabuľka 2.1 obsahuje porovnanie obvodov ktoré by bolo možné použiť na ovládanie zariadenia. Od troch výrobcov bol vybraný jeden z nižšej rady u ktorého sa predpokladalo že by túto funkciu zvládol. Všetky obsahujú časovač s funkciou capture a UART (u Freescale označovaný ako SCI).

Tabuľka 2.1: Mikrokontroléry vhodné na použitie

Výrobca	Rodina	Názov	Prog. pamäť	RAM	Interný oscilátor	Puzdro	Cena
Atmel	AVR	ATmega48A	4 kB	512 b	8 MHz	TQFP32	2,54 €
Freescale	HC08	MC908QB4	4 kB	128 b	8 MHz	SOIC16	2,87 €
Microchip	PIC16	PIC16F628A	3,5 kB	224 b	4 MHz	SOIC16	2,44 €

Pre ovládanie čítačky k PC bol vybraný mikrokontrolér PIC16F628A. Pri jeho výbere zohrávala svoju úlohu cena, ale aj skúsenosti s týmito obvodmi vďaka čomu sa môže

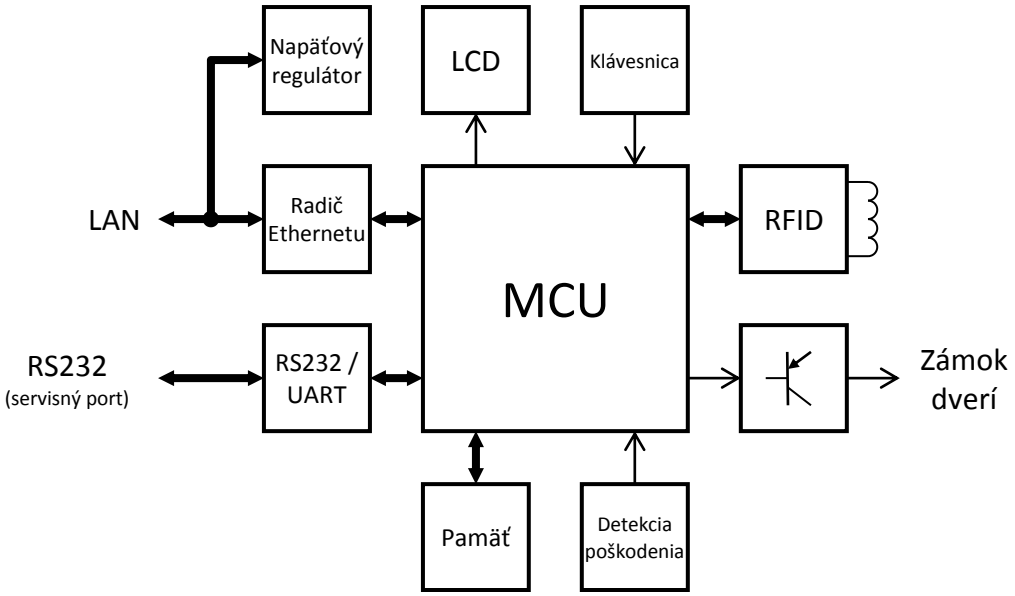
doba vývoja skrátiť. Mikrokontrolér bude doplnený o prevodník USB-UART realizovaný obvodom FT232RL. Pri komunikovaní pomocou USB nebude potrebné navrhovať napájací zdroj.

2.3.2 Prístupový terminál

Na funkciu terminálu sú vyššie nároky, pretože musí zvládať nasledujúce funkcie:

- Komunikácia s RFID transpondérmi
- Komunikácia pomocou Ethernetu
- Komunikácia s užívateľom
- Ovládanie zámku dverí
- Detekcia poškodenia

Všetky časti nachádzajúce sa v termináli sú znázornené v blokovej schéme (obr. 2.6).



Obr. 2.6: Bloková schéma RFID terminálu

2.3.2.1 RFID modul

Tak ako pre technológiu pracujúci na frekvencií 125 kHz, tak aj pre 13,56 MHz sú na trhu dostupné už hotové moduly. Tie sú väčšinou vytvorené ako hotové zapojenie na plošnom spoji. Prvým príkladom je modul MM-U57D [14] od firmy Netronix (obr. 2.7). Jedná sa o modul založený na integrovanom obvode MFRC500 doplnený o riadiaci mikrokontrolér vďaka ktorému je možné s ním komunikovať cez sériovú linku UART. Medzi nevýhodu patrí že neobsahuje anténu a tak by sa musela navrhnúť zvlášť.

Obr. 2.7: Modul MM-U57D (Foto: Netronix)

Ďalším zástupcom pre hotové moduly je SB2240MC [15] od firmy SunBest. Podobne ako MM-U57D je tiež založený na obvode MFRC500. Navyše obsahuje anténu, takže je možné ho ihneď použiť bez potreby ďalšieho návrhu.

Keďže je väčšina dostupných modulov založená na integrovaných obvodoch MFRC500, môže sa vytvoriť vlastný návrh s podobným zapojením. Toto riešenie je z cenového hľadiska najlepšie.

Obvody MFRC500 slúžia pre bezkontaktnú komunikáciu na frekvencií 13,56 MHz. Ich výrobcom je NXP Semiconductors. V jeho ponuke sú aj podobné obvody ako napríklad MFRC530, MFRC531, MFRC522 a MFRC523. Rozdiely medzi nimi ukazuje tabuľka 2.2. Viac informácií o obvodoch je možné nájsť na stránkach výrobcu [16].

Tabuľka 2.2: Porovnanie integrovaných obvodov rady MFRC

Označenie	Operačná vzdialenosť	Komunikačné rozhranie	Komunikačná rýchlosť [kbit/s]	Štandard	Napájacie napätie
MFRC500	100 mm	8bit paralel, SPI	106	ISO14443A	5 V
MFRC530	100 mm	8bit paralel, SPI	106 / 212 / 424	ISO14443A	3,3V / 5V
MFRC531	100 mm	8bit paralel, SPI	106 / 212 / 424	ISO14443A ISO14443B	3,3V / 5V
MFRC522	70 mm	SPI, I2C, UART	106 / 212 / 424 / 848	ISO14443A	3,3 V
MFRC523	70 mm	SPI, I2C, UART	106 / 212 / 424 / 848	ISO14443A ISO14443B	3,3 V

Z dôvodu dostupnosti bol vybraný obvod MFRC530. Ak by bola žiadaná zmena, tak obvody MFRC500, 530 a 531 sú medzi sebou pinovo kompatibilné.

2.3.2.2 Komunikácia po Ethernete

Pre pripojenie terminálu do lokálnej siete je možné využiť už hotové moduly, ktoré už podporujú rôzne protokoly. To je výhoda z hľadiska šetrenia výpočtového výkonu mikrokontroléra.

Tabuľka 2.3: Prehľad Ethernetových modulov

Výrobca	Názov	Podporované protokoly	Cena
ConnectOne	Nano SocketLAN	ARP, ICMP, IP, UDP, TCP, DHCP, DNS, NTP, SMTP, POP3, MIME, HTTP, FTP, Telnet Clients	30,30 €
WIZnet	EG-SR-7100A	TCP, UDP, IP, ICMP, ARP, DHCP	36,10 €
Lantronix	XPort	TCP/, UDP/, IP, ARP, ICMP, SNMP, TFTP, Telnet, DHCP, BOOTP, HTTP, AutoIP	od 39,70 €

Modulom Nano SocketLAN je možné pripojiť zariadenie do siete Ethernet pomocou UART alebo SPI. Podporuje množstvo internetových protokolov a to aj zabezpečených. Tiež je možné priamo na ňom prevádzkovať server a ovládať tak mikrokontrolér pomocou webového rozhrania. Jeho konštrukcia obsahuje konektor pre pripojenie do siete pomocou štandardného kábla a kolíkové lišty pre osadenie do plošného spoja (obr. 2.8).

Obr. 2.8: Modul Nano SocketLAN (Foto: ConnectOne)

Modul EG-SR-7100A je určený pre rozšírenie aplikácií o komunikáciu po Ethernete pripojením na sériový port. Podporuje len základné protokoly. Do plošného spoja sa osadzuje pomocou kolíkových líšt. Pre pripojenie do siete je potrebné pridať konektor RJ45 (obr. 2.9).

Obr. 2.9: Modul EG-SR-7100A (Foto: WIZnet)

Moduly XPort sú integrované priamo do konektora RJ45 (obr. 2.10). Komunikácia s mikrokontrolérom je realizovaná pomocou UARTu. Z konštrukčného hľadiska by to

bol najlepší spôsob riešenia. Podľa počtu protokolov ktoré podporujú sa mení aj ich cena. Tiež existuje varianta ktorá podporuje Power Over Ethernet. Cena takéhoto modulu je až 87,92€.

Obr. 2.10: Modul XPort (Foto: Lantronix)

Nevýhodou všetkých modulov je ich vysoká cena. Keďže nebudú používané všetky dostupné protokoly, je výhodnejšie použiť jeden z radičov od firmy Microchip (tabuľka 2.4). Ich výhodou je integrovaná MAC a PHY vrstva. Vyššie vrstvy sa budú musieť implementovať pomocou mikrokontroléra. Tiež je možné vytvoriť možnosť napájania cez Ethernet, čo uľahčí montáž zariadenia v budove.

Tabuľka 2.4: Ethernetové radiče firmy Microchip

Názov	Veľkosť pamäte	Komunikácia s MCU	Puzdro	Ďalšie vlastnosti	Cena
ENC28J60	4 kB	SPI	SOIC28	-	3,00 €
ENC424J600	24 kB	SPI 8bit paralel	TQFP44	Šifrovanie, unikátna MAC adresa	3,38 €
ENC624J600	24 kB	SPI 16bit paralel	TQFP64	Šifrovanie, unikátna MAC adresa	3,65 €

Pre účel pripojenia terminálu do siete Ethernet bol zvolený obvod ENC424J600. Pre jeho výber prispela prítomnosť registrovanej MAC adresy a hardwarová podpora šifrovania.

2.3.2.3 Komunikácia s užívateľom

Pre komunikáciu s užívateľom sa použije klasický LCD displej s radičom HD44780 alebo s ním kompatibilným. Tiež bude použitá maticová klávesnica. Táto časť je použitá z dôvodu, keby bolo potrebné užívateľa dodatočne overiť, prípadne informovať ho o stave v akom sa zámok nachádza. Navyše môže byť použitý piezo menič pre akustickú signalizáciu, na ktorú človek reaguje rýchlejšie ako na textový popis.

2.3.2.4 Ovládanie zámku dverí

Ovládanie zámkov závisí od ich typu. Pre konštrukciu elektronicky ovládaných dverí sú využívané tri princípy:

- Elektromechanické zámky
- Elektromagnetické zámky
- Elektromotorické zámky

Elektromechanický zámok sa odblokuje po privedení napätia na cievku. Tá k sebe pritiahne jazýček, čím sa uvoľní strelka. Zámok je v takomto prípade možné ovládať kľučkou a tak mať z jednej strany dvere vždy prechodné. Ovládacie napätie týchto zámkou sa pohybuje v hodnotách 6-12 V jednosmerných alebo striedavých. Odoberaný prúd neprekračuje hodnotu 800 mA.

Elektromagnetické zámky sú vhodné pre miesta s častým pohybom osôb, pretože neobsahujú mechanické časti. Elektromagnet svojou silou udržiava dvere v zatvorenej polohe. Dvere je možné otvoriť jedine v prípade, keď je magnet odpojený od zdroja. Potrebné napätie na uzamknutie sa pohybuje v rozsahu 12-24 V jednosmerných. Odoberaný prúd je maximálne 500 mA.

Elektromotorické zámky ovládajú závoru v zámku. V tomto prípade je možné mať kľučku na oboch stranách a pri tom zostanú zabezpečené. Elektronické ovládanie zámku je podobné používaniu kľúča. Napätie na ovládanie má hodnotu 12 V a odoberaný prúd býva 500 mA.

Podrobnejší popis jednotlivých zámkov je v online katalógu predajcu [17]. Je vidieť, že všetky druhy zámkov majú jednu spoločnú hodnotu jednosmerného napätia 12 V. Môže sa stať, že by hodnota napätia potrebná pre ovládanie zámku bola iná. V takom prípade je možné využiť PWM reguláciu a tak spraviť zapojenie univerzálnejšie.

2.3.2.5 Pamäť terminálu

Terminál bude potrebné vybaviť aspoň malou pamäťou EEPROM pre uloženie jeho nastavení. Ak by bolo potrebné zaznamenávať činnosť terminálu je vhodné túto pamäť zvoliť väčšiu pre prípad, že by nebolo možné komunikovať po sieti. Jej veľkosť by sa mohla určiť priamo pri montáži podľa počtu užívateľov a predpokladaného pohybu osôb.

2.3.2.6 Detekcia poškodenia

Poškodenie zariadenia môže byť zistené na základe komunikácie medzi obvodmi. Napríklad pri odstránení displeja nebude možné načítať jeho stav. V miestach kde to nebude možné sa použije fotocitlivý prvok ktorý bude umiestnený pod krytom terminálu. V prípade jeho odstránenia začne na súčiastku dopadať svetlo. Ako iný spôsob by mohlo byť použitie koncových spínačov na kryte zariadenia.

2.3.2.7 Mikrokontrolér

Vzhľadom na to že mikrokontrolér bude ovládať všetky časti zariadenia, bude periodicky kontrolovať jeho stav a navyše bude obsahovať IP protokoly, je vysoká pravdepodobnosť že 8-bitové mikrokontroléry budú pracovať na hranici svojich možností. Z toho dôvodu bude volená 32-bitová architektúra.

Tabuľka 2.5 obsahuje prehľad vlastností dostupných 32-bitových mikrokontrolérov. Od každého zo štyroch výrobcov bol vybraný jeden najlacnejší, ktorý má 32 kB programovej pamäte.

Tabuľka 2.5: Vzorka lacných 32-bitových mikrokontrolérov

Výrobca	Názov	Jadro	Výkon [DMIPS/MHz]	Frekvencia [MHz]	Cena
Microchip	PIC32MX320F032	MIPS M4K	1,56	40	4,51 €
Freescale	MCF51QE32	Coldfire V1	0,94	50	4,88 €
Atmel	AT32UC3L032	UC3L	1,39	50	3,46 €
ST Microelectronics	STM32F100	Cortex M3	1,25	24	2,50 €

Zaujímavá je ponuka firmy ST Microelectronic, ktorá má v sebe jadro ARM za priaznivú cenu. To že má oproti ostatným menší výpočtový výkon nebude vadiť. Ak by však nastala situácia pri ktorej bude potrebná väčšia rýchlosť, bude ho možné nahradiť iným modelom, pretože obvody STM32F1xx sú medzi sebou pinovo kompatibilné.

2.3.2.8 Napájanie

Napájanie terminálu bude riešené pomocou Ethernetu. Tu nastáva problém v tom, že napätie zdroja sa pohybuje v hodnotách 44-57 V a dokáže dodať výkon maximálne 15,4 W. Podľa [18] je praktická hodnota 13 W. Pre otvorenie zámku je potrebné napätie 12 V a potrebný prúd môže dosahovať až 800 mA. Tieto hodnoty pomocou lineárnych regulátorov nie je možné získať. Z tohto dôvodu bude potrebné vytvoriť DC-DC menič. Potrebné napätia sú:

- 3,3 V
- 5 V
- 12 V

Pri použití meniča bude potrebné dbať na jeho spínaciu frekvenciu. V prípade že by bola v blízkosti pracovnej frekvencie, mohlo by nastať rušenie čítačky. To platí aj pre ďalšie harmonické. Napätia 3,3 V a 5 V by už mohli byť vytvorené pomocou lineárnych regulátorov z 12 V.

3 Návrh zapojenia

Nasledujúca kapitola sa bude zaoberať návrhom zapojenia čítačky RFID tagov určenú pre pripojenie k PC a prístupového terminálu.

3.1 Čítačka RFID tagov k PC

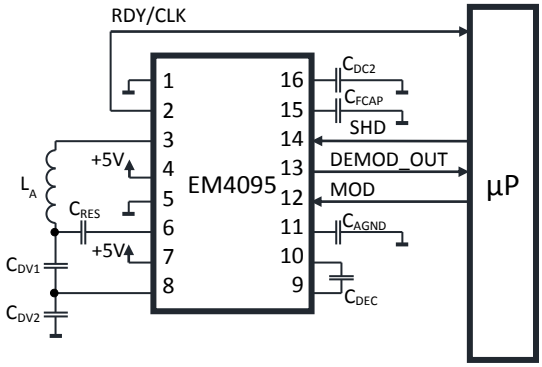
Ako už bolo spomenuté, táto čítačka bude pracovať na frekvencií 125 kHz. Pri návrhu sa bude vychádzať z blokovej schémy zobrazenej na obr. 2.3.

3.1.1 Obvod EM4095

Obvod EM4095 je integrovaný obvod navrhnutý pre použite v zariadeniach určených pre komunikáciu RFID. Jeho hlavnými úlohami sú:

- Budenie antény
- Amplitúdová modulácia pre použitie s tagmi ktoré umožňujú zápis
- Demodulácia signálu vysielaného tagom

Výrobcom odporúčané zapojenie je znázornené na obr. 3.1. Anténa je tvorená cievkou L_A. Tá môže byť vytvorená na doske plošného spoja, alebo mimo nej. Od jej rozmerov budú závisieť hodnoty súčiastok C_{RES}, C_{DV1} a C_{DV2}.



Obr. 3.1: Odporúčané zapojenie EM4095 (prevzaté z [19])

3.1.1.1 Význam signálov

Aby sa vedelo ako čo najlepšie pripojiť obvod k mikrokontroléru, je potrebné vedieť význam signálov pripojených k riadiacemu obvodu.

Privedením vysokej logickej úrovne na pin SHD sa obvod uvedie do úsporného režimu. Podľa [19] musí byť po zapnutí SHD na vysokej úrovni aby došlo k riadnemu nastaveniu vnútorných obvodov EM4095. Preto ho nie je možné napevno pripojiť k nízkej úrovni.

Signál DEMOD_OUT obsahuje demodulovaný signál vysielaný RFID tagom. Tento signál nie je dekódovaný. Vysielané informácie sa najčastejšie prevádzajú do kódu Manchester.

Signál MOD sa používa pri prípadoch, kedy sa komunikuje s tagmi, ktoré umožňujú zápis. Pri privedení vysokej úrovne sa vypne budenie antény. Ak by sa pracovalo s tagmi ktoré umožňujú len čítanie, môže byť tento pin trvalo privedený na nízku logickú úroveň.

Výstup RDY/CLK obsahuje hodinový signál ktorý je synchrónny so signálom na pine ANT1. Tento signál sa môže použiť na meranie času pri dekódovaní informácií vysielaných tagom.

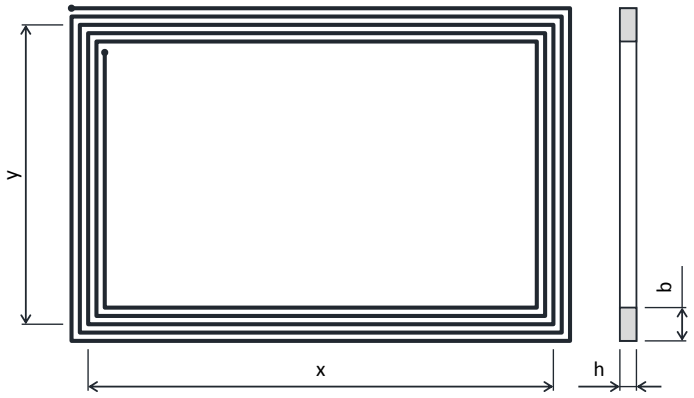
3.1.1.2 Návrh antény

Hodnoty súčiastok sú závislé na konštrukcií použitej cievky. Pri ich výpočte sa bude vychádzať z jej rozmerov.

Cievka bude vytvorená na obojstrannom plošnom spoji. Jej rozmery sú dané veľkosťou zariadenia a nevyužitým miestom ktoré ostalo po rozmiestnení ostatných súčiastok. Je však dobré aby sa rozmery pohybovali v okolí 5 až 10 cm. Pre túto konštrukciu boli zvolené nasledovné hodnoty:

- x = 58 mm
- y = 39 mm
- b = 10 mm
- h = 2 mm
- N = 32 závitov

Význam jednotlivých veličín je znázornený na obr. 3.2.



Obr. 3.2: Význam označenia rozmerov cievky

Pre indukčnosť obdĺžnikovej cievky platí podľa [20] vzťah

$$L_A = \frac{0{,}0276 \cdot (C \cdot N)^2}{1{,}908 \cdot C + 9 \cdot b + 10 \cdot h} \ , \tag{3.1}$$

kde

$$\mathrm{C} = \mathrm{x} + \mathrm{y} + 2 \cdot \mathrm{h} \, . \tag{3.2}$$

Po dosadení rozmerov dostávame hodnotu L_A = 95,2 µH. Táto hodnota nebude presná, pretože vzťah (3.2) platí pre vzduchové cievky. Pre účely ďalšieho výpočtu však táto presnosť postačuje. Výpočet hodnoty súčiastok sa ďalej riadi podľa príkladu uvedenom v [21].

Ak poznáme indukčnosť použitej cievky, môže sa vypočítať potrebný odpor antény podľa vzťahu

$$R_{ANT} = \frac{2 \cdot \pi \cdot f_0 \cdot L_A}{Q_A}, \tag{3.3}$$

kde sa volí Q_A = 3,8. V takom prípade je hodnota celkového odporu antény R_{ANT} = 19,7 Ω. Ak by odpor cievky nedosahoval túto hodnotu, je potrebné k nej do série zapojiť rezistor R_{SER} s odporom

$$R_{SER} = R_{ANT} - R_L , \tag{3.4}$$

kde R_L je odpor vytvorenej cievky.

Ďalej sa počíta hodnota kondenzátora C_{RES}. Pre L_A a C_{RES} v zapojení musia rezonovať na frekvencií f_0 = 125 kHz. Aby sa to dosiahlo, musí platiť

$$C_{RES} = \frac{1}{(2 \cdot \pi \cdot f_0)^2 \cdot L_A}, \tag{3.5}$$

vypočítaná kapacita má hodnotu 17 nF. Keďže sa kondenzátory s takouto hodnotou bežne nevyrábajú, zvolíme najbližšiu hodnotu C_{RES} = 18 nF. Ak by bol rozdiel veľký, kondenzátor C_{RES} by nahradilo sériovo-paralelné zapojenie dostupných kondenzátorov.

Pred ďalším výpočtom sa overí, či je pretekajúci prúd obvodom menší, ako je maximálny prúd ktorý dokáže budič antény dodať. Pre amplitúdu prúdu pri rezonančnej frekvencií platí

$$I_{ANT} = \frac{4}{\pi} \cdot \frac{V_{dd}}{R_L + R_{SER} + 2 \cdot R_{AD}}, \tag{3.6}$$

kde je napájacie napätie V_{dd} = 5 V a výstupný odpor budiča antény R_{AD} = 9 Ω. Potom I_{ANT} = 169 mA. V [19] je udávaná maximálna hodnota dodávaného prúdu I_{ANTmax} = 300 mA.

Výpočet kapacitného deliča C_{DV1}, C_{DV2} je o niečo zložitejší, pretože sa najprv volí ich hodnota a potom sa počíta, či sú splnené podmienky pre správnu funkciu. Výrobca v [21] udáva, že by sa kapacita C_{DV2} mala pohybovať v rozsahu 1 nF až 2 nF. Kapacita C_{DV1} bude musieť mať takú hodnotu, aby napätie na vstupe DMOD_IN bolo menšie napätie ako 4 V, ale nie zas tak nízke že by nebolo možné prijímať signál z antény.

Hodnoty kapacity kondenzátorov sa volia C_{DV1} = 150 pF a C_{DV2} = 1 nF. V tomto prípade bude špičkové napätie na anténe

$$V_{ANT(pp)} = \frac{I_{ANT}}{\pi \cdot f_0 \cdot C_0}, \tag{3.7}$$

kde je hodnota C_0 daná vzťahom

$$C_0 = C_{RES} + \frac{C_{DV1} \cdot C_{DV2}}{C_{DV1} + C_{DV2}}. \tag{3.8}$$

Po výpočte je zistená hodnota napätia na anténe $V_{ANT(pp)}$ = 23,7 V. Napätie na výstupe deliča a tým aj na vstupe DMOD_IN je daný vzťahom

$$V_{DMOD} = V_{ANT(pp)} \cdot \frac{C_{DV1}}{C_{DV1} + C_{DV2}}. \tag{3.9}$$

Pri takejto kombinácií C_{DV1} a C_{DV2} je napätie na vstupe V_{DMOD} = 3,1 V, čo spĺňa podmienku V_{DMOD} < 4 V.

Na záver sa môže overiť aká bude skutočná rezonančná frekvencia obvodu. Tá sa vypočíta pomocou vzťahu

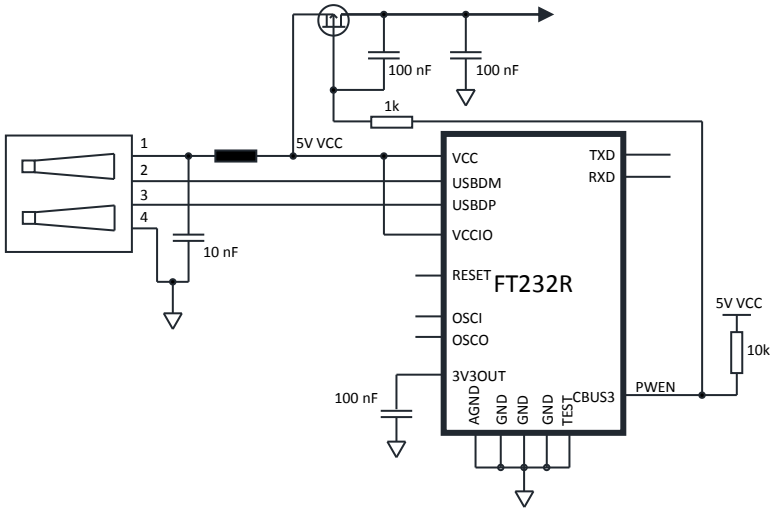
$$f_{RES} = \frac{1}{2 \cdot \pi \cdot \sqrt{L_A \cdot C_0}}, \tag{3.10}$$

kde C_0 je daný vzťahom (3.8). Skutočná frekvencia bude f_{RES} = 121 kHz. Táto hodnota je v tolerancií, pretože tagy s pracovnou frekvenciou 125 kHz majú pracovný rozsah od 100 kHz do 150 kHz.

Tento postup návrhu nie je možné použiť pre RFID systémy pracujúcich na vyšších frekvenciách. Ďalší návrh pre pracovnú frekvenciu 13,56 MHz bude spomenutý v kapitole 3.2.1.

3.1.2 Prevodník USB/UART

Pre komunikáciu s PC je použitý integrovaný obvod FT232RL. Jedná sa o prevodník USB/UART, ktorý sa po pripojení k počítaču hlási ako virtuálny sériový port. To umožňuje jednoduchú implementáciu komunikácie pomocou USB aj na jednoduchých mikrokontroléroch. Zapojenie vychádza z katalógového zapojenia dané výrobcom (obr. 3.3). Obvod okrem funkcie vytvárať virtuálny sériový port navyše spína napájacie napätie pre ostatné obvody. Ak by bola čítačka pripojená do USB portu ktorý by nebol schopný dodať potrebný prúd, ostatné obvody by neboli napájané a nehrozilo by poškodenie portu.



Obr. 3.3: Zapojenie prevodníku USB/UART (prevzaté z [22])

3.1.3 Mikrokontrolér

Pre dekódovanie a odosielanie načítaných údajov do PC bol zvolený obvod PIC16F628A od firmy Microchip. Jedná sa o jednoduchý 8-bitový mikrokontrolér, ktorý obsahuje 4 MHz interný oscilátor, UART a 3 čítače/časovače s funkciou Capture. Obsahuje aj ďalšie periférie, ktoré pre účel čítačky RFID tagov nie sú podstatné. Tabuľka 3.1 obsahuje prepojenie portov mikrokontroléra s vonkajšími obvodmi.

Tabuľka 3.1: Pripojenie portov mikrokontroléra PIC

Funkcia	Pin mikrokontroléra	Pripojenie k obvodu
Odosielané dáta do PC	RB2/TX	FT232-RXD
Prijímané dáta z PC	RB1/RX	FT232-TXD
Úsporný režim	RB5	EM4095-SHD
Hodinový signál RFID	RB0/INT	EM4095-RDY/CLK
Prijímané dáta RFID	RB3/CCP1	EM4095-DEMOD_OUT
Modulácia RFID	RB4	EM4095-MOD
Signalizácia LED1	RA0	LED anóda
Signalizácia LED2	RA1	LED katóda
Signalizácia piezo	RA2	Piezo bzučiak
Program clock	RB6/PGC	Programátor PGC
Program data	RB7/PGD	Programátor PGD
Master clear	RA5/MCLR	Programátor MCLR

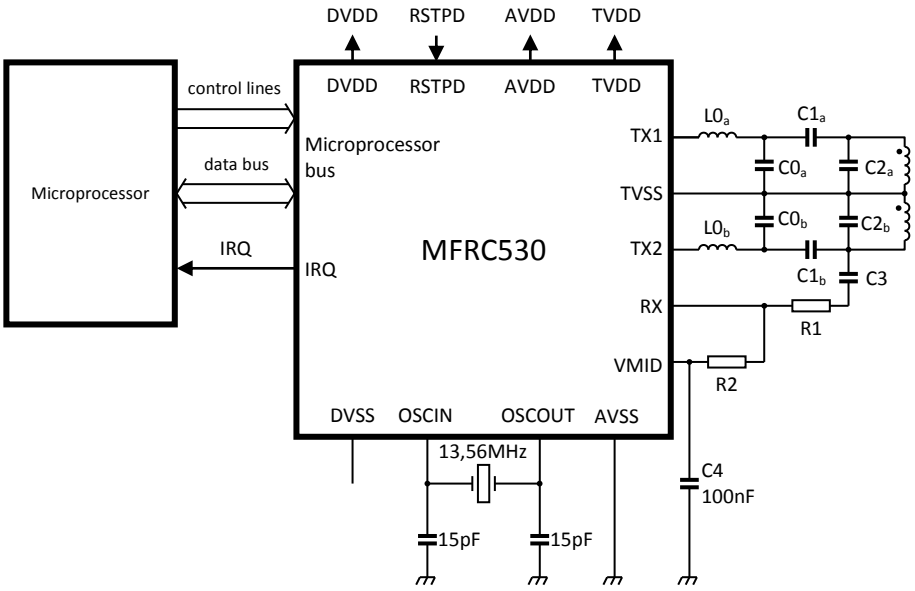
Okrem už spomínaných obvodov je mikrokontrolér pripojený k signalizačným prvkom (dvojfarebná led, piezo) a ICSP konektor.

3.2 Prístupový terminál

Prístupový terminál bude navrhovaný už pre použitie s tagmi pracujúcimi na frekvencií 13,56 MHz. Pri návrhu sa bude postupovať podľa blokovej schémy na obr. 2.6.

3.2.1 Obvod MFRC530

Tento integrovaný obvod slúži pre bezkontaktnú komunikáciu na frekvencií 13,56 MHz. Obvod je plne kompatibilný so štandardom ISO14443A. Dokáže rozpoznať chyby v prenose (parita a CRC). Navyše je vybavený podporou šifrovacieho algoritmu Crypto-1 pre podporu MiFare.



Obr. 3.4: Typické zapojenie MFRC530 (prevzaté z [23])

Podobne ako pri obvode EM4095, aj tu hodnoty súčiastok pri anténe nie sú pevne dané. Tie závisia od konštrukcie antény a vypočítajú sa v nasledujúcom postupe.

3.2.1.1 Pripojenie k mikrokontroléru

Komunikácia s obvodom je možná dvoma spôsobmi:

- Paralelnou 8-bitovou zbernicou
- Sériovým rozhraním SPI

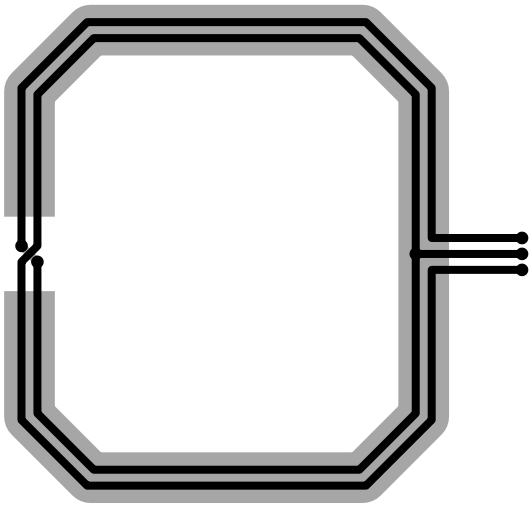
Kvôli jednoduchšiemu zapojeniu sa volí SPI. V tomto režime sa obvod správa ako slave. Pre SPI nie sú na obvode vyhradené zvlášť vývody. Tie sú spoločné ako pre SPI tak pre paralelnú zbernicu. Aby obvod rozpoznal ako bude komunikovať, nestačí len pripojiť SPI linku, ale aj ďalšie signály na pevné logické úrovne (tabuľka 3.2).

Tabuľka 3.2: Zapojenie MFRC530 pre SPI

MFRC530	SPI
ALE	NSS (CS)
A2	SCK
A1	Log 0
A0	MOSI
NRD	Log 1
NWR	Log 1
NCS	Log 0
D7-D1	nezapájať
D0	MISO

3.2.1.2 Návrh antény

Anténa bude vytvorená cievkou realizovanou na doske plošného spoja. Tu však nestačí vytvoriť len závity ako v prípade EM4095. Postup návrhu antény je uvedený v [24].



Obr. 3.5: Rozloženie cievky pre anténu

Na obr. 3.5 je znázornený odporúčaný tvar cievky. Tá je symetrická s vyvedeným stredom. Jej indukčnosť je podľa [23] daná vzťahom

$$L = 2 \cdot l \cdot \left[\ln\left(\frac{l}{D}\right) - K\right] \cdot N^{1,8}\,, \tag{3.11}$$

kde *l* je dĺžka jedného závitu, *D* priemer vodiča (šírka spoja na DPS), *N* počet závitov a *K* konštanta udávajúca tvar. Pre cievku v tvare kružnice je *K* = 1,07 a pre štvorcovú je *K* = 1,47. Rozmery musia byť dosadené v cm a výsledná indukčnosť bude mať rozmer nH.

Vytvorená cievka antény má nasledujúce parametre:

- *l* = 18 cm
- *D* = 0,08 cm
- *N* = 4

Po dosadení do (3.11) je vypočítaná indukčnosť L_A = 1,74 µH.

Ďalej sa zisťuje aký má mať anténa odpor podľa zvoleného *Q*, ktoré by malo byť menšie ako 40. Pre vysoké prenosové rýchlosti musí byť *Q* maximálne 22. V tomto prípade sa volí $Q = 22$. Pre odpor R_{ANT} platí rovnaký vzťah ako v prípade EM4095. Po dosadení do (3.3) sa získa hodnota R_{ANT} = 6,7 Ω. Ak by vytvorená cievka nemala taký odpor, pridajú sa k nej do série rezistory pre ktoré platí (3.4).

Článok C_1, C_2 slúži na prispôsobenie impedancie. Odporúča sa aby impedancia Z_a = 250 Ω. Ich kapacita sa podľa [24] určí pomocou vzťahov

$$C_2 = \frac{1}{\omega \cdot \sqrt{\left(\frac{\omega \cdot L}{1 - \frac{R_{ANT}}{Z_a}}\right)^2 - \frac{{R_{ANT}}^2 + \omega^2 \cdot L^2}{1 - \frac{R_{ANT}}{Z_a}}} + \frac{\omega^2 \cdot L}{1 - \frac{R_{ANT}}{Z_a}}} \tag{3.12}$$

a

$$C_1 = \frac{{R_{ANT}}^2 + \left(\omega \cdot L - \frac{1}{\omega \cdot C_2}\right)^2}{\frac{\omega \cdot L}{C_2} \cdot \left(\frac{1}{\omega \cdot C_2} - \omega \cdot L\right) - \frac{{R_{ANT}}^2}{C_2}}\ , \tag{3.13}$$

kde

$$\omega = 2 \cdot \pi \cdot f\ . \tag{3.14}$$

Po dosadení sú zistené hodnoty po C_1 = 66,4 pF a C_2 = 13,5 pF.

Článok L_0, C_0 tvorí EMC filter. Zabraňuje vyžarovaniu vyšších harmonických do okolia. Jeho medzná frekvencia by mala byť približne 14,4 MHz (13,56 MHz + 847,5 kHz). To však závisí od šírky pásma prenášaného signálu. V [24] sú odporúčané hodnoty L_0 = 1 µH a C_0 je dané paralelnou kombináciou 68 pF a 56 pF.

V dokumente [24] sa nič nespomína o výpočte hodnôt súčiastok pre prijímaciu časť obvodu. Sú tu len dané hodnoty C_3 = 1 nF, C_4 = 100 nF, R_1 = 470 Ω až 4,7 kΩ a R_2 = 820 Ω. Odpor R_1 sa musí voliť tak, aby striedavá zložka napätia na pine RX bola v rozsahu 1,5 V_{PP} < U_{RX} < 3 V_{PP}.

3.2.2 Obvod ENC424J600

Obvod ENC424J600 slúži ako ethernetový radič. Obsahuje v sebe MAC a PHY vrstvu. Dokáže pracovať v sieťach 10Base-T a 100Base-TX. Oproti jeho predchodcovi ENC28J60 obsahuje navyše hardwarovú podporu pre šifrovacie algoritmy RSA, Diffie-Hellman, AES, MD5 a SHA-1.

3.2.2.1 Pripojenie k mikrokontroléru

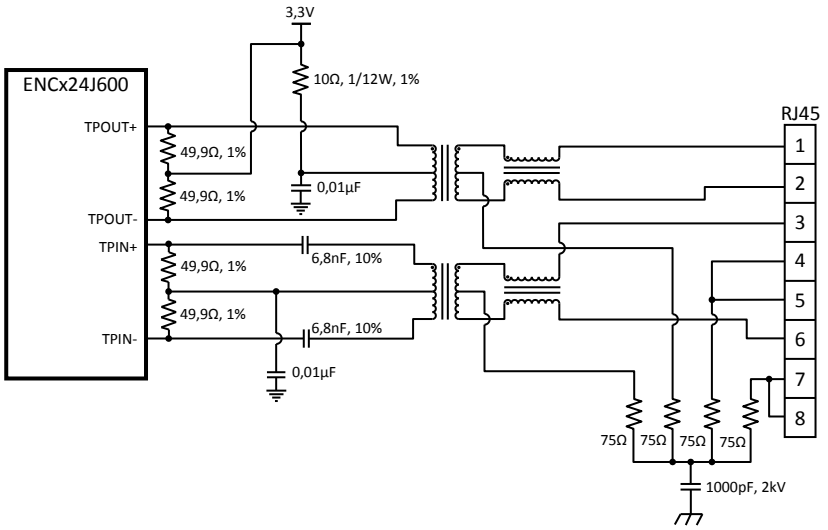
Komunikácia s obvodom môže prebiehať dvoma spôsobmi:

- Paralelnou 8-bitovou zbernicou
- Pomocou SPI

Komunikácia cez paralelnú zbernicu má výhodu v tom, že je možné dosiahnuť vyššie prenosové rýchlosti oproti SPI. Takáto rýchlosť nebude pre tento účel potrebná, pretože sa nebudú prenášať veľké objemy dát. Preto sa použije komunikácia pomocou SPI, čo prinesie úsporu vo využití portov mikrokontroléra. Pripojenie jednotlivých pinov je možné nájsť v [25]. Je však potrebné dbať na to, že pin INT/SPISEL je po privedení napájania nastavený ako vstup a podľa logickej úrovne rozhodne o tom či sa bude komunikovať cez paralelnú zbernicu alebo cez SPI. Preto je dobré k tomuto signálu pripojiť pull-up rezistor.

3.2.2.2 Pripojenie do siete Ethernet

Keďže radič ENC424J600 obsahuje aj PHY vrstvu, stačí len k nemu pripojiť oddeľovací transformátor.



Obr. 3.6: Pripojenie oddeľovacieho transformátora k ENC424J600 (prevzaté z [25])

Na trhu je možné zohnať transformátory integrované priamo do konektoru RJ45. Pri výbere je však nutné brať do úvahy, že pri napájaní z dátovej siete PoE musia byť prístupné voľné páry, prípadne aj stredy transformátorov.

3.2.3 LCD displej

Pre komunikáciu s užívateľom bol zvolený LCD displej z rady BC1602H od firmy Bolymin. Jedná sa o znakový displej s rozložením znakov 16x2 kompatibilný s radičom HD44780. Z konštrukčného hľadiska má výhodu v tom, že má lištu pre pripojenie na spodnej strane. Vďaka tomu ho je možné osadiť čo najvyššie aj keď sa na vrchnej strane zariadenia nachádzajú konektory. Pri pripájaní k mikrokontroléru je potrebné

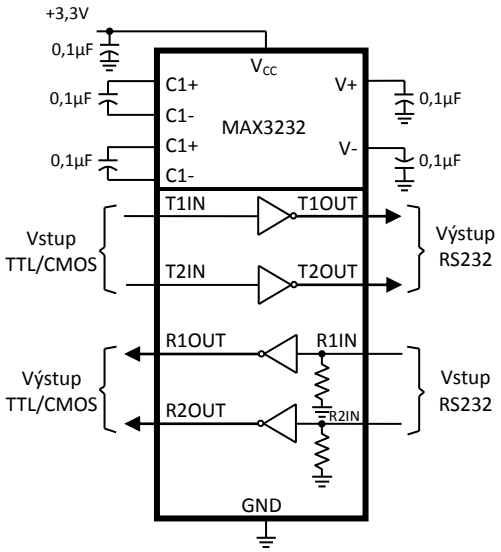
dbať na to, že jeho napájacie napätie je 5 V. Preto sa musia pripojiť na port tolerantný voči takémuto napätiu, alebo použiť prevodník logických úrovní.

3.2.4 Klávesnica

Pre zadávanie údajov od užívateľa je použitá maticová klávesnica ECO12150 06 s rozložením kláves 3x4. K mikrokontroléru môže byť pripojená k ľubovoľnému portu.

3.2.5 Prevodník RS232/UART

Prevodník logických úrovní je založený na integrovanom obvode MAX3232. Zapojenie je založené na katalógovom zapojení dané výrobcom (obr. 3.7).



Obr. 3.7: Zapojenie MAX3232 (prevzaté z [26])

Tento port bude slúžiť ako servisný pre nastavovanie parametrov, prípadne zmenu existujúceho firmwaru. Práve kvôli tomu sa musí využívať jednotka UART1 aby bolo možné využívať bootloader predprogramovaný výrobcom mikrokontroléra. K počítaču sa bude pripájať štandardným 9-pinovým konektorom Cannon. V zapojení sa budú zapojené len signály RXD a TXD. Riadiace signály sa nebudú využívať.

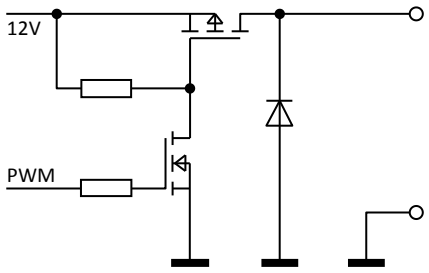
3.2.6 Pamäť flash

Terminál bude obsahovať aj úložné miesto pre nastavenia. Na to slúži obvod AT25DF041A. Jedná sa o sériovú pamäť flash s veľkosťou 4 Mb. To je dostatok aj pre uloženie čísel RFID tagov v prípade, že by sa rozhodlo použiť tento terminál ako samostatnú jednotku. Inak sa môže použiť riešenie s menšou kapacitou.

Komunikácia prebieha pomocou SPI. Pri zapájaní stačí pripojiť len napájanie a sériovú linku. Signály WP a HOLD je možné nechať nezapojené, pretože sú vnútorne prepojené cez pull-up rezistory a tak funkcia pamäte nebude nimi obmedzená.

3.2.7 Ovládanie zámku dverí

Ako už bolo spomenuté, spínacie napätie zámku dverí sa môže pohybovať od 6 V do 12 V. Preto je potrebné aby výstupné tranzistory mali možnosť riadenia pomocou PWM. Zámok predstavuje indukčnú záťaž, preto je tiež nutné chrániť výstup pred napäťovými špičkami ktoré vznikajú pri rozopnutí obvodu. Pri riadení pomocou PWM je to o to dôležitejšie.



Obr. 3.8: Zapojenie tranzistorového spínača

3.2.8 Detekcia poškodenia

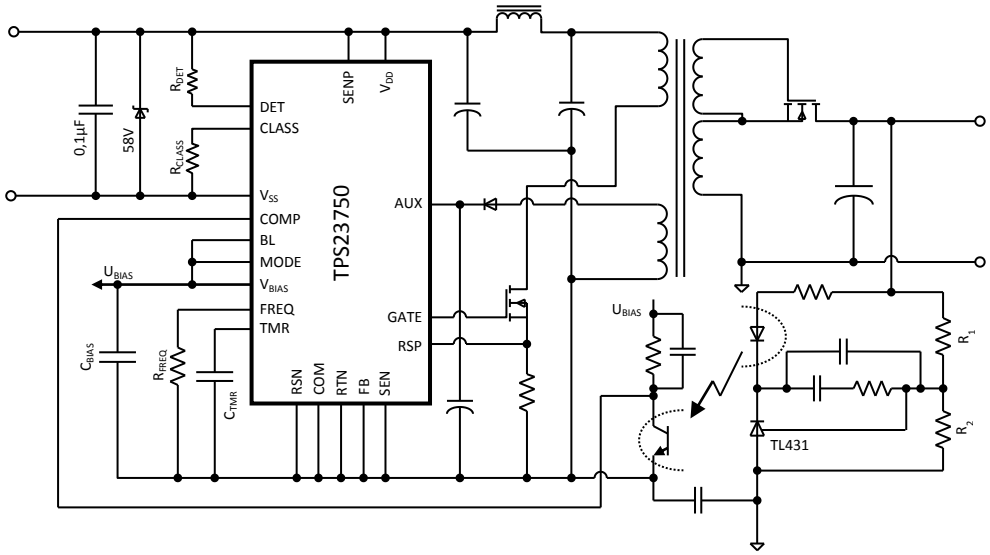
Možné zistenie poškodenia polo rozobrané v kapitole 2.3.2.6. Na portoch mikrokontroléra sa vyhradia nasledovné piny:

- 2x vstup A/D prevodníku pre fotocitlivé prvky (možno použiť aj s mechanickými spínačmi)
- 1x pin pre všeobecné použitie pripojený na rovnaký konektor ako výstup tranzistorového spínača (kontrolná slučka od zámku dverí)
- 1x pin pre všeobecné použitie (jazýčkový senzor ovládaný magnetom na dverách)

3.2.9 Napájanie

Ako bolo spomenuté v kapitole 2.3.2.8, je potrebné navrhnúť spínaný zdroj zo 48 V na 12 V. Aby bolo napájanie korektné, zdroj by mal mať detekciu triedy zariadenia podľa štandardu IEEE802.3af.

Pre účel vytvorenia takéhoto zdroja bol vybraný integrovaný obvod TPS23750 od firmy Texas Instruments. Jedná sa o obvod kombinujúci v sebe detekciu triedy zariadenia a PWM kontrolér pre DC/DC menič.



Obr. 3.9: Typické zapojenie TPS23750 (prevzaté z [27])

Trieda zariadenia sa určuje pomocou rezistora R_{CLASS}. Jeho hodnota sa volí na základe hodnôt ktoré udáva tabuľka 3.3.

Tabuľka 3.3: Voľba triedy zariadenia

Trieda	**Príkon zariadenia** [W]	**Rozsah prúdu** [mA]	**R_{CLASS}** [Ω]
0	0,44 – 12,95	0 – 4	4420
1	0,44 – 3,84	9 – 12	953
2	3,84 – 6,49	17 – 20	549
3	6,49 – 12,95	26 – 20	357
4	---	36 – 44	255

Navrhované zariadenie bude zaradené do triedy 3, pretože pri zopnutí zámku bude odoberať veľký výkon. Keby bolo zariadenie nastavené v nižšej triede, mohlo by sa stať že pri pokuse odomknúť dvere bude odpojené od napájania.

Spínacia frekvencia meniča sa určuje rezistorom R_{FREQ}. Jeho odpor sa vypočíta vzťahom

$$R_{FREQ} = \frac{15000}{f_S}. \tag{3.15}$$

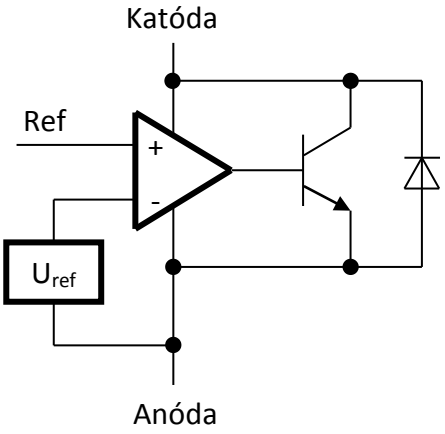
Výsledná hodnota R_{FREQ} je v kΩ. Spínacia frekvencia meniča f_S musí byť dosadená v kHz. Pre zvolenú frekvenciu f_S = 100 kHz je R_{FREQ} = 150 kΩ.

Hodnota C_{TMR} slúži pre nastavenie času pri mäkkom štarte meniča. Výpočet kapacity podľa zvoleného času sa riadi vzťahom

$$C_{TMR} = 33 \cdot 10^{-6} \cdot t_{start}. \tag{3.16}$$

Pre zvolený čas t_{start} = 2 ms je kapacita C_{TMR} = 66 nF.

Výstupné napätie meniča sa nastavuje odporovým deličom R_1, R_2. Náhradná schéma súčiastky TL431 je na obr. 3.9.



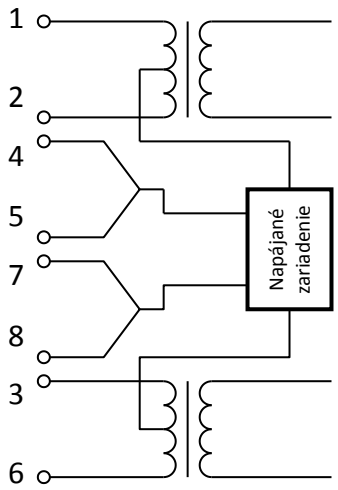
Obr. 3.10: Náhradná schéma TL431 (prevzaté z [28])

Referenčné napätie je U_{ref} = 2,495 V. Pre výstupné napätie meniča platí

$$U_{OUT} = \frac{R_1 + R_2}{R_2} \cdot U_{ref} \, . \tag{3.17}$$

Pre zvolenú kombináciu R_1 = 10 kΩ a R_2 = 2,6 kΩ je výstupné napätie U_{OUT} = 12,1 V.

Vo všeobecnosti môže byť zariadenie PoE napájané cez signálové alebo nevyužité páry. Z nevyužitých párov sa napájanie získava priamo. Pre signálové páry musia byť vyvedené stredy oddeľovacieho transformátora. Zapojenie je znázornené na obr. 3.11. Problematiku zapojenia rieši použitý konektor, ktorý má v sebe okrem transformátora navyše aj Graetzove mostíky, takže z jeho vývodov je možné napájacie napätie odoberať priamo.



Obr. 3.11: Získanie napájacieho napätia

3.2.10 Mikrokontrolér

Pre riadenie zariadenia bol vybraný obvod STM32F100. Jedná sa o lacný mikrokotrolér s jadrom ARM Cortex-M3. Pri takýchto obvodoch je pre spoľahlivú funkciu dôležité kvalitné napájanie. Preto je ku každému napájaciemu pinu privedené napätie cez blokovací kondenzátor. Zapojenie ďalších periférií obsahuje tabuľka 2.1.

Tabuľka 3.4: Pripojenie portov mikrokontroléra STM32

Funkcia	Pin mikrokontroléra	Využívané periférie
Riadky klávesnice	PC0-PC3	GPIO
StĺPce klávesnice	PB4-PB6	GPIO
CS pre flash	PC4	GPIO
CP pre RFID	PB12	GPIO
SPI pre flash a RFID	PB13-PB15	SPI2
Prerušenie z RFID	PB0	IRQ
Reset RFID	PB1	GPIO
LCD	PC5-PC11 (5V)	GPIO
Podsvietenie LCD	PB9	TIM17_CH1
Detekcia poškodenia krytu	PA0-PA1	ADC
Prerušenie z Ethernetu	PA3	IRQ
CS pre Ethernet	PA4	GPIO
SPI pre Ethernet	PA5-PA7	SPI1
Ovládanie zámku	PB7	TIM4_CH2
Piezo menič	PB8	TIM16_CH1
Kontrolné slučky na dverách	PB10-PB11	IRQ
Sériová linka	PA9-PA10	USART1
Ladiace rozhranie	PA13-PA14	SWD

4 Softwarová obsluha periférií

Táto časť práce sa bude zaoberať tvorbou knižníc pre ovládanie jednotlivých periférií v zapojeniach.

4.1 Ovládanie EM4095

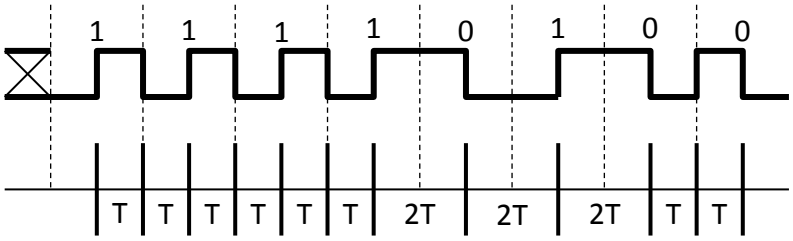
Funkcie pre ovládanie EM4095 sú vytvorené pre prácu s tagmi typu EM4100 a s nimi kompatibilnými.

4.1.1 Inicializácia

Pre správnu funkciu obvodu je potrebné po privedení napájacieho napätia dať vstup SHD na logickú hodnotu 1, čím sa vypnú všetky interné časti. Po opätovnom spustení je obvod nastavený a môže vykonávať svoju funkciu. Pre povolenie budenia antény je ešte potrebné na vstup MOD priviesť logickú hodnotu 0.

4.1.2 Prijímanie demodulovaného signálu

Demodulovaný signál na výstupe DEMOD_OUT je presne taký, ako sa vysiela z tagu. V prípade EM4100 sú dáta kódované linkovým kódom Manchester. Jeden z možných spôsobov dekódovania je opísaný v [29]. Dekódovanie je vykonávané na základe merania dĺžky impulzov.



Obr. 4.1: Princíp dekódovania Manchestru

Vo väčšine prípadov je doba jedného bitu odoslaná z EM4100 64-násobkom periódy nosnej frekvencie. Je však dobré pre meranie času vytvoriť okno z dvoch dôvodov:

- Anténa nemusí rezonovať presne na frekvencií 125 kHz
- Keď nie je priložený tag, na výstupe sa objavuje signál s frekvenciou 50 Hz

Princíp dekódovania je zobrazený na obr. 4.1. Ak nastala zmena vo vysielanom bite, čas medzi dvoma hranami je 2*T*. Ak je prijatý bit rovnaký ako predchádzajúci, bude meraný čas medzi hranami *T* 2-krát za sebou. V inom prípade by to znamenalo chybu prenosu.

4.1.3 Formát prijímaných dát

Po dekódovaní dát je nakoniec potrebné overiť, či pri prenose nedošlo k chybe. Zabezpečenie je realizované pomocou paritných bitov. Ich rozmiestnenie v bloku je znázornené na obr. 4.2. Podľa tohto znázornenia sú bity odosielané zľava doprava postupne po riadkoch.

1	1	1	1	1	1	1	1	1
				V0	V1	V2	V3	P0
				V4	V5	V6	V7	P1
				D0	D1	D2	D3	P2
				D4	D5	D6	D7	P3
				D8	D9	D10	D11	P4
				D12	D13	D14	D15	P5
				D16	D17	D18	D19	P6
				D20	D21	D22	D23	P7
				D24	D25	D26	D27	P8
				D28	D29	D30	D31	P9
				PC0	PC1	PC2	PC3	0

Obr. 4.2: Formát výstupných dát (prevzaté z [30])

Ak by počas prenosu došlo k chybe, pomocou súradníc určených cez paritné bity by sa dala chyba odstrániť. Ak by sa chyba neodstránila, môže sa čakať na ďalšie dáta pretože sú opakovane vysielané pokiaľ je tag v blízkosti.

4.2 Ovládanie MFRC530

Ovládanie obvodu prebieha pomocou SPI. Nastavovanie a spúšťanie funkcií je realizované pomocou zápisu do registrov v obvode. V tejto podkapitole budú spomenuté základné postupy pre prácu s týmto obvodom.

4.2.1 Inicializácia

Po pripojení napájacieho napätia je potrebné uviesť obvod do vypnutého stavu privedením logickej hodnoty 1 na vstup RSTPD. Tento stav by mal trvať minimálne 100 µs. Po opätovnom spustení sa vykoná reset obvodu, čím sa nastavia registre na hodnoty nastavené výrobcom. Tie sú potom štandardne pripravené pre prácu podľa štandardu ISO14443A. Počas inicializácie sa register Command nastaví na hodnotu 0x3F. Po skončení je jeho hodnota nulová.

4.2.2 Práca s registrami

Pre zápis alebo načítanie registra je potrebné najskôr odoslať jeho adresu. Pri odosielaní adresy sa zároveň určuje či sa dáta budú zapisovať alebo načítavať.

R/W	A5	A4	A3	A2	A1	A0	0

Obr. 4.3: Byte udávajúci adresu registra MFRC530

Na obr. 4.3 je zobrazený formát bytu, ktorým sa určuje adresa registra. Najvyšší bit udáva, či sa z neho bude načítavať alebo do neho zapisovať (0-zápis, 1-čítanie). Bity A0 až A5 udávajú adresu registra. Je vidieť, že adresu treba pred odoslaním rotovať doľava, pretože najnižší bit musí byť nastavený na 0.

Po adrese nasledujú už samotné dáta či už sa načítava alebo zapisuje.

4.2.3 Zásobník FIFO

Obvod MFRC530 obsahuje 64 bytový zásobník FIFO. Ten je používaný pri zápise a načítavaní internej EEPROM, zadávaní šifrovacích kľúčov alebo pri samotnom prenose dát s RFID tagom.

Zápis aj načítavanie zo zásobníku FIFO sa vykonáva pomocou registra FIFOData. Rozdiel medzi vyčítacím a zapisovacím ukazateľom je uložený v registri FIFOLength.

V zásobníku nie je možné určiť či uložené dáta patria do jedného alebo viacerých prenosov. Preto pred volaním príkazu využívajúci zásobník je dobré zásobník vymazať pre prípad, že by v ňom zostali staré dáta. To sa vykoná nastavením bitu FlushFIFO v registri Control.

4.2.4 Spúšťanie príkazov

Spustenie príkazu sa vykoná zápisom jeho hodnoty do registra Command. Po jeho vykonaní sa tento register znovu nastaví na nulovú hodnotu. V prípade že by sa zadávali argumenty alebo odosielali dáta, tak pred spustením príkazu musia byť uložené v zásobníku FIFO. Ak sa príkazom prijímajú dáta, tak sú po vykonaní príkazu uložené v zásobníku.

4.2.5 Prenos medzi MFRC530 a tagom

Prenos sa vykonáva pomocou príkazov Transmit (0x1A) alebo Transceive (0x1E). Existuje aj zvlášť príkaz Receive (0x16), ale ten sa neodporúča používať kvôli časovej závislosti medzi odosielaním a prijímaním. Postup prenosu je nasledovný:

- Uložiť odosielanú hodnotu do zásobníka FIFO
- Zavolať príkaz Transmit (0x1A) alebo Transceive (0x1E) uložením ich hodnoty do registra Command
- Testovať dokončenie príkazu (hodnota registra Command je nulová)
- Testovať vzniknuté chyby pri prenose pomocou registra ErrorFlag
- Načítať obsah zásobníka FIFO

Posledné dva kroky platia, keď sa použije príkaz Transceive. Tiež je dobré zapnúť časovač obvodu a pomocou externého prerušenia testovať, či už neprešiel určitý čas. Ak by sa totiž zavolal príkaz Transceive a v blízkosti by nebol žiadny tag, obvod by stále čakal na začiatok príjmu dát.

4.2.6 Komunikácia s tagmi MiFare

Tagy MiFare majú príkazy pre identifikáciu a výber tagu implementovanú podľa štandardu ISO14443A.

4.2.6.1 Request

Týmito príkazom sa zisťuje, či je v blízkosti RFID tag. Odosielaná hodnota z čítačky je 0x26. Tu je však potrebné preniesť len 7 bitov. To sa nastaví pomocou bitov TxLastBits v registri BitFraming. Návratová hodnota z tagu udáva jeho typ. Pre MiFare je táto hodnota 0x04 0x00.

4.2.6.2 Wake-up

Príkaz pre zobudenie tagu je takmer totožný s príkazom Request. Jediný rozdiel je v odosielanej hodnote. Tá je 0x52. Odpoveď tagu je tiež totožná.

4.2.6.3 Anti-collision

Pomocou tohto príkazu je možné zistiť sériové číslo priloženého tagu. Odosielaná hodnota je 0x93 0x20. Odpoveď tagu predstavuje jeho sériové číslo.

Za odosielaným príkazom môže nasledovať časť sériového čísla. Odpoveď v tomto prípade bude zvyšok tohto čísla.

4.2.6.4 Select

Zavolaním tohto príkazu sa určí s ktorým tagom bude komunikácia pokračovať. Ostatné tagy sa dostanú do stavu, ako keby príkazy pred tým neboli prijaté. Pre vykonanie príkazu sa odosiela hodnota 0x93 0x70 s nasledujúcim sériovým číslom tagu. Hodnota odpovede je 0x08.

4.2.6.5 Halt

Po zavolaní tohto príkazu sa tag dostane do stavu, kedy nebude reagovať na pokyny. Spôsob ako ho dostať do pôvodného stavu je zavolať príkaz Wake-up alebo ho dostať mimo čítačky čím sa reštartuje. Hodnota príkazu je 0x50 0x00.

4.3 Ovládanie ENC424J600

Pri komunikácií s obvodom prostredníctvom SPI sa využívajú takzvané inštrukcie. Tie je možné rozdeliť na nasledujúce skupiny:

- Jednobytové – priame inštrukcie s jedinečnou funkciou ktoré nevyžadujú argumenty ani nevracajú žiadnu hodnotu
- Dvojbytové – existuje len jedna, ktorá vracia hodnotu zvolenej banky pamäte
- Trojbytové – určené hlavne na prácu s registrami a ukazateľmi
- N-bytové – vo všeobecnosti sa používanú pre prácu s registrami a pamäťou obvodu

Formáty jednotlivých inštrukcií sú uvedené v [25].

4.3.1 Inicializácia

Pred tým než sa zariadenie začne využívať na prenos paketov, je potrebná jeho správna konfigurácia.

4.3.1.1 Reset

Prvým krokom je vykonanie resetu. Ten sa vykoná nastavením bitu ETHRST v registri ECON2. Jednoduché nastavenie bitu nie je výrobcom odporúčané, pretože hneď po pripojení napájacieho napätia nemusí obvod správne reagovať a tak je postup podľa [25] nasledovný:

- Zapísať hodnotu 0x1234 do registra EUDAST
- Načítať register EUDAST a ak jeho hodnota nie je 0x1234 znamená to, že SPI ešte nie je pripravené a treba postup zopakovať
- Vynulovať bit CLKRDY v registri ESTAT a čakať kým sa opäť nenastaví
- Vykonať reset nastavením bitu ETHRST v registri ECON2
- Počkať minimálne 25 μs, aby SPI bolo znovu k dispozícií
- Ak je hodnota registra EUDAST 0x0000 znamená to, že bol reset vykonaný správne
- Počkať minimálne 256 μs

Po tejto procedúre je obvod pripravený prijímať ďalšie príkazy.

4.3.1.2 Zásobník pre prijímanie

Zásobník pre odosielanie sa nastaví zapísaním adresy do ukazateľa ERXST. Potom sa pre príjem paketov využíva pamäť obvodu SRAM medzi adresami ERXST a 0x5FFF. Veľkosť sa určuje podľa odhadu využívania Ethernetu. Podmienkou je, aby adresa uložená v ERXST bola násobkom 2 pre zarovnanie pamäte na 16-bitové dáta.

4.3.1.3 Zásobník pre odosielanie

Zásobník pre odosielanie sa nijako nedefinuje. Dáta sa môžu ukladať do ktorejkoľvek časti nevyužitej pamäte SRAM.

4.3.1.4 Nastavenie filtrov

Nastavením filtrovania určíme, ktoré prijaté pakety sa uložia do pamäte a ktoré boli označené ako nevyžiadané a tým sa zahodia. Filter sa nastavuje registrom ERXFCON. Pre potreby navrhovaného zariadenia je nastanená hodnota 0x005B. To znamená:

- Povolenie broadcast paketov
- Povolenie multicast paketov
- Povolenie paketov s adresou zodpovedajúcou príjemcovi
- Zahodenie paketov menších ako 63 bytov
- Zahodenie paketov s chybným CRC

4.3.1.5 Nastavenie MAC

Nastavenie sa vykoná zmenou obsahu registra MACON2. Podľa [25] však pre väčšinu aplikácií postačuje hodnota uložená po vykonaní resetu. Ďalej sa nastavuje maximálna dĺžka paketov s ktorými sa bude pracovať. Dĺžka v bytoch sa uloží do registra MAMXFL. Pre siete založených na Ethernete je maximálna dĺžka 1518 bytov.

4.3.1.6 Nastavenie PHY

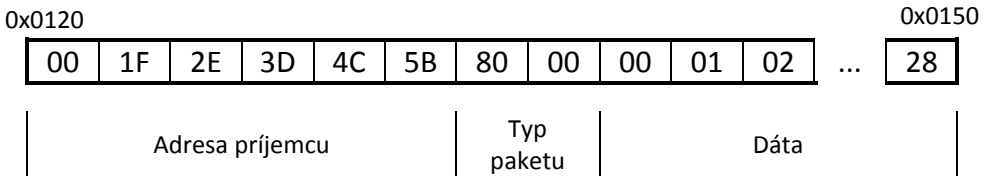
Nastavenie PHY sa vykoná zápisom do registru PHANA. Jeho odporúčaná hodnota je 0x05E1. Ostané hodnoty podľa [25] slúžia skôr pre testovacie účely.

4.3.2 Odoslanie paketu

Pred odoslaním paketu je jeho obsah uložený v pamäti obvodu SRAM. Ten je potom definovaný dvoma hodnotami:

- Počiatočnou adresou ETXST
- Dĺžkou paketu ETXLEN

Požadovaný obsah paketu je závislý od nastavenia MAC vrstvy. Tu je možné nastaviť automatické vkladanie adresy odosielateľa, výpočet CRC alebo dopĺňanie paketu nulami. Na obr. 4.4 je znázornený príklad obsahu pamäte na odoslanie pri nastavenom automatickom dopĺňaní.



Obr. 4.4: Formát odosielaného obsahu s automatickým dopĺňaním

Po nastavení obsahu sa odosielanie začne po nastavení bitu TXRTS v registri ECON1. Po dokončení odosielania sa tento bit automaticky vynuluje.

4.3.3 Prijatie paketu

Prijaté pakety sa ukladajú do kruhového zásobníka, ktorý je vymedzený adresou nastavenou v registri ERXST. Ukladanie je ošetrené aby sa pri zaplnení zásobníka nezačali navzájom prepisovať.

4.3.3.1 Nastavenie príjmu paketov

Po nastavení MAC a PHY je zariadenie pripravené pre príjem paketov. Pred povolením príjmu je potrebné nastaviť ukazatele, aby sa pakety správne ukladali do pamäte SRAM. Povolenie príjmu sa vykoná nasledujúcim postupom:

- S nastavením ukazateľa ERXST sa automaticky nastaví aj ERXHEAD.
- Vytvoriť si v programe premennú NextPacketPointer a priradiť jej hodnotu rovnakú ako ERXST.

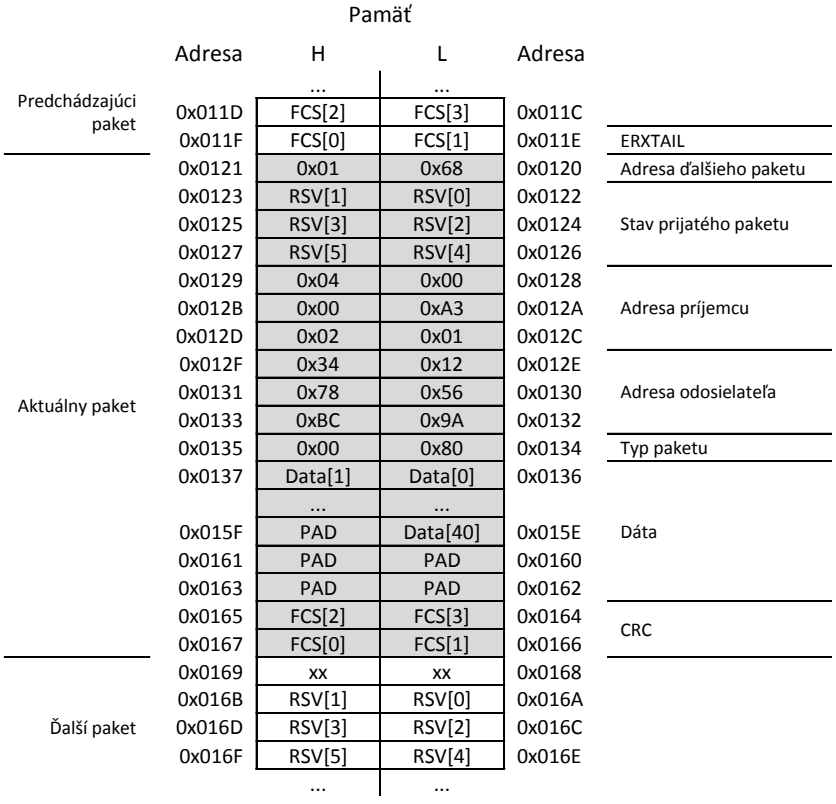
- Nastaviť ukazateľ ERXTAIL na koniec zásobníka hodnotou 0x5FFE.
- Povoliť príjem nastavením bitu RXEN v registri ECON1.

Po povolení príjmu sa už neodporúča meniť veľkosť prijímacieho zásobníka registrom ERXST.

4.3.3.2 Načítanie prijatého paketu zo zásobníka

Po správnom prijatí paketu sa zvýši hodnota registra PKTCNT. Tiež je možné nastaviť, aby sa po prijatí paketu vyvolalo externé prerušenie. Postup načítania je nasledovný:

- Uistiť sa že bol prijatý paket buď načítaním počtu nespracovaných paketov PKTCNT alebo príznakom prerušenia PKTIF v registri EIR.
- Začať načítavať obsah pamäte SRAM na adrese uloženej v NextPacketPointer.
- Načítať prvé 2 byty a uložiť ich do premennej NextPacketPointer.
- Načítať ďalších 6 bytov, ktoré obsahujú stav paketu.
- Načítať rámec Ethernetu, ktorého dĺžka je obsiahnutá v prvých dvoch bytoch načítanom v predchádzajúcom bode.
- Nastaviť adresu v ukazateli ERXTAIL pred začiatok ďalšieho možného paketu (NextPacketPointer – 2). Treba dávať pozor že sa jedná o kruhový zásobník a ošetriť situáciu, keby NextPacketPointer bol na jeho začiatku.
- Nastaviť bit PKTDEC v registri ECON1, čím sa zníži hodnota PKTCNT.



Obr. 4.5: Rozloženie prijatého paketu v pamäti (prevzaté z [25])

4.4 Ovládanie LCD

Použitý radič na LCD je kompatibilný s HD44780. O obsluhe tohto displeja je možno nájsť množstvo zdrojov, preto jeho ovládanie nebude detailne rozoberané. Podrobnejšie informácie je možné nájsť napríklad v [31].

Vo vytvorených knižniciach je implementovaná komunikácia pomocou 4-bitovej zbernice. Ďalej sa tu nachádzajú funkcie pre vypísanie textu, vypínanie displeja, mazanie displeja, načítanie stavu a definíciu vlastných znakov. Tiež bola vytvorená funkcia pre ovládanie jasu podsvietenia pomocou PWM.

4.5 Ovládanie klávesnice

Použitá klávesnica je v maticovom zapojení. Piny ktoré sú pripojené na riadky sú nastavené ako vstupy so zapnutými pull-up rezistormi. Piny pripojené na stĺpce sú nastavené ako výstupy push-pull.

Ovládanie spočíva v postupnom spínaní stĺpcov na nízku úroveň a keď sa na niektorom z pinov objaví tiež nízka úroveň, znamená to že bola stlačená tlačítko na danej pozícií.

4.6 Flash pamäť

Pamäť flash je obsluhovaná pomocou SPI. Ovládanie funkcií prebieha pomocou príkazov, kde prvý byte v prenose je číslo prenosu a ostatné byty sú jeho argumenty. Formáty všetkých príkazov je možné nájsť v [32]. Pri práci s pamäťou je nutné dbať na nasledujúce vlastnosti:

- Pri zápise dát sa pamäťovej bunke vnucuje 0. To znamená že pred zápisom musí byť časť pamäte vymazaná, čím sa bunky nastavia na hodnotu 1.
- Pred zápisom alebo mazaním je potrebné zavolať funkciu pre povolenie zápisu. Po uložení dát sa toto povolenie zruší.
- Všetky sektory sú všetky sektory pamäte chránené pred zápisom. Odstránenie ochrany nefunguje ako v predchádzajúcom prípade, takže ho postačuje vykonať len raz.
- Pri zápise viacerých bytov sa môžu dáta ukladať len v rámci jednej stránky (256 B).

5 Program terminálu

Program pre mikrokontrolér je písaný v jazyku C. Jeho jednotlivé časti budú spomenuté v nasledujúcej kapitole. Výnimku tvorí komunikácia s perifériami ktorých princíp už bol spomenutý.

5.1 Program ako celok

Po spustení programu sa vykoná inicializácia všetkých potrebných periférií mikrokontroléru ako aj k nemu pripojených obvodov. V nasledujúcom kroku sa z pripojenej pamäte flash načítajú potrebné parametre pre chod terminálu. Ich rozmiestnenie znázorňuje tabuľka 5.1. V prípade že je pamäť vymazaná, heslo sa zmení na text „default“, aby bolo možné tieto parametre nastaviť pomocou servisného portu.

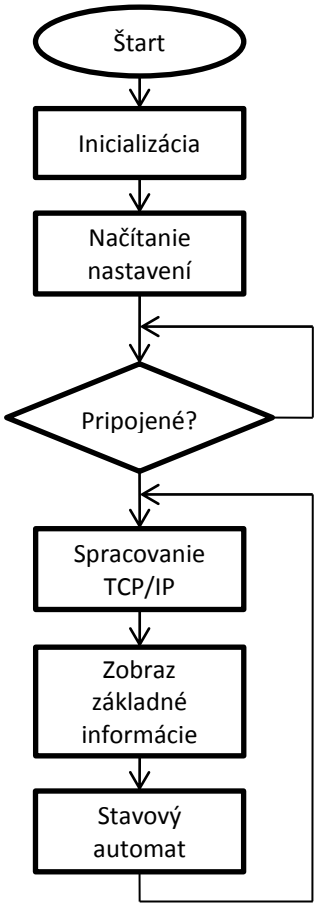
Tabuľka 5.1: Uložené nastavenia v pamäti flash

Funkcia	Počiatočná adresa	Dĺžka [B]
IP adresa terminálu	0x00	4
IP adresa brány	0x04	4
Maska siete	0x08	4
IP adresa servera	0x0C	4
Názov zariadenia	0x10	9
Heslo pre servisný port	0x19	9
Časový interval pre kontrolu dverí	0x22	2
Kalibračná hodnota svetelného senzoru 1	0x24	2
Kalibračná hodnota svetelného senzoru 2	0x26	2
Hodnota pre striedu PWM na zámku	0x28	2

Pred tým ako program vojde do nekonečnej slučky, testuje sa pripojenie do siete Ethernet. V prípade že tomu tak nie je, program sa na tomto mieste zastaví pokiaľ zariadenie nebude pripojené.

V hlavnej slučke sa vykonáva spracovanie komunikácie po sieti Ethernet a vykonanie aktuálneho stavu v stavovom automate ktorý ma za úlohu spracovávať údaje od užívateľa. Takáto štruktúra bola zvolená vzhľadom na použitý TPC/IP stack uIP [33]. Opísaný algoritmus je znázornený na obr. 5.1.

Popri hlavnom behu programu je pomocou prerušení spracovávaná komunikácia cez servisný port, obnova hodnôt hodín a obsluha A/D prevodníka.

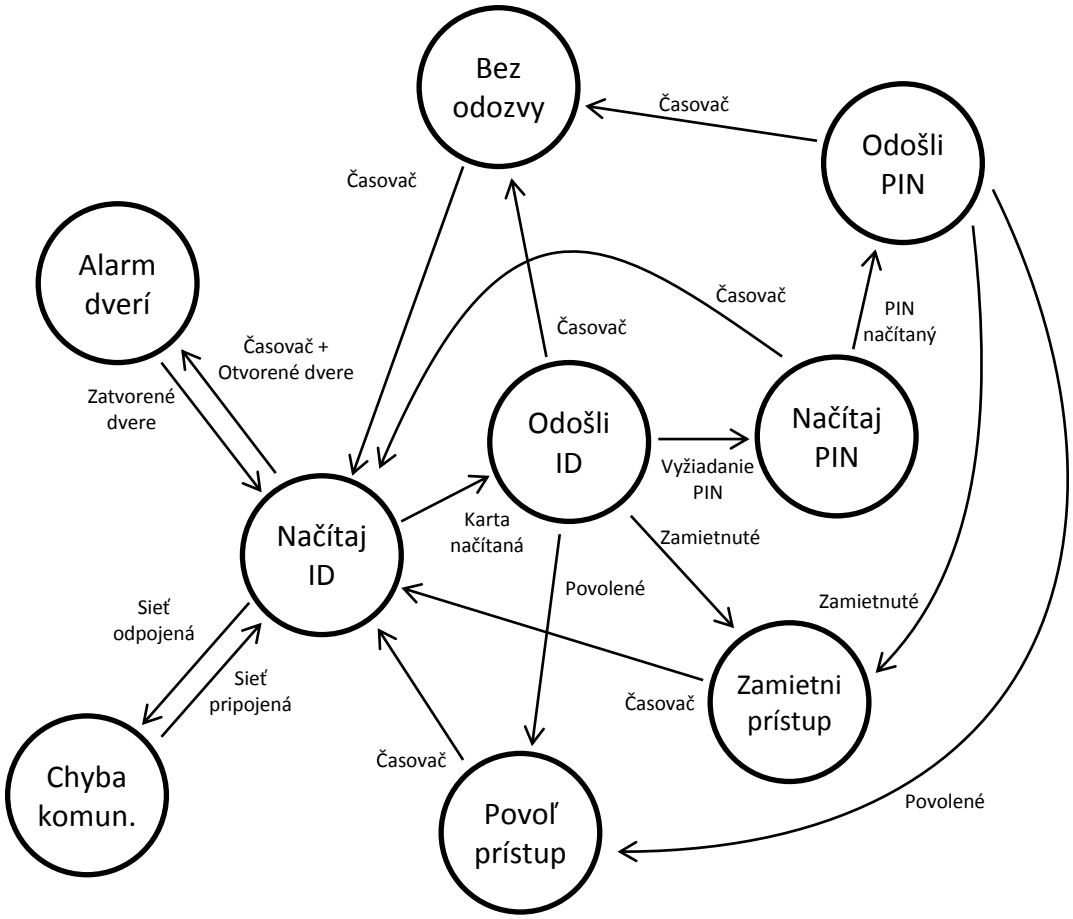


Obr. 5.1: Vývojový diagram hlavného behu programu

5.2 Stavový automat

Keďže použitý TCP/IP stack je vytvorený tak že nevyužíva systém prerušenia, musí byť neustále kontrolovaný. Kvôli tejto vlastnosti nie je možné počas behu programu čakať na načítanie RFID tagu alebo zadanie PINu na klávesnici. Preto komunikácia s užívateľom a k nej pridružené funkcie pracuje ako stavový automat. Jeho realizácia je znázornená na obr. 5.2.

V počiatočnom stave sa terminál pokúša načítať sériové číslo RFID tagu. Po jeho úspešnom zistení ho odošle serveru a čaká na ďalšie pokyny. Server môže hneď rozhodnúť o prístupe užívateľa alebo po ňom požadovať jeho PIN. Ak je vyžadovaný PIN tak po jeho načítaní sa opäť odošle a čaká sa na vyhodnotenie serverom. Celé vyhodnocovanie oprávnenosti prístupu je tým pádom presunuté na aplikáciu servera.



Obr. 5.2: Stavový diagram automatu v termináli

Stavový automat je ošetrený časovačmi, ktoré zamedzujú programu aby trvalo pretrval v stavoch kedy užívateľ pristupuje do systému. Taký stav by nastal keby sa niektoré činnosti nedokončili. Ide hlavne o nadväzovanie spojenia medzi terminálom a serverom alebo nezadanie PINu na klávesnici.

V automate sú navyše doplnené funkcie pre kontrolu pripojenia do siete a kontrola uzavretia dverí. Ak by užívateľ za sebou nezavrel dvere tak sa po čase spustí akustická signalizácia pre jeho upozornenie.

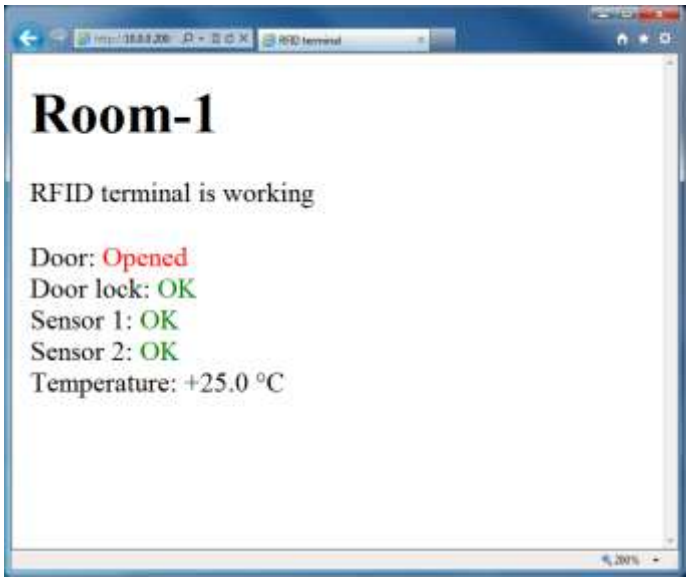
5.3 Komunikácia pomocou TCP/IP

Ako už bolo spomenuté tak komunikácia prebieha pomocou stacku uIP [33]. Jedná sa o open-source TCP/IP stack pôvodne určený pre embedded zariadenia využívajúce 8 a 16-bitové mikrokontroléry. Vďaka tomu je nenáročný na množstvo použitej pamäte. Obsahuje podporu protokolov ARP, IP, UDP, ICMP a TCP. Pri konfigurácií stacku však podpora UDP nebola povolená.

Aby bolo možné používať spomenutý TCP/IP stack, museli byť vytvorené závislé na zariadení. Ide o funkcie odoslania a prijatia paketu a načítanie hodnoty čítača/časovača.

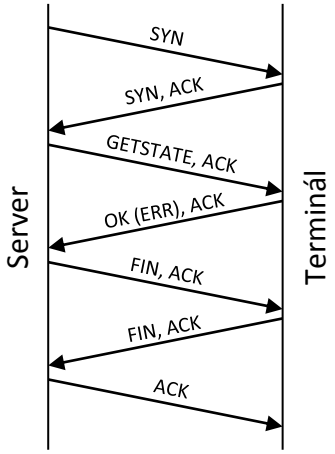
5.3.1 Aplikačná vrstva TCP/IP

V aplikačnej vrstve boli vytvorené 3 funkcie. Prvou je jednoduchý webový server pomocou ktorého sa dá overiť funkcia terminálu. Po zadaní adresy v internetovom prehliadači sa zobrazia informácie o stave dverí, pripojení zámku a optických snímačoch (obr. 5.3). V prípade že by sa na terminál pristupovalo z iného počítača ako je server, tak sa tieto informácie nezobrazia.



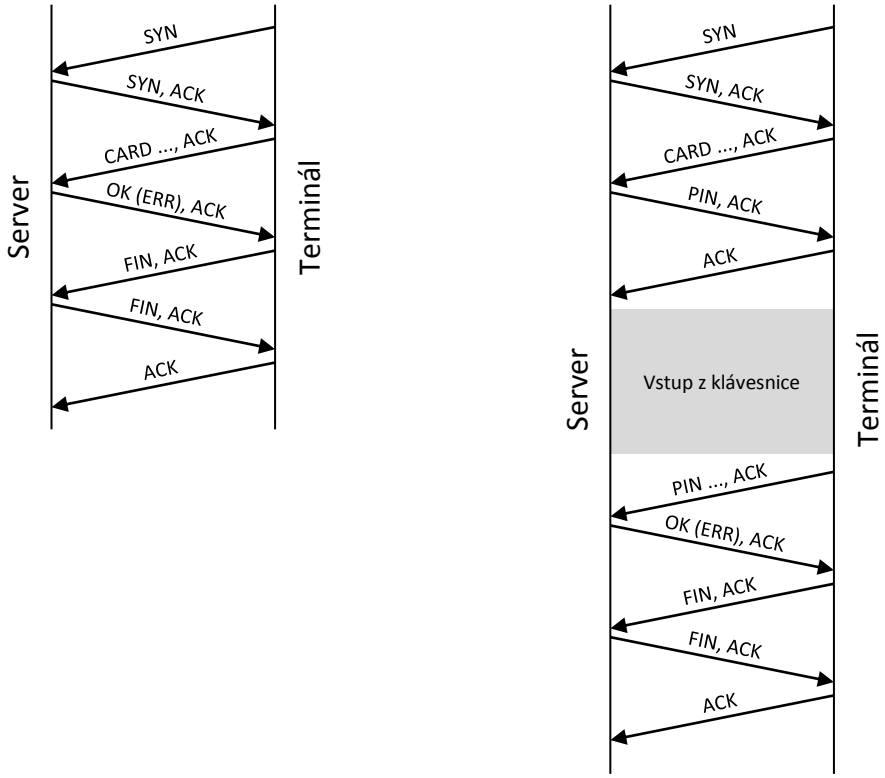
Obr. 5.3: Zobrazované informácie pomocou HTTP

Ďalšia funkcia je odpoveď na požiadavku servera o stave terminálu. Pri tejto požiadavke si terminál zároveň aktualizuje svoj čas, pretože je v požiadavke umiestnená časová značka. Formát správy je „DD. MM. RRRR HH:MM:SS GETSTATE“. Odpovede na požiadavku sú buď „OK“ alebo „ERR“. Za chybu sa považuje odpojenie zámku, dlhodobé otvorenie dverí a osvetlenie senzorov. Podobne ako v predchádzajúcom prípade, tak aj tu terminál odpovedá len na požiadavku odoslanej z adresy servera. Priebeh znázorňuje obr. 5.4.



Obr. 5.4: Komunikácia pri kontrole stavu

Posledná funkcia je nadviazanie komunikácie so serverom po načítaní RFID tagu a vyžiadanie informácie o oprávnenosti vstupu. Po nadviazaní spojenia je odoslaná požiadavka „CARD xxxxxxxxx“ kde je sériové číslo tagu v hexadecimálnom tvare. Odpovede na požiadavku môžu byť „OK“, „ERR“ alebo „PIN“. Po odpovedi „PIN“ je používateľ požiadaný o zadanie svojho čísla ktoré je následne odoslané v tvare „PIN xxxx“. Odpovede môžu byť už len „OK“ alebo „ERR“. Odpoveď „ERR“ v sebe nesie tiež dôvod zamietnutia, ktorý sa zobrazí na displeji terminálu.

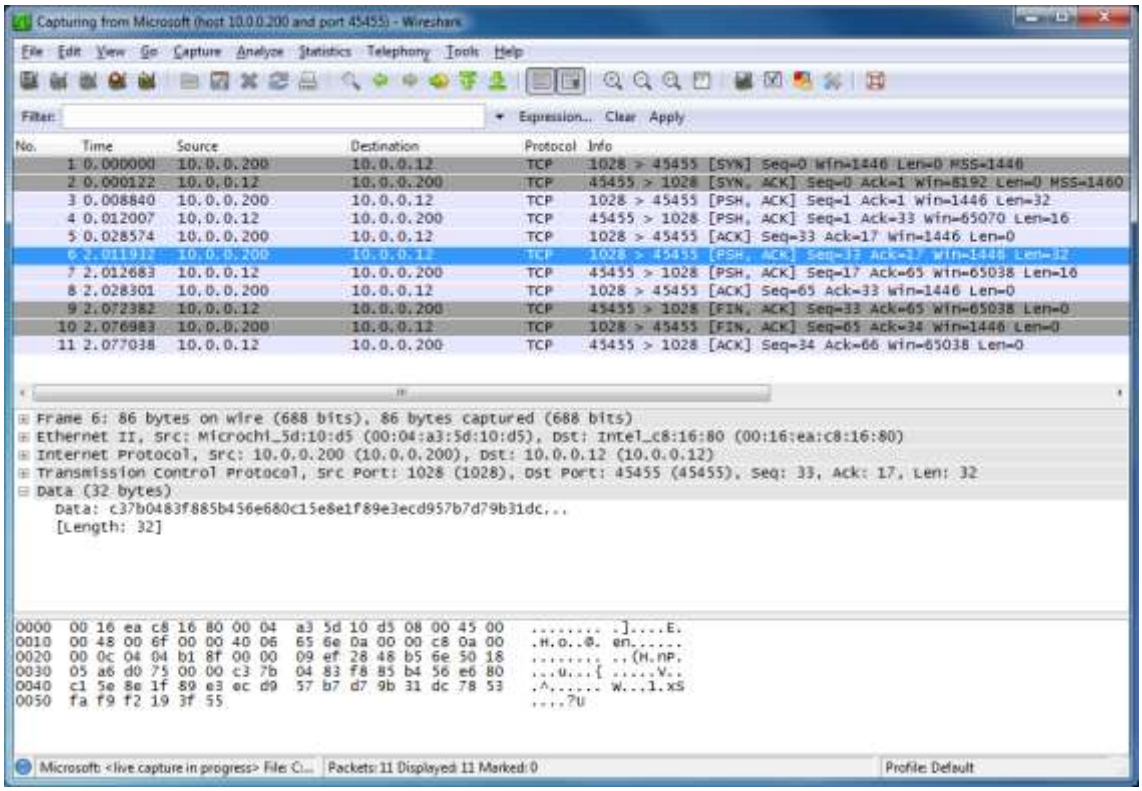


Obr. 5.5: Komunikácia počas prístupu užívateľa

5.3.2 Zabezpečenie prenosu

Požiadavky medzi terminálom a serverom sa spracovávajú ako textové reťazce. Ak by takto boli aj prenášané, hrozilo by riziko odchytenia a následného zneužitia získaných informácií. Z toho dôvodu je prenos šifrovaný algoritmom AES s veľkosťou kľúča 128 bitov.

Na obr. 5.6 je zachytený priebeh komunikácie medzi terminálom a serverom počas jedného prístupu užívateľa. Označený paket v sebe obsahuje PIN zadaný užívateľom. Je vidieť že na prvý pohľad nie je možné rozoznať o akú správu sa jedná.

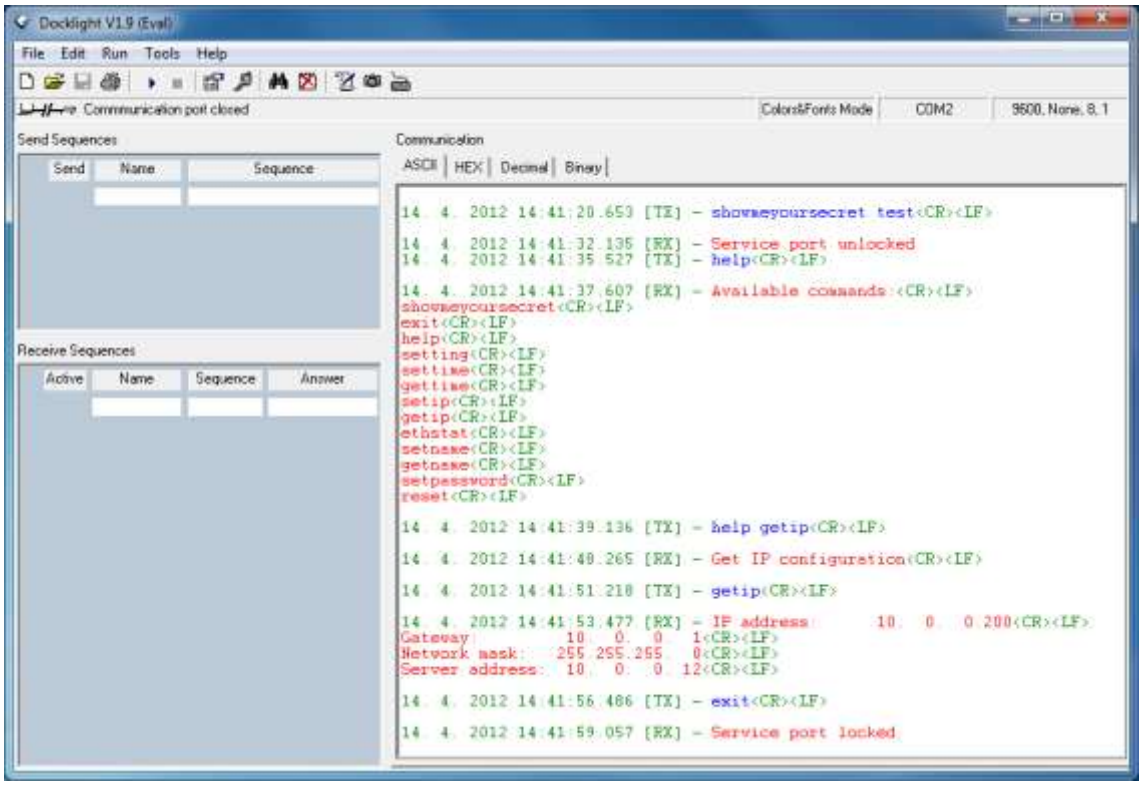


Obr. 5.6: Zachytená komunikácia medzi terminálom a serverom

5.4 Servisný port

Servisný port je realizovaný ako sériová linka RS232. Pomocou neho sa v termináli nastavujú jeho parametre. Komunikácia prebieha v textovej podobe pomocou konzoly, takže pre nastavenie terminálu nie je potrebný žiadny špeciálny software. Jednotlivé príkazy sa však sprístupnia až po prihlásení heslom. Pokiaľ heslo nie je zadané, terminál na požiadavky užívateľa neodpovedá. Príklad komunikácie je zobrazený na obr. 5.7.

Aby komunikácia sériovej linky neobmedzovala beh programu čakaním na načítanie alebo odoslanie reťazcov, sú tieto správy postupne ukladané do zásobníka a spracovávané pri volaní prerušenia od sériovej linky. Vykonanie príkazu sa realizuje hneď po prijatí posledného znaku reťazca pred návratom z prerušenia.



Obr. 5.7: Komunikácia pomocou servisného portu

6 Aplikácia pre server

Server má za úlohu kontrolovať jednotlivé registrované terminály a spracovávať ich požiadavky. Pre tento účel bola vytvorená aplikácia, ktorá tieto úlohy vykonáva. Tá je realizovaná v jazyku C# s použitím frameworku .NET vo vývojovom prostredí Visual Studio 2008. Funkcia aplikácie bude vysvetlená v nasledujúcej kapitole.

6.1 Databáza

Aby bolo možné kontrolovať terminály a ich užívateľov, je potrebné udržiavať ich zoznam v pamäti. K tomuto slúži databáza obsahujúca 4 tabuľky, ktorých funkcia je opísaná nižšie.

Prvá tabuľka s názvom „Terminals“ obsahuje informácie o registrovaných termináloch. Číslo terminálu je automaticky generované pri vytvorení záznamu. Parameter „StatusOK“ sa v databáze nachádza, ale pri jej uložení sa automaticky maže.

Tabuľka 6.1: Štruktúra tabuľky obsahujúcej zoznam terminálov

Názov	Typ	Funkcia
ID	Int32	Unikátne číslo terminálu
Name	String	Názov terminálu
IP	String	IP adresa terminálu
StatusOK	Boolean	Odpoveď na požiadavku o stave terminálu
RequiredPIN	Boolean	Požadovať PIN užívateľa pri vstupe

Zoznam užívateľov sa uchováva v tabuľke „Users“. Jej funkcia je podobná ako v predchádzajúcom prípade.

Tabuľka 6.2: Štruktúra tabuľky obsahujúcej zoznam užívateľov

Názov	Typ	Funkcia
ID	Int32	Unikátne číslo užívateľa
Name	String	Meno užívateľa
CardNo	String	Číslo karty v hexadecinálnom tvare
PIN	String	Osobné identifikačné číslo užívateľa
Blocked	Boolean	Označenie blokovanej karty
FailCounter	Byte	Počet chybných pokusov pri zadávaní PIN

Aby bolo možné triediť užívateľov medzi jednotlivé prístupové body, je potrebné medzi sebou priradiť záznamy z prvých dvoch tabuliek. K tomuto účelu slúži tabuľka „UserToTerminal“. Tá v sebe obsahuje záznamy s pármi identifikačných čísel užívateľa a terminálu.

Tabuľka 6.3: Štruktúra tabuľky priradenia užívateľa s terminálom

Názov	Typ	Funkcia
UserID	Int32	Unikátne číslo užívateľa
TerminalID	Int32	Unikátne číslo terminálu

Posledná tabuľka „Logging“ slúži pre záznam akcií užívateľov v prístupovom systéme.

Tabuľka 6.4: Štruktúra tabuľky záznamu akcií

Názov	Typ	Funkcia
UserID	Int32	Unikátne číslo užívateľa
TerminalID	Int32	Unikátne číslo terminálu
Time	DateTime	Čas vykonania akcie
Action	String	Popis akcie

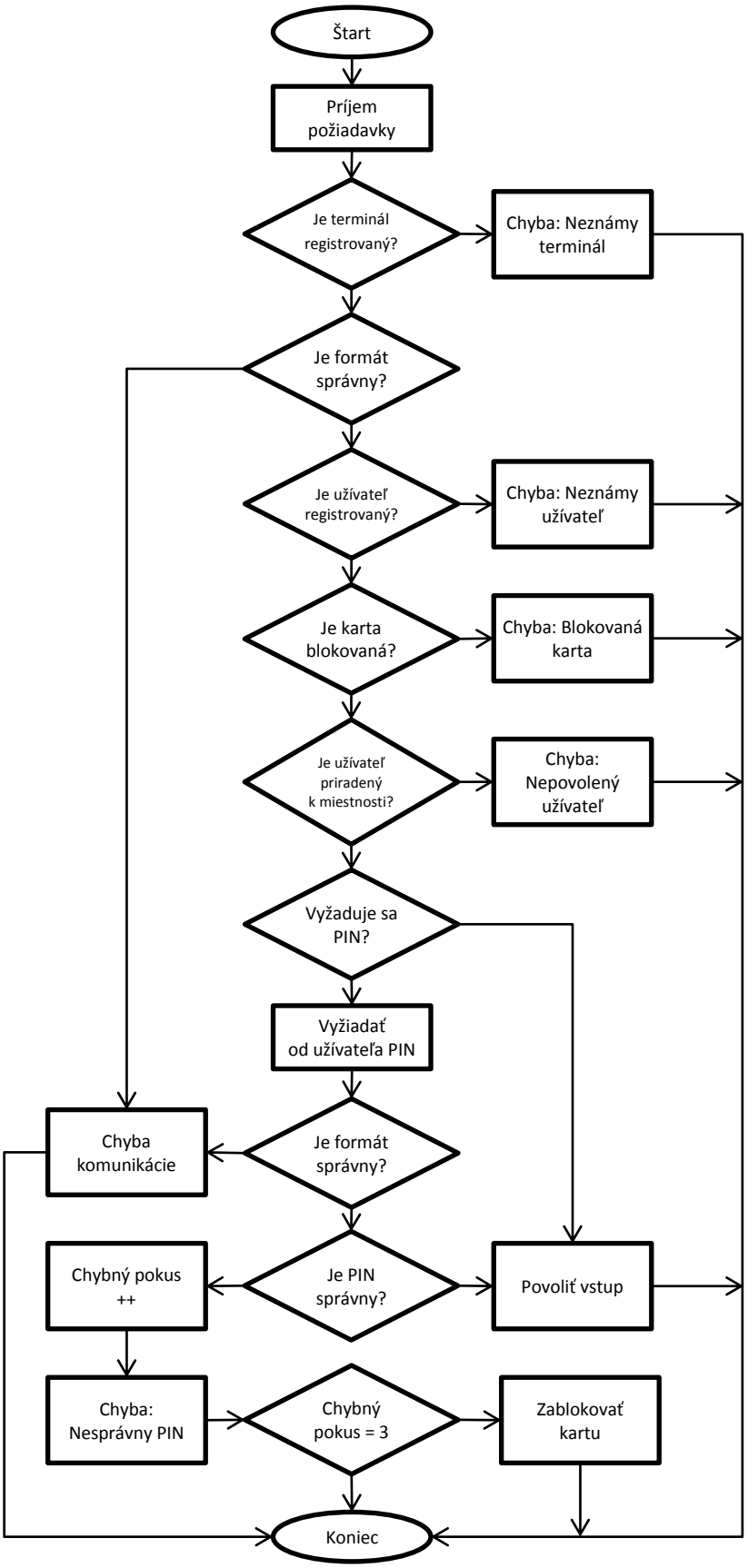
6.2 Komunikácia s terminálmi

Komunikácia s terminálmi prebieha v krokoch popísanými v kapitole 5.3. Kontrola stavu jednotlivých terminálov prebieha postupne podľa zoznamu v tabuľke. Táto kontrola sa vykonáva každých 10 s pre všetky terminály. Pred tým než sa s terminálom aplikácia pokúsi nadviazať spojenie, je na terminál odoslaná správa protokolu ICMP „Echo request“, aby sa zistilo či je terminál dosiahnuteľný. Tento postup bol zvolený pretože sa v .NET nedá pri nadväzovaní spojenia nastaviť timeout. Ak by sa aplikácia pokúsila nadviazať spojenie bez tejto kontroly a terminál by bol odpojený, jej beh by sa výrazne spomalil a nemusela by odpovedať na ostatné požiadavky jej užívateľa.

Príjem požiadaviek terminálov je v aplikácií spracovávaný v inom vlákne. Toto vlákno má za úlohu čakať na prichádzajúce spojenie. V prípade nadviazania spojenia sa vytvorí ďalšie vlákno určené len pre komunikáciu pre konkrétny terminál. Takto sa môže vybavovať viacero požiadaviek naraz.

6.3 Spracovanie požiadavky

Ako už bolo spomenuté, každá požiadavka sa spracováva vo svojom vlákne. Po jej prijatí sa vyhodnotí oprávnenosť vstupu a odošle sa jeho výsledok. Počas spracovania môže byť dodatočne od užívateľa požadovaný PIN. Tým pádom kontrola užívateľa môže byť menená len zmenou riadiacej aplikácie v serveri a táto zmena nebude vyžadovať zmenu programu v termináloch. Postup vyhodnocovania prístupu užívateľa je znázornený na obr. 6.1.

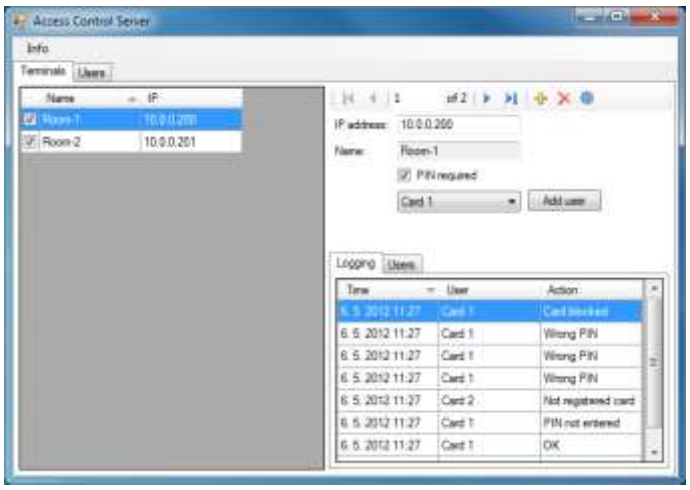


Obr. 6.1: Algoritmus vyhodnocovania prístupu užívateľa

6.4 Užívateľské prostredie

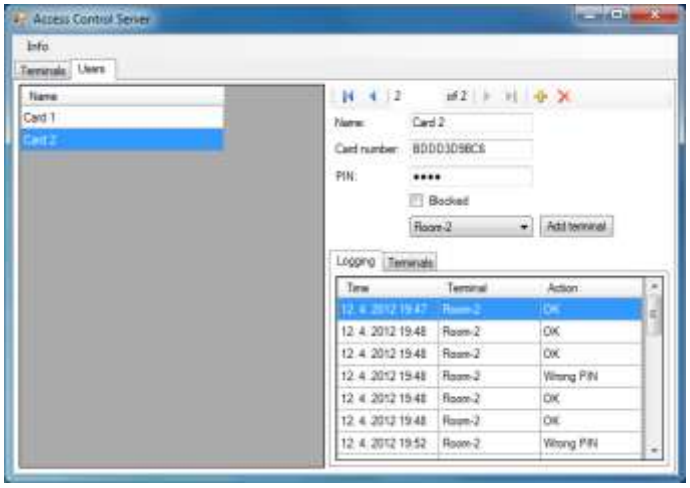
Používateľské prostredie je delené do dvoch hlavných častí. Prvá časť slúži pre správu terminálov a druhá pre správu užívateľov. Prepínanie medzi nimi prebieha pomocou záložiek vo vrchnej časti okna.

V záložke správy terminálov (obr. 6.2) sa v ľavej časti okna nachádza zoznam registrovaných terminálov. V zozname je tiež označený ich stav po kontrole. V pravej časti je možné zobraziť, prípadne upraviť vlastnosti zvoleného terminálu zo zoznamu. Tiež je možné zobraziť si vyfiltrovaný záznam vykonaných akcií alebo priradených užívateľov.



Obr. 6.2: Užívateľské prostredie správy terminálov

Správa užívateľov je v podstate rovnaká ako správa terminálov. Rozdiel je v položkách ktoré je možné upravovať. Ak sa povolí užívateľovi prístupový bod, nie je potrebné túto zmenu vykonať v správe terminálov, pretože sa jedná o tú istú tabuľku v inom zobrazení.



Obr. 6.3: Užívateľské prostredie správy užívateľov

7 Záver

V práci bol uvedený základný princíp činnosti technológie RFID. Tiež boli spomenuté možné bezpečnostné riziká spojené s jej používaním, ako aj možnosti ako by sa takéto riziko dalo znížiť.

Počas riešenia projektu boli navrhnuté dve zariadenia. Ako prvá bola navrhnutá a skonštruovaná čítačka k PC. V dobe návrhu bol na trhu nedostatok integrovaných obvodov pre prácu s MiFare, takže pracuje s jednoduchšími tagmi na frekvencií 125 kHz. Prístupový terminál už pracuje na frekvencií 13,56 MHz. Prototypy terminálu boli vytvorené dva. Na prvom boli osadené súčiastky s vypočítanými hodnotami, prípadne odporúčanými výrobcom. Následne tieto hodnoty boli odladené a po úpravách bol vytvorený druhý prototyp ktorého dokumentácia je v prílohách. Na ňom už po osadení súčiastok nebol potrebný žiadny ďalší zásah v obvodovom zapojení.

Technológia pracujúca na frekvencií 125 kHz má výhody v nízkej cene, jednoduchosti návrhu a vyššej vzdialenosti na ktorú je možné načítať tag. Tá sa pohybuje v rozsahu 5 – 10 cm od antény v závislosti na jeho vyhotovení. Technológia MiFare prináša viac možností pre zabezpečenie systému. To je však sprevádzané vyššou cenou a väčšou zložitosťou návrhu. Vzdialenosť načítania tagu je približne 4 cm od antény. Porovnanie vychádza z návrhov uvedených v práci, takže uvedené vzdialenosti sa môžu meniť v závislosti od vyhotovenia antény.

Pre prístupový systém bola tiež vytvorená riadiaca aplikácia ktorá s jednotlivými bodmi pracuje prostredníctvom počítačovej siete. Tá v sebe obsahuje základné funkcie pre zabezpečenie systému. Bez zásahu do firmwaru terminálov by bolo možné pridať napríklad funkcie pre vyhodnocovanie prístupov na základe topológie budovy v ktorej je systém umiestnený.

Pri testovaní systému v reálnej sieti s malým počtom zariadení pri požiadavkách o prístup od užívateľa nenastávali žiadne problémy. Pri kontrole stavu terminálu sa pri zvýšenom čase odozvy v sieti občas stávalo, že aplikácia chybne vyhodnotila že je terminál nedostupný. Pri zvýšení hodnoty timeout pre ping v aplikácií sa tento problém odstránil, avšak nie je vylúčené že by sa pri väčšej prevádzke neobjavili chybné varovania znova. Pri vytváraní požiadaviek z viacerých terminálov a tým aj vytváraní viacerých vláken v aplikácií sa objavoval problém s tým, že sa niektoré vlákna neukončili. Prejav bol taký, že po zatvorení okna sa aplikácia neukončila úplne, ale zostala v zozname spustených procesov.

V prípade že by sa na projekte pokračovalo, mala by sa práca zamerať hlavne na zlepšenie aplikácie pre PC, pretože v tomto štádiu slúži skôr na demonštračné účely. Okrem úpravy komunikácie medzi aplikáciou a terminálom sa môže vylepšiť

užívateľské rozhranie alebo pridať ďalšie funkcie, ktoré by zvyšovali bezpečnosť systému. Do samotného terminálu by sa mohli pridať funkcie, vďaka ktorým by mohol byť umožnený prístup do miestnosti aj v prípade výpadku komunikácie so serverom. To by sa dalo realizovať len zmenou programu, pretože obvodové zapojenie takúto vec umožňuje vďaka prítomnosti dostatočne veľkej pamäte flash.

Použitá literatúra

[1] **RFID Journal.** *A Summary of RFID Standards.* [Online] 2005. [Dátum: 21. Apríl 2011] <http://www.rfidjournal.com/article/view/1335/>.

[2] **Finkenzeller, Klaus.** *RFID Handbook.* Chichester : Wiley & Sons, 2003. ISBN 0-470-84402-7.

[3] **Aikaterini Mitrokotsa, Melanie R. Rieback a Andrew S. Tanenbaum.** *Classification of RFID Attacks.* [Online] 2008. [Dátum: 22. Apríl 2011] <http://www.cs.vu.nl/~ast/publications/iwrt-2008.pdf>.

[4] **Půhoný, Jan.** *RFID Zapper.* [Online] 2006. [Dátum: 1. Máj 2011] <http://hw.cz/Teorie-a-praxe/Navrhy-vyvojare/ART1641-RFID-Zapper.html>.

[5] **Krumnikl, Michal.** *Unique (EM4001) RFID Emulator.* [Online] 2007. [Dátum: 22. Apríl 2011] <http://mrl.cz/projects/rfid/rfid.pdf>.

[6] **Meriac, Milosch, Meriac, Brita a Welte, Harald.** *OpenPCD Passive RFID Project.* [Online] 2007. [Dátum: 22. Apríl 2011] <http://www.openpcd.org/>.

[7] **Řehák, Jan a Staněk, Jan.** *RS 485 & 422.* [Online] 1998. [Dátum: 24. Apríl 2011] <http://hw.cz/Teorie-a-praxe/Dokumentace/ART821-RS-485-422.html>.

[8] **EM Microelectronic-Marin SA.** *RFID Circuits.* [Online] 2012. [Dátum: 5. Máj 2012] <http://www.emmicroelectronic.com/Line.asp?IdLine=3>.

[9] **Atmel Corporation.** *T5557.* [Online] 2006. [Dátum: 5. Máj 2012] <http://www.atmel.com/devices/t5557.aspx>.

[10] **NXP Semiconductors.** HITAG transponder ICs have served low-frequency applications for more than 15 years. [Online] 2010. [Dátum: 5. Máj 2012] <http://www.nxp.com/products/identification_and_security/smart_label_and_tag_ics/hitag/>.

[11] **NXP Semiconductors**. *MIFARE™ Security.* [Online] 2011. [Dátum: 30. Apríl 2011] <http://www.mifare.net/technology/security/>.

[12] **SOS electronic.** *Online katalóg.* [Online] 2011. [Dátum: 1. Máj 2011] <http://www.sos.sk/>.

[13] **Farnell.** *Online katalóg.* [Online] 2011. [Dátum: 1. Máj 2011] <http://sk.farnell.com/>.

[14] **Netronix.** *MM-U57D, D5, Z5.* [Online] 2011. [Dátum: 5. Máj 2012] <http://www.netronix.pl/product.php?no=56>.

[15] **Shenzhen Sunbest Technology Co., Ltd.** *SB2230/2240.* [Online] 2007. [Dátum: 5. Máj 2012] <http://www.sunbestrfid.com/showproduct_e.php?ref=sb2230-2240&l=e>.

[16] **NXP Semiconductors.** *MIFARE™ Reader ICs.* [Online] 2011. [Dátum: 2. December 2011] <http://mifare.net/products/mifare-reader-ic-s/>.

[17] **CB elektro.** *Elektroinštalačný materiál.* [Online] 2011. [Dátum: 1. Máj 2011] <http://www.cbelektro.sk/>.

[18] **Mrázek, Oldřich.** *Power Over Ethernet - napájení ethernetových zařízení po datovém kabelu.* [Online] 2004. [Dátum: 1. Máj 2011.] <http://hw.cz/Produkty/Ethernet/ART1068-Power-Over-Ethernet.html>.

[19] **EM Microelectronic-Marin SA.** *Read/Write analog front end for 125kHz RFID Basestation.* [Online] 2011. [Dátum: 2. December 2011] <http://www.emmicroelectronic.com/webfiles/product/rfid/ds/EM4095_DS.pdf>.

[20] **Microchip Technology.** *Antenna Circuit Design for RFID Applications.* [Online] 2003. [Dátum: 2. December 2011] <http://ww1.microchip.com/downloads/en/AppNotes/00710c.pdf>.

[21] **EM Microelectronic-Marin SA.** *EM4095 Application Note.* [Online] 2002. [Dátum: 2. December 2011] <http://www.emmicroelectronic.com/webfiles/product/rfid/an/an404.pdf>.

[22] **Future Technology Devices International.** *FT232R USB UART IC.* [Online] 2010. [Dátum: 2. December 2011] <http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT232R.pdf>.

[23] **NXP Semiconductors.** *MFRC530; ISO/IEC 14443 A Reader IC.* [Online] 2010. [Dátum: 3. December 2011] <http://www.nxp.com/documents/data_sheet/MFRC530.pdf>.

[24] **NXP Semiconductors**. *Micore Reader IC Family; Directly Matched Antenna Design.* [Online] 2006. [Dátum: 2. December 2011] <http://www.nxp.com/documents/application_note/077925.pdf>.

[25] **Microchip Technology.** *ENC424J600/624J600 Data Sheet.* [Online] 2009. [Dátum: 3. December 2011] <http://ww1.microchip.com/downloads/en/DeviceDoc/39935b.pdf>.

[26] **Maxim Integrated.** *MAX3222/MAX3232/MAX3237/MAX3241.* [Online] 2007. [Dátum: 3. December 2011] <http://datasheets.maxim-ic.com/en/ds/MAX3222-MAX3241.pdf>.

[27] **Texas Instruments.** *Integrated 100-V IEEE 802.3af PD and DC/DC Controller (Rev. B).* [Online] 2008. [Dátum: 3. December 2011] <http://www.ti.com/lit/ds/symlink/tps23750.pdf>.

[28] **Texas Instruments**. *Precision Programmable Reference.* [Online] 2011. [Dátum: 3. December 2011] <http://www.ti.com/lit/ds/symlink/tl431.pdf>.

[29] **Atmel Corporation.** *Manchester Coding Basics.* [Online] 2009. [Dátum: 6. December 2011] <http://www.atmel.com/dyn/resources/prod_documents/doc9164.pdf>.

[30] **EM Microelectronic-Marin SA.** *EM4100 Read Only Contactless Identification Device.* [Online] 2004. [Dátum: 6. December 2011] <http://www.mikroe.com/eng/downloads/get/1084/em4100_datasheet.pdf>.

[31] **Maslan, Stanislav.** *Ovládání znakových LCD s řadičem HD44780.* [Online] 2009. [Dátum: 9. December 2011] <http://www.hw.cz/novinky/art2727-ovladani-znakovych-lcd-s-radicem-hd44780.html>.

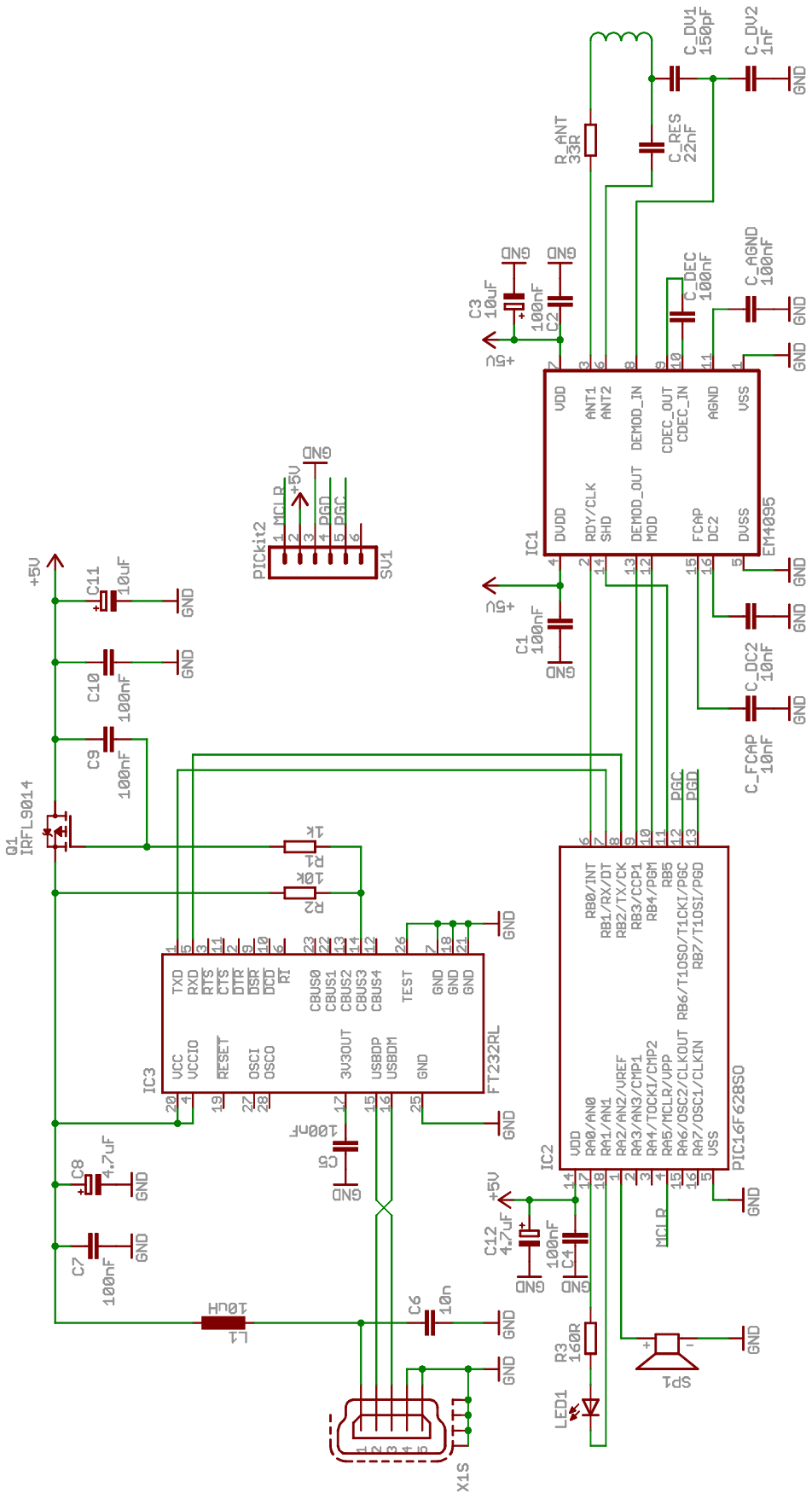
[32] **Atmel Corporation.** *AT25DF041A; SPI Serial Flash.* [Online] 2008. [Dátum: 2011. December 2011] <http://www.atmel.com/dyn/resources/prod_documents/doc3668.pdf>.

[33] **Dunkels, Adam.** *The old webpages for the uIP Embedded TCP/IP Stack.* [Online] 2006. [Dátum: 28. Február 2012] <http://www.sics.se/~adam/old-uip>.

Zoznam príloh

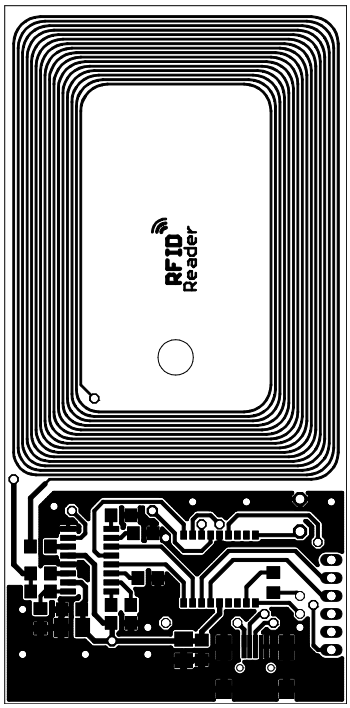
A Schéma zapojenia čítačky k PC 57
B Motív plošného spoja čítačky k PC 58
C Osadenie súčiastok čítačky k PC 59
D Zoznam súčiastok čítačky k PC 60
E Namerané priebehy na čítačke k PC 61
F Fotografie čítačky k PC 62
G Schéma zapojenia terminálu 63
H Motív plošného spoja terminálu 66
I Osadenie súčiastok terminálu 68
J Zoznam súčiastok terminálu 70
K Namerané priebehy na termináli 72
L Fotografie terminálu 73

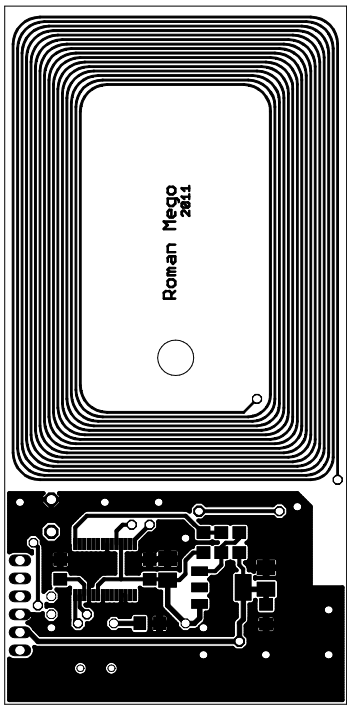
A Schéma zapojenia čítačky k PC



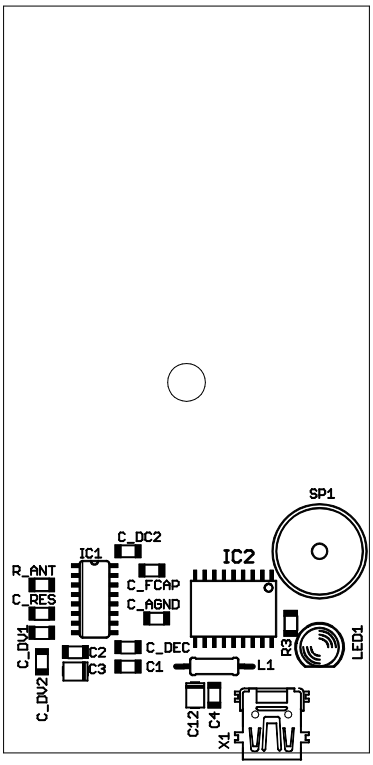
B Motív plošného spoja čítačky k PC

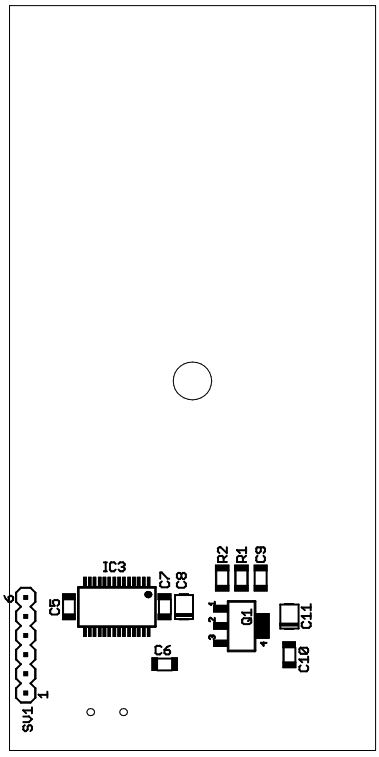
Rozmer: 48,5 mm x 98,7 mm





C Osadenie súčiastok čítačky k PC

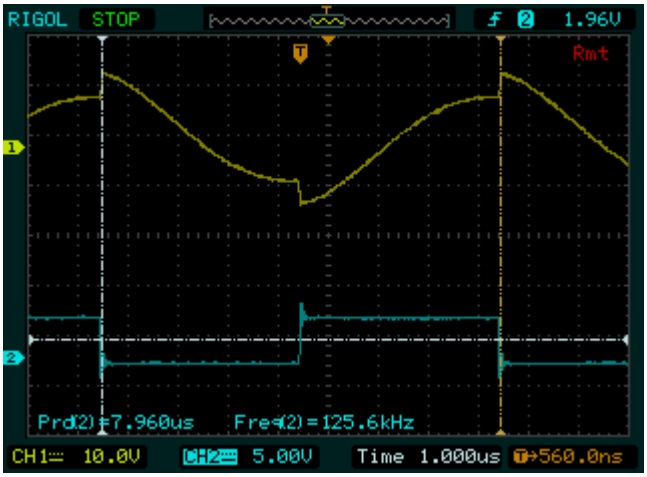




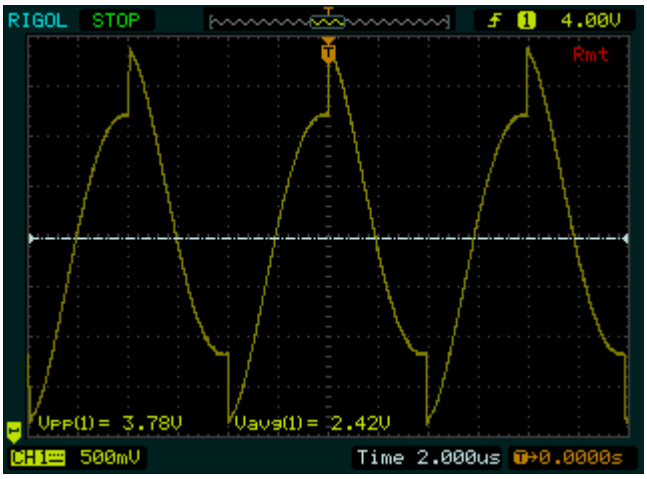
D Zoznam súčiastok čítačky k PC

Označenie	Hodnota	Puzdro
C1	100nF	C1206
C2	100nF	C1206
C3	10uF	SMD B
C4	100nF	C1206
C5	100nF	C1206
C6	10nF	C1206
C7	100nF	C1206
C8	4.7uF	SMD B
C9	100nF	C1206
C10	100nF	C1206
C11	10uF	SMD B
C12	4.7uF	SMD B
C_AGND	100nF	C1206
C_DC2	10nF	C1206
C_DEC	100nF	C1206
C_DV1	150pF	C1206
C_DV2	1nF	C1206
C_FCAP	10nF	C1206
C_RES	22nF	C1206
IC1	EM4095	SO16
IC2	PIC16F628SO	SO-18W
IC3	FT232RL	SSOP28
L1	10uH	0207/10
LED1		LED 5mm
Q1	IRFL9014	SOT223
R1	1k	R1206
R2	10k	R1206
R3	160R	R1206
R_ANT	33R	R1206
SP1	AL11P	
X1	MINI-USB	

E Namerané priebehy na čítačke k PC

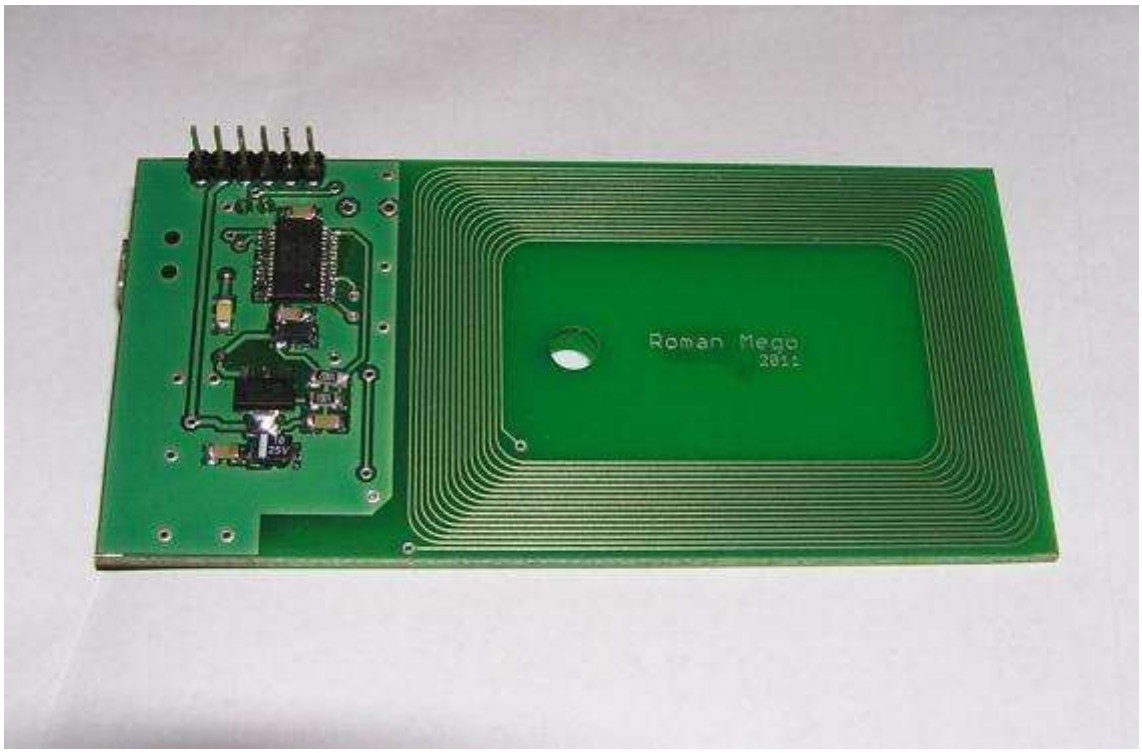


Priebeh signálu medzi anténou a C_RES (CH1) a výstupe CLK/RDY (CH2)

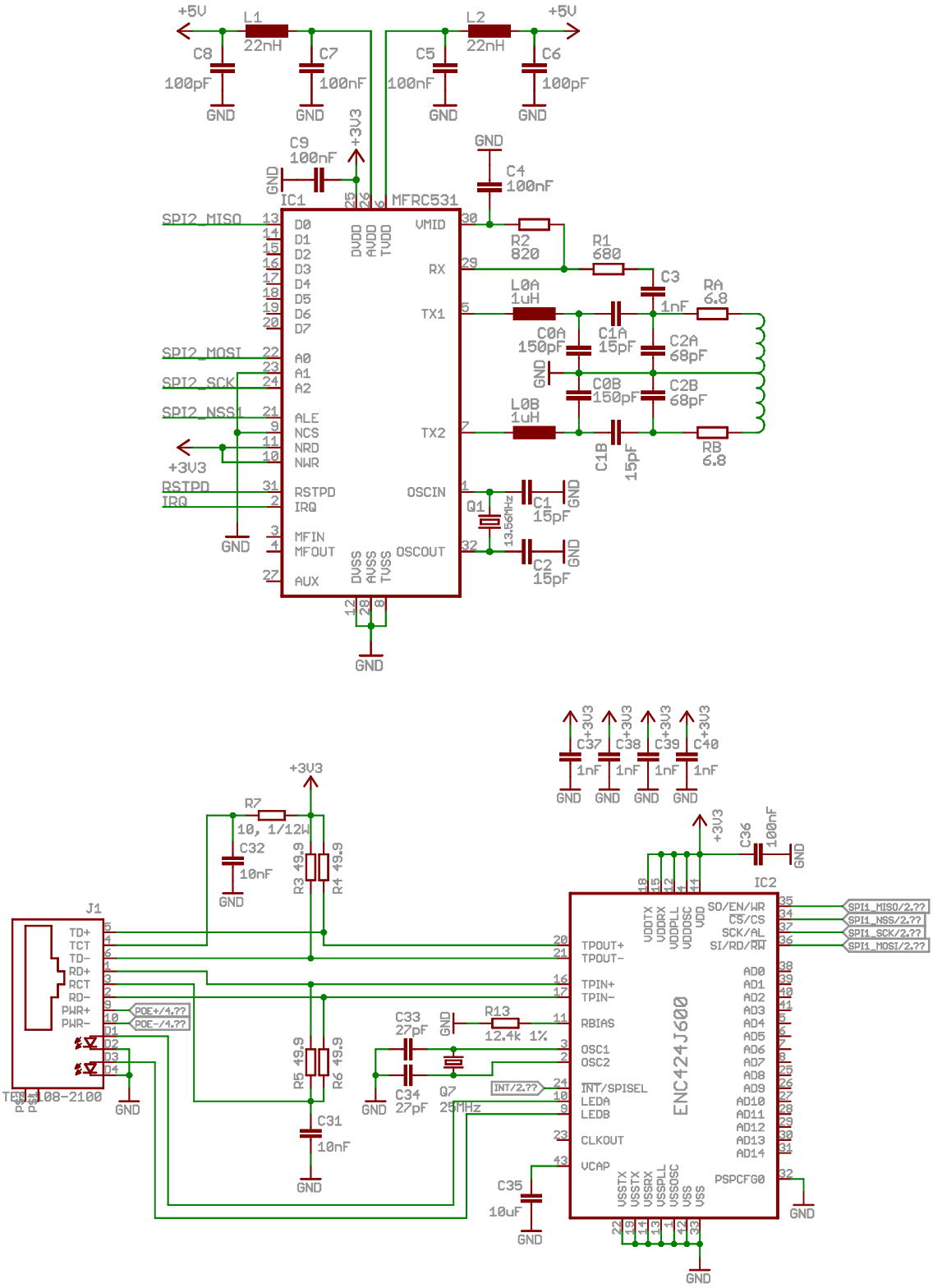


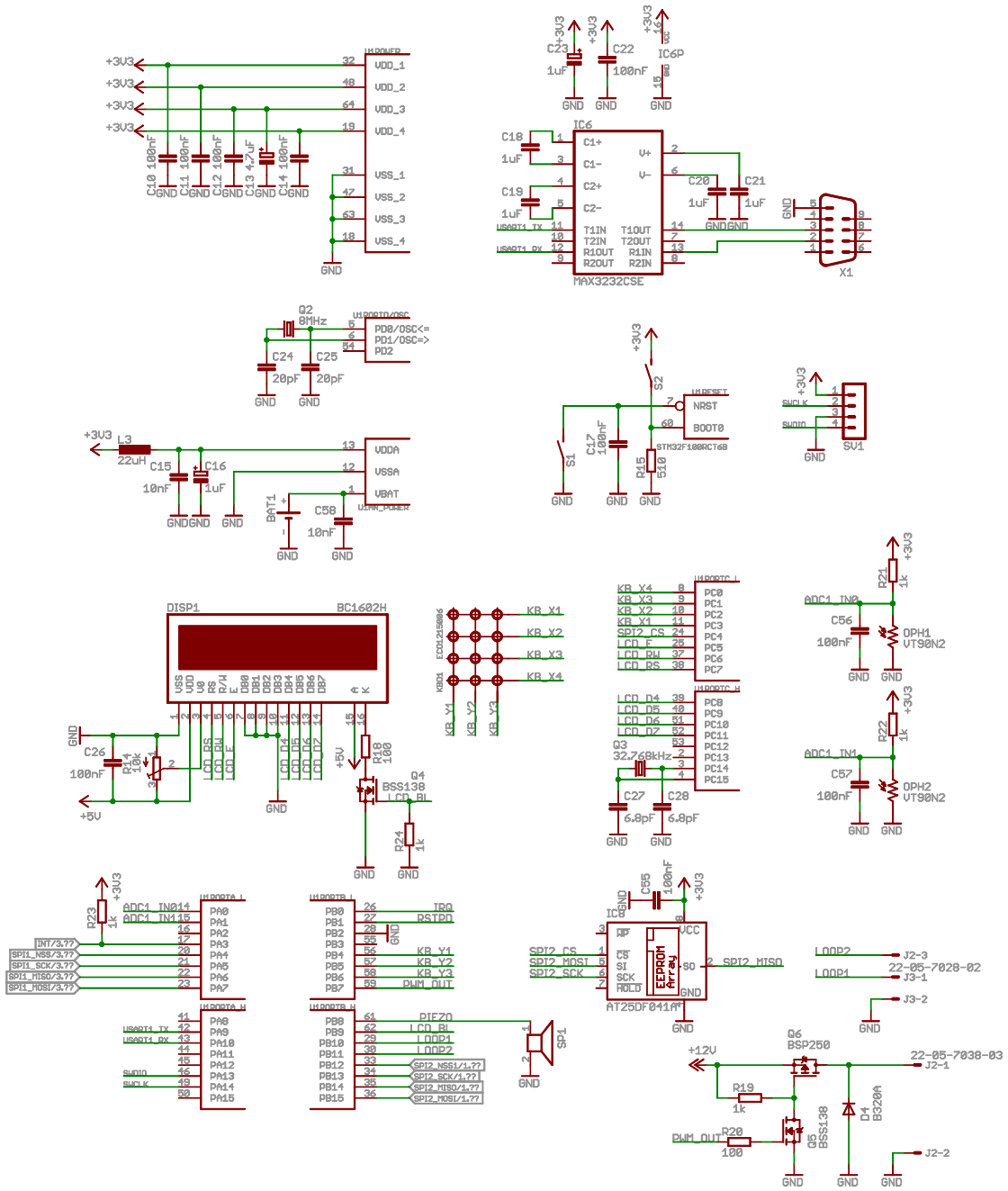
Priebeh signálu na vstupe DEMOD_IN

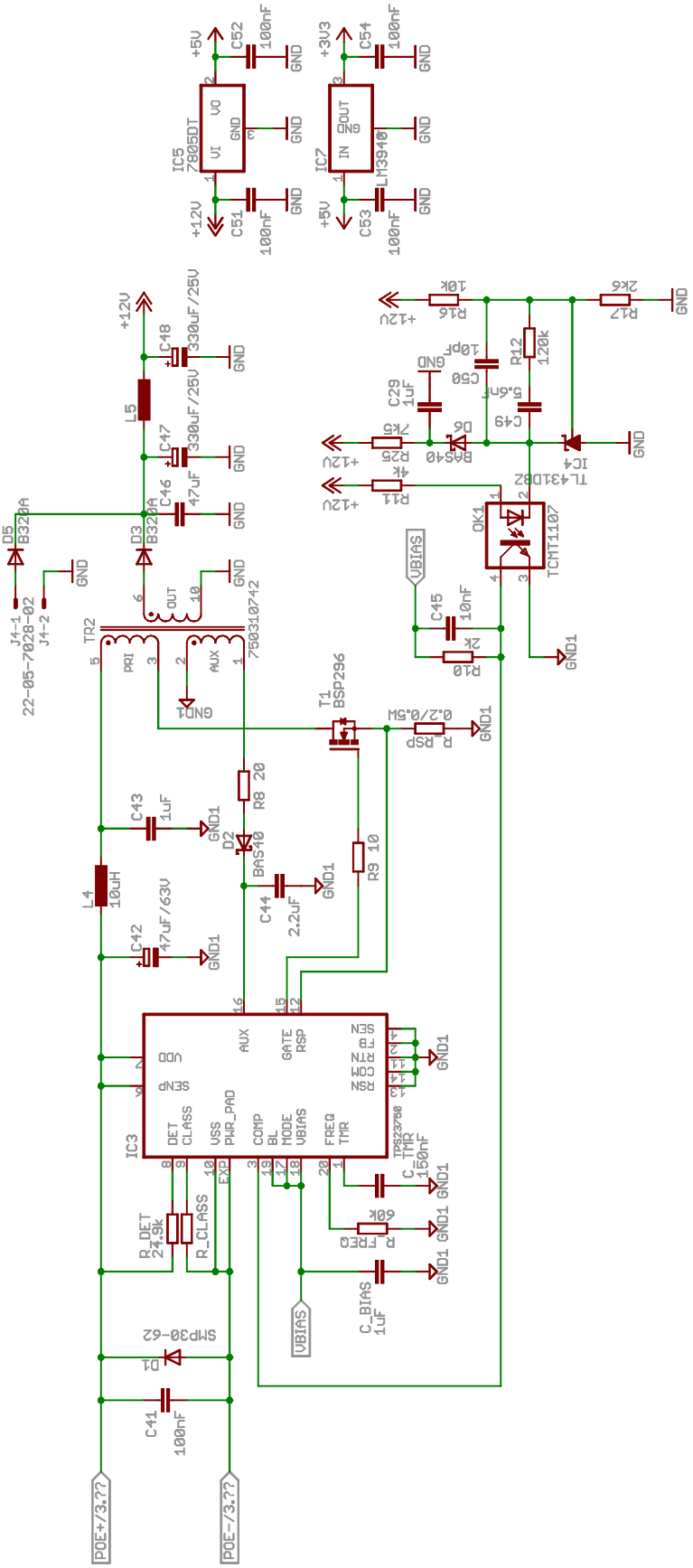
F Fotografie čítačky k PC



G Schéma zapojenia terminálu

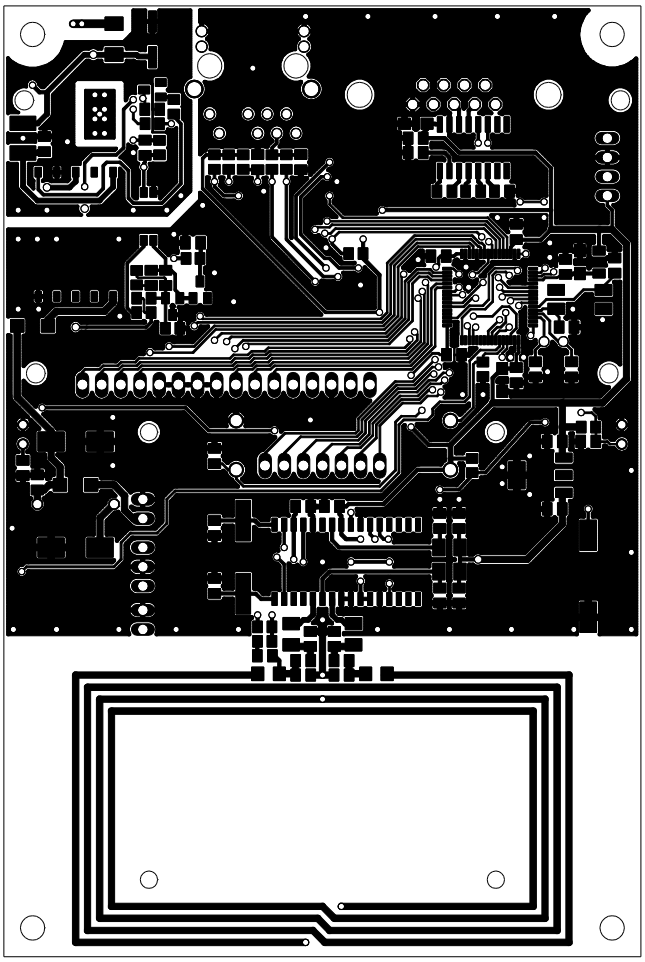


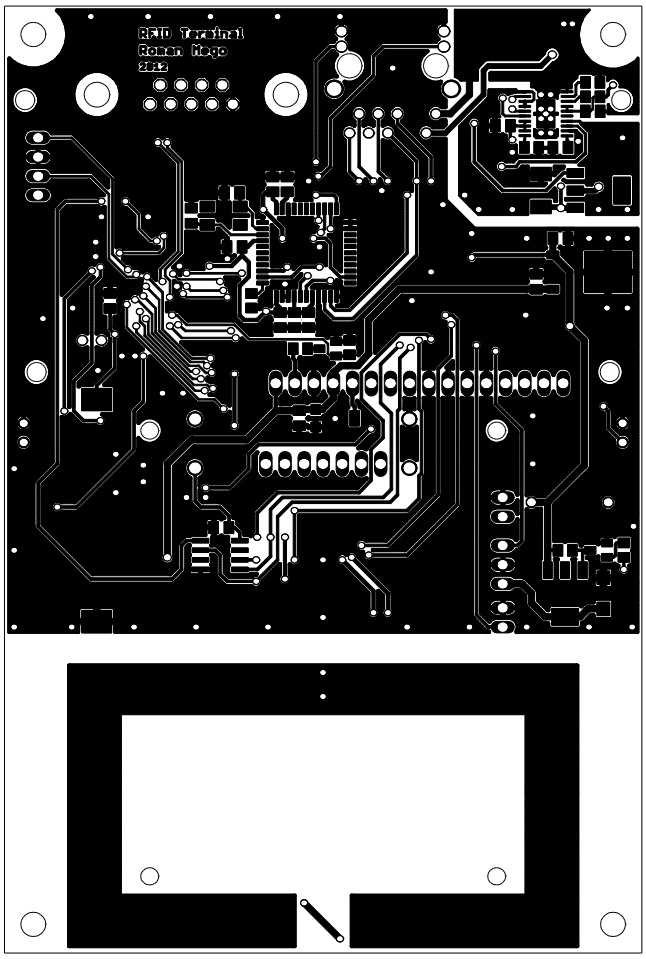

+3V3
VDD_1
VDD_2
VDD_3
VDD_4
VSS_1
VSS_2
VSS_3
VSS_4
GND
C10 100nF
C11 100nF
C12 100nF
C13 4.7uF
C14 100nF
C23 1uF
C22 100nF
IC6P
IC6
C18 1uF
C19 1uF
C20 1uF
C21 1uF
MAX3232CSE
X1
Q2 8MHz
C24 20pF
C25 20pF
PD0/OSC=
PD1/OSC=>
PD2
L3 22uH
C15 10nF
C16 1uF
VDDA
VSSA
VBAT
BAT1
C58 10nF
S2
S1
NRST
BOOT0
STM32F100RCT6B
C17 100nF
R15 510
SV1
DISP1
BC1602H
VSS VDD V0 RS R/W E DB0 DB1 DB2 DB3 DB4 DB5 DB6 DB7 A K
C26 100nF
R14 10k
R18 100
Q4 BSS138
LCD_BL
R24 1k
KB_X1
KB_X2
KB_X3
KB_X4
KB_Y1
KB_Y2
KB_Y3
LCD_D4
LCD_D5
LCD_D6
LCD_D7
LCD_RW
LCD_RS
LCD_E
Q3 32.768kHz
C27 6.8pF
C28 6.8pF
R21 1k
R22 1k
ADC1_IN0
ADC1_IN1
C56 100nF
C57 100nF
OPH1 VT90N2
OPH2 VT90N2
R23 1k
ADC1_IN14
ADC1_IN15
INT/3.??
SPI1_NSS/3.??
SPI1_SCK/3.??
SPI1_MISO/3.??
SPI1_MOSI/3.??
USART1_TX
USART1_RX
SWDIO
SWCLK
IRQ
RSTPD
PWM_OUT
DIF20
LCD_BL
LOOP1
LOOP2
SPI2_NSS/1.??
SPI2_SCK/1.??
SPI2_MISO/1.??
SPI2_MOSI/1.??
SP1
C55 100nF
IC5
AT25DF041A*
SPI2_CS
SPI2_MOSI
SPI2_SCK
SPI2_MISO
J2-3
J3-1
J3-2
22-05-7028-02
Q6 BSP250
R19 1k
R20 100
Q5 BSS138
D4 B320A
+12V
22-05-7038-03
J2-1
J2-2


IC5
7805DT
VI
VO
GND
+12V
+5V
C51
100nF
C52
100nF
IC7
LM3940
IN
OUT
+5V
+3V3
C53
100nF
C54
100nF
GND
L5
C46
47uF
C47
330uF/25V
C48
330uF/25V
D5
B320A
D3
B320A
J4-1
J4-2
22-05-7028-02
TR2
750310742
PRI
AUX
OUT
GND1
T1
BSP296
R_RSP
0.2/0.5W
R8
20
D2
BAS40
C43
1uF
C44
2.2uF
R9
10
L4
10uH
C42
47uF/63V
IC3
TPS23750
DET
CLASS
VSS
PWR_PAD
COMP
BL
MODE
VBIAS
FREQ
TMR
VDD
SENP
AUX
GATE
RSP
SEN
FB
RTN
COM
RSN
EXP
R_DET
24.9k
R_CLASS
C_TMR
150nF
R_FREQ
60k
C_BIAS
1uF
VBIAS
D1
SMP30-62
C41
100nF
POE+/3.??
POE-/3.??
R11
4k
R25
7k5
D6
BAS40
C29
1uF
C50
10pF
C49
5.6nF
R12
120k
R16
10k
R17
2k6
IC4
TL431DBZ
OK1
TCMT1107
C45
10nF
R10
2k
GND1

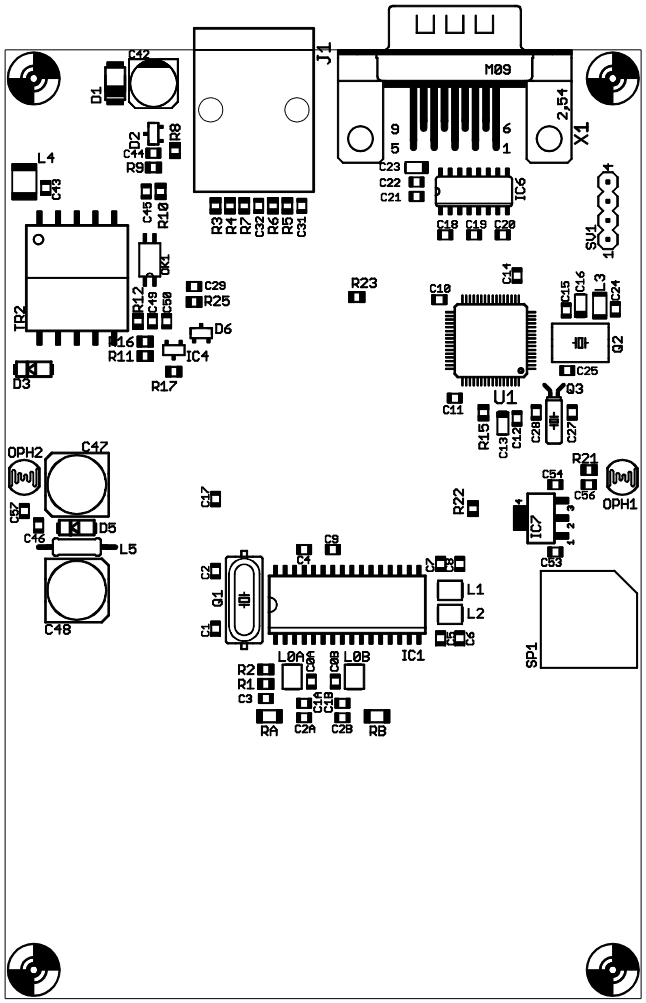
H Motív plošného spoja terminálu

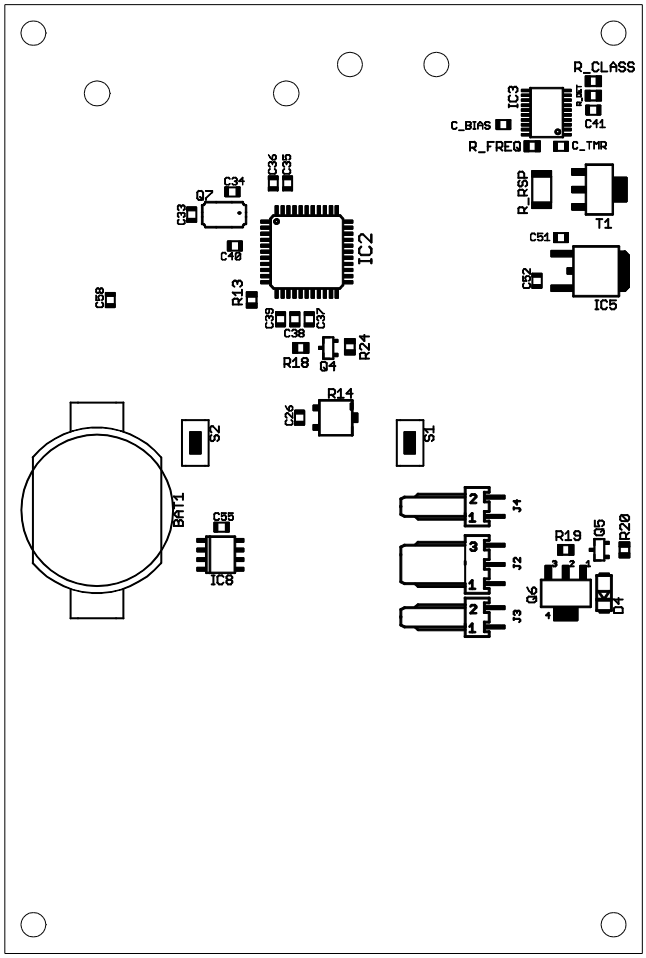
Rozmer: 84,4 mm x 125,4 mm




RFID Terminal
Roman Hugo
2012

I Osadenie súčiastok terminálu



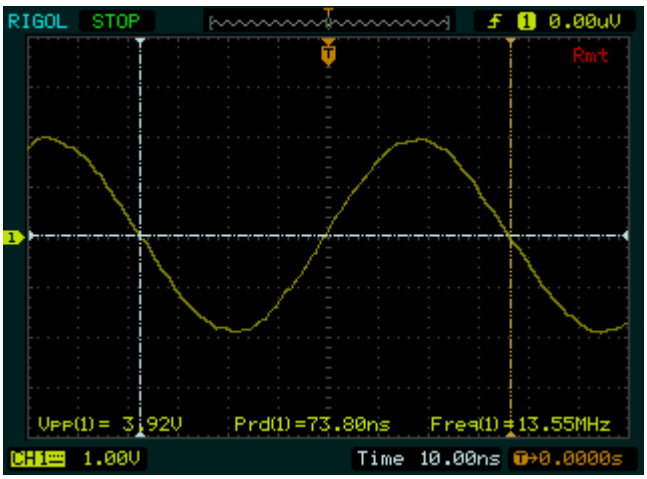

R_CLASS
IC3
C_BIAS
R_FREQ
C_TMR
C41
R_RSP
T1
C51
C52
IC5
C34
C35
C33
Q7
C31
C40
IC2
R13
C58
C39
C37
C38
R18
Q4
R24
R14
C26
S2
S1
BAT1
C55
IC8
J4
J2
J3
R19
Q5
R20
Q6
D4

J Zoznam súčiastok terminálu

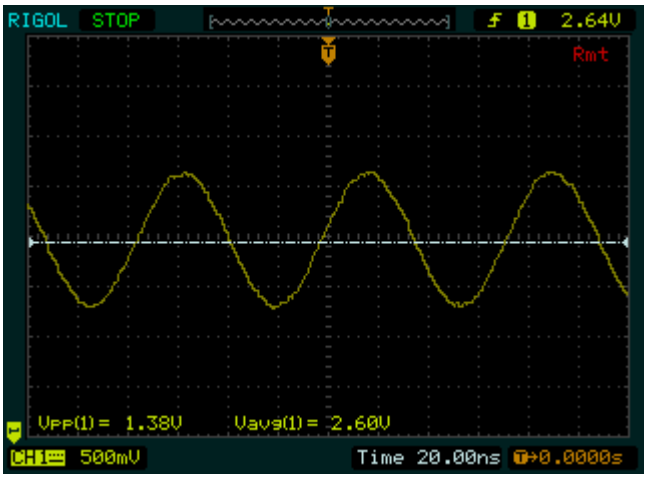
Označenie	Hodnota	Puzdro
BAT1	CR2032	SMTU2032-LF
C0A, C0B	150pF	0805
C1, C1A, C1B, C2	15pF	0805
C2A, C2B	68pF	0805
C3, C37, C38, C39, C40	1nF	0805
C4, C5, C7, C9, C10, C11, C12, C14, C17, C22, C26, C36, C41, C51, C52, C53, C54, C55, C56, C57	100nF	0805
C6, C8	100pF	0805
C13	4.7uF	SMC_A
C15, C31, C32, C45, C58	10nF	0805
C16, C23	1uF	SMC_A
C18, C19, C20, C21, C29, C43, C_BIAS	1uF	0805
C24, C25	20pF	0805
C27, C28	6.8pF	0805
C33, C36	27pF	0805
C35	10uF	0805
C42	47uF/63V	6,3x7,7
C44	2.2uF	0805
C46	47uF	0805
C47, C48	330uF/25V	153CLV-0810
C49	5.6nF	0805
C50	10pF	0805
C_TMR	150nF	0805
D1	SMP30-62	DO-214AC
D2, D6	BAS40	SOT23
D3, D4, D5	B320A	DO214AC
DISP1	BC1602H	BC1602H
IC1	MFRC530	SOT287-1
IC2	ENC424J600	TQFP44
IC3	TPS23750	HTSSOP20
IC4	TL431DBZ	SOT23
IC5	7805DT	TO252
IC6	MAX3232CSE	SO16
IC7	LM3940	SOT223
IC8	AT25DF041A	SO-08
J1	TEC-108-2100	
KBD1	ECO1215006	
L0A, L0B	1uH	L3230M
L1, L2, L3	22nH	L3230M
L4	10uH	L1812

L5	10uH	
OK1	TCMT1107	SOP4
OPH1, OPH2	VT90N2	VT900
Q1	13.56MHz	HC49UP
Q2	8MHz	12SMX(B)
Q3	32.768kHz	TC26H
Q4, Q5	BSS138	SOT23
Q6	BSP250	SOT223
Q7	25MHz	CTS406
R1	680	0805
R2	820	0805
R3, R4, R5, R6	49.9	0805
R7, R9	10	0805
R8	20	0805
R10	2k	0805
R11	4k	0805
R12	120k	0805
R13	12.4k 1%	0805
R14	10k	SM-42/43B
R15	510	0805
R16	10k	0805
R17	2k6	0805
R18, R20	100	0805
R19, R21, R22, R23, R24	1k	0805
R25	7k5	0805
RA, RB	6.8	1206
R_CLASS	357 1%	0805
R_DET	24.9k	0805
R_FREQ	60k	0805
R_RSP	0.2/0.5W	2010
S1, S2	DTS31N	DTS31N
SP1	ABT-427-RC	
T1	BSP296	SOT223
TR2	750310742	
U1	STM32F100RCT6B	
X1	M09H	

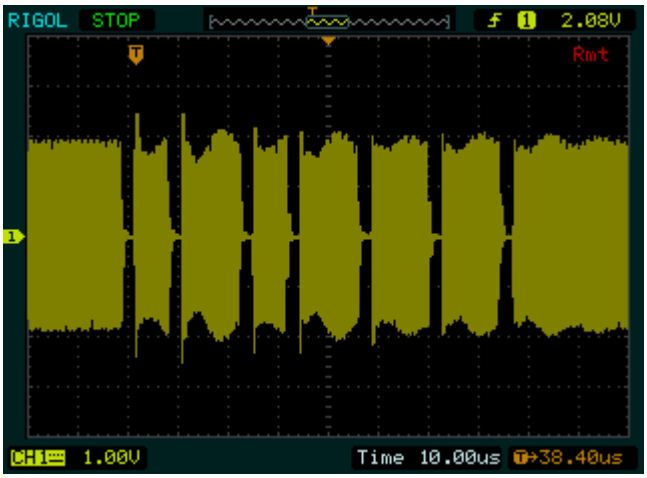
K Namerané priebehy na terminály



Priebeh signálu medzi C1A a RA

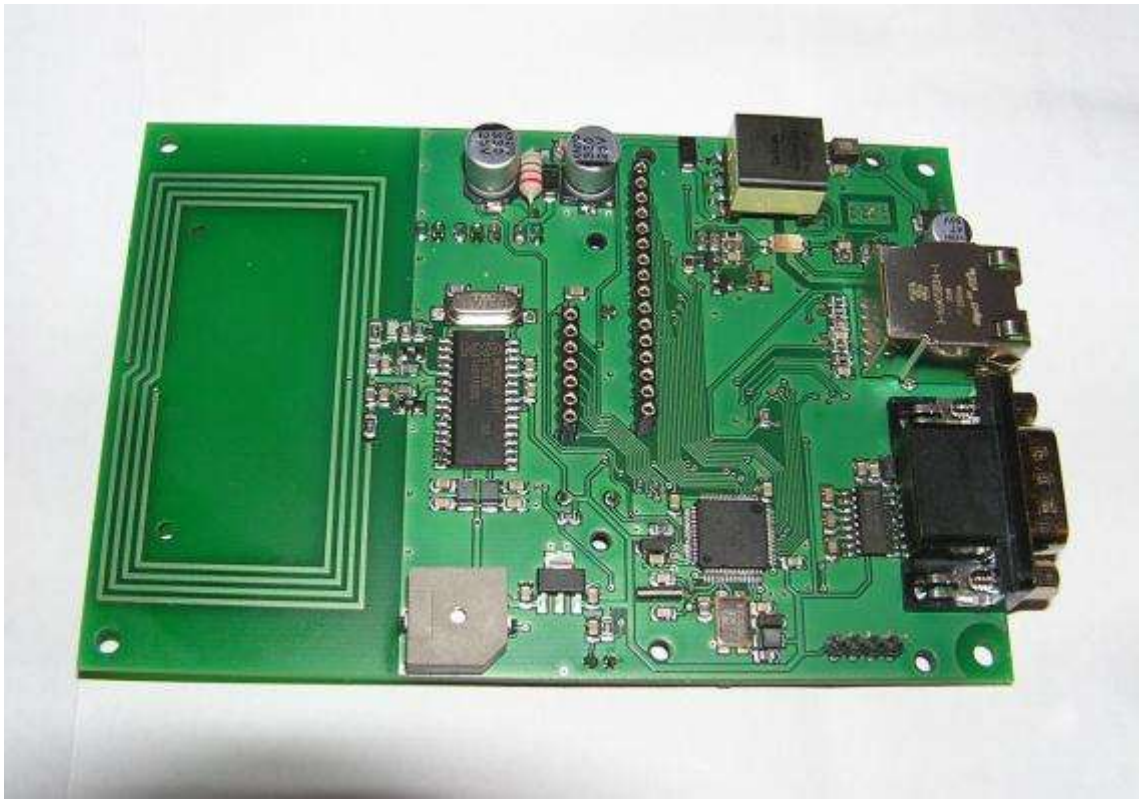


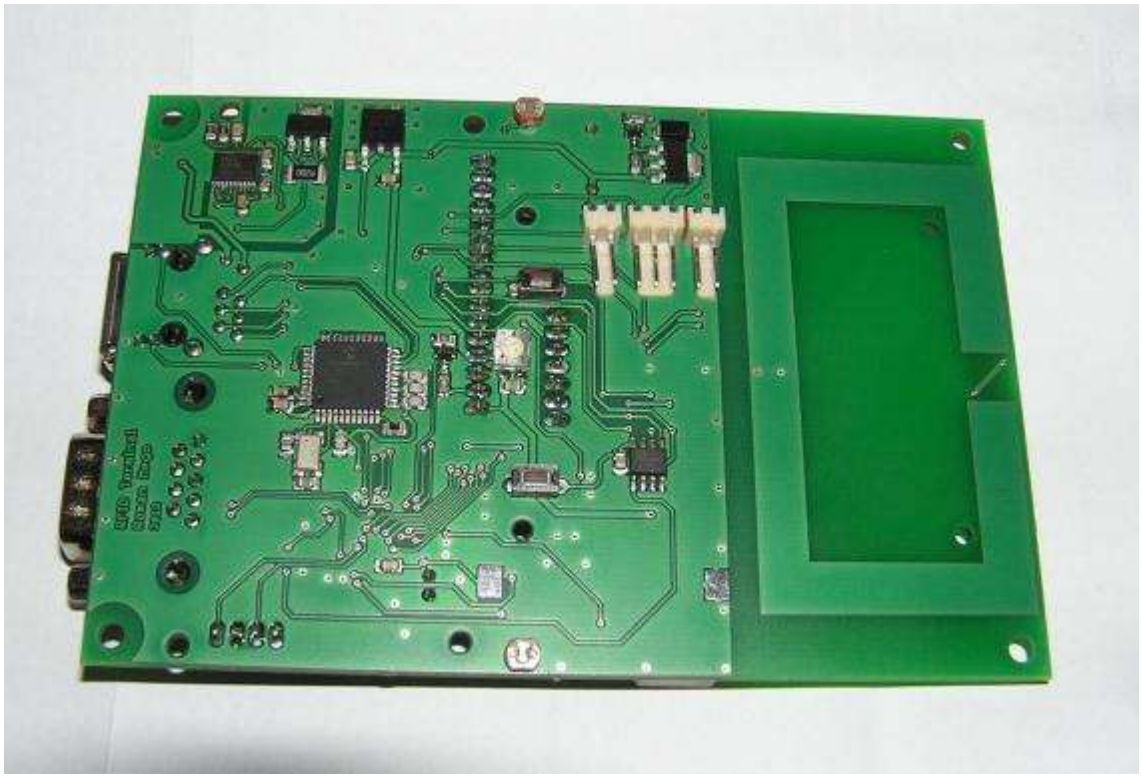
Priebeh signálu na vstupe RX

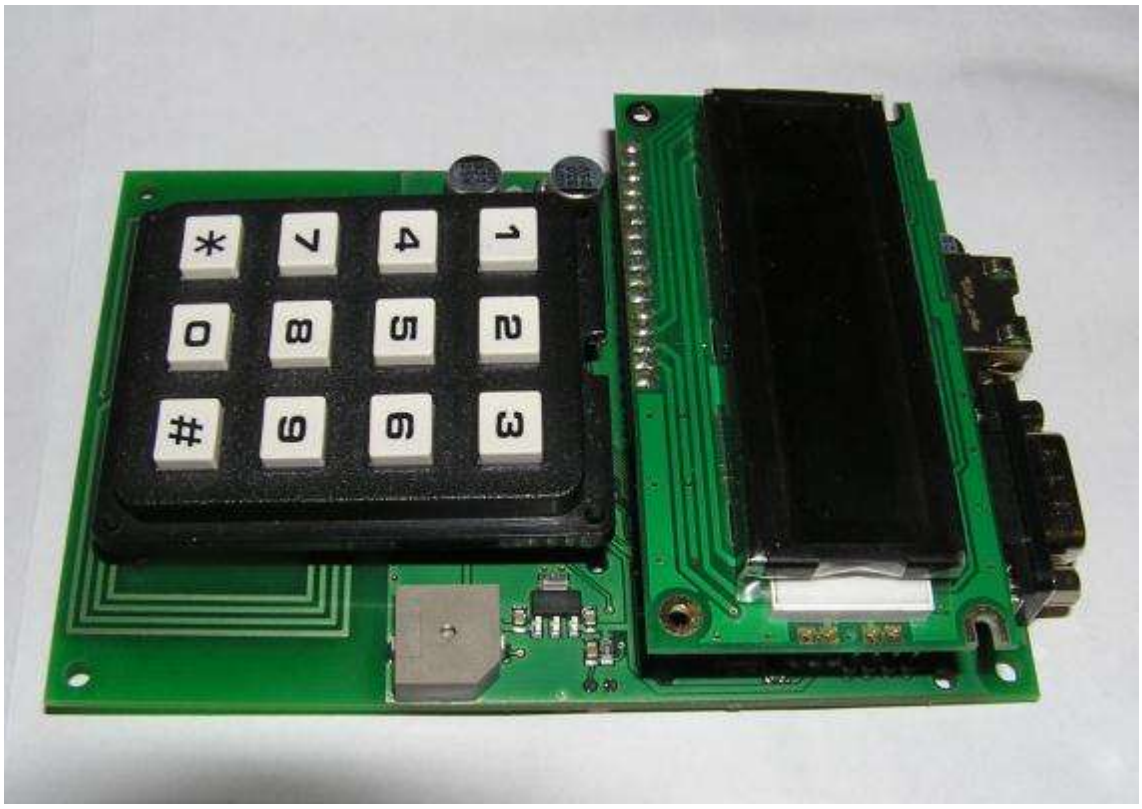


Komunikácia s tagom

L Fotografie terminálu






*
7
4
1
0
8
5
2
#
9
6
3