



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV AUTOMATIZACE A INFORMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF AUTOMATION AND COMPUTER SCIENCE

REALIZACE PŘÍSTUPOVÉHO SYSTÉMU PRO INTELIGENTNÍ BUDOVY NA BÁZI RFID

RFID ACCES SYSTEM REALIZATION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

PAVEL MIKŠÍČEK

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. TOMÁŠ MARADA, Ph.D.

BRNO 2012

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav automatizace a informatiky

Akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

student(ka): Pavel Mikšíček

který/která studuje v **bakalářském studijním programu**

obor: **Aplikovaná informatika a řízení (3902R001)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Realizace přístupového systému pro inteligentní budovy na bázi RFID

v anglickém jazyce:

RFID acces system realization

Stručná charakteristika problematiky úkolu:

Cílem práce je návrh a realizace přístupového systému pro otevírání dvěří v inteligentních budovách na bázi RFID čtečky. Jednotka bude řízena mikrokontrolérem ATMEGA. Při řízení přístupu např. do laboratoře je nutností vyřešit správu stávajících a zadávání nových ID do přístupového systému.

Cíle bakalářské práce:

1. Seznamte se s RFID problematikou.
2. Navrhněte přístupový systém na bázi RFID.
3. Navržený přístupový systém realizujte.
4. Demonstrujte funkčnost realizovaného řešení.

Seznam odborné literatury:

[1] <http://www.robotika.cz>

[2] <http://www.robotika.sk>

[3]

<http://www.hw.cz/Produkty/Obecne-produkty/ART878-Ctecka-karet-pro-bezkontaktni-identifikaci-ID-12-Picomax.html>

Vedoucí bakalářské práce: Ing. Tomáš Marada, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2011/2012.

V Brně, dne 20.11.2011

L.S.

Ing. Jan Roupec, Ph.D.
Ředitel ústavu

prof. RNDr. Miroslav Doupovec, CSc., dr. h. c.
Děkan fakulty

ABSTRAKT

Tato bakalářská práce se zabývá možnostmi využití RFID technologie v inteligentních budovách. V první části popisuje hlavní části technologie, princip funkce a uvádí příklady využití v různých oblastech. Druhá část se zabývá návrhem RFID technologie na pracovní frekvenci 125 kHz pro výrobu prototypu funkčního zařízení, návrhem vhodného hardwaru pro realizaci a otázkou bezpečnosti. Podrobně popisuje funkce, kterými zařízení disponuje. V poslední části práce popisuje postup při realizaci, od kresby schémat, přes návrh a výrobu plošných spojů, až po testování vyrobeného zařízení. Získané poznatky při tvorbě této bakalářské práce jsou shrnuty v závěru.

ABSTRACT

This bachelor thesis deals with possibilities of using RFID technology in intelligent buildings. The first part of thesis describes main parts of the technology, principle functions and gives examples of applications in various fields. The second part deals with selection suitable RFID technology on frequency 125 kHz for manufacture the functional prototype of the device, design hardware for realization and discusses security. There is a detailed description of device functions. In the last part thesis describes the implementation process from drawing schematics to design and manufacture of printed circuit boards and testing prototype. The knowledge gained in the creation of this work are summarized in the conclusion.

KLÍČOVÁ SLOVA

RFID, přístupový systém, identifikace, transpondér, mikrokontrolér, AVR, Atmel, ATmega.

KEYWORDS

RFID, access system, identification, transponder, microcontroller, AVR, Atmel, ATmega.

PROHLÁŠENÍ O ORIGINALITĚ

Prohlašuji, že jsem tuto bakalářskou práci na téma „Realizace přístupového systému pro inteligentní budovy na bázi RFID“ vypracoval samostatně a veškerá použitá literatura a prameny jsou uvedeny v seznamu použitých zdrojů.

V Brně dne 25.5.2012

podpis.....

BIBLIOGRAFICKÁ CITACE

MIKŠÍČEK, P. *Realizace přístupového systému pro inteligentní budovy na bázi RFID*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2012. 47 s.
Vedoucí bakalářské práce Ing. Tomáš Marada, Ph.D..

PODĚKOVÁNÍ

Děkuji svému vedoucímu Ing. Tomáši Maradovi Ph.D. za cenné rady a pomoc při tvorbě této bakalářské práce.

OBSAH

Abstrakt	5
Klíčová slova	5
Prohlášení o originalitě	7
Bibliografická citace	7
Poděkování.....	9
1 Úvod.....	13
2 Problematika identifikace objektů.....	15
2.1 Úvod k technologii RFID	15
2.2 Komunikace mezi čtečkou a transpondérem	15
2.3 Pracovní frekvence	16
2.4 Transpondéry	18
2.4.1 Aktivní.....	18
2.4.2 Pasivní	18
2.4.3 Semi-aktivní	18
3 Návrh přístupového systému.....	19
3.1 Základní informace a požadavky	19
3.2 Pracovní frekvence	19
3.3 Zabezpečení proti útokům	20
3.4 Funkce	20
3.4.1 Správa uživatelů	20
3.4.2 Reálný čas	21
3.4.3 Logování přístupů	22
3.4.4 Přenos logovacího souboru na microSD kartu	22
3.5 Mikrokontrolér.....	23
3.6 Převodník USB – UART	24
3.7 Sériová EEPROM paměť.....	25
4 Realizace.....	27
4.1 Schéma.....	27
4.1.1 Mikrokontrolér	27
4.1.2 Napájení	27
4.1.3 Spínání kontaktu relé.....	29
4.1.4 Čtečka microSD karet	30
4.1.5 ISP programovací konektor.....	31
4.2 Výběr pouzdra	32
4.3 Návrh DPS	33
4.4 Výroba a osazení DPS	34
4.4.1 Metody přenesení obrazce na DPS.....	34
4.4.2 Osvit a vyvolání	36
4.4.3 Leptání.....	36
4.4.4 Dokončovací výroba a osazení.....	37
4.5 Programování firmwaru.....	38
4.6 Funkčnost hotového zařízení	42
4.7 Návrhy na zlepšení	42
5 Závěr.....	43
Seznam použité literatury.....	45
Seznam příloh.....	47

1 ÚVOD

V dnešní době se moderní technologie čím dál rychleji rozvíjí do všech odvětví a stává se naším každodenním společníkem téměř na každém kroku. Lidé si chtějí zjednodušovat život novými, lepšími a modernějšími věcmi. V některých případech se tyto věci stávají jejich osobní vizitkou. Jako zástupce této kategorie lze jmenovat například drahé automobily, mobilní telefony nebo notebooky. Druhou skupinu tvoří věci, které lidem skutečně výrazně usnadňují, zrychlují a zefektivňují práci, a tím mnohdy šetří značnou část jejich nákladů. Pro příklad to mohou být myčky nádobí a robotické vysavače v domácnostech nebo číslíkové ovládané stroje a roboti v komerční sféře. A nakonec třetí, pravděpodobně nejširší skupinu využívající nejmodernější technologie, představují věci zajišťující bezpečnost, administraci, kontrolu a měření. Zástupcem mohou být zařízení monitorující a identifikující osoby a objekty nebo přístroje ve zdravotnictví.

Tato bakalářská práce se zabývá poslední jmenovanou skupinou, a to konkrétně identifikací osob v moderních automatizovaných tzv. inteligentních budovách. Technologie RFID, která identifikaci zajišťuje, je známá již řadu let. Je bezkontaktní a plně elektronická, což zvyšuje bezpečnost a zrychluje přístupy.

Cílem práce bylo seznámit se s aktuálně používanými technologiemi RFID ve všech odvětvích a na základě těchto poznatků navrhnout vlastní přístupový systém, který bude splňovat požadavky zadání. Celé zařízení bude realizováno, odzkoušeno a případně využito pro potřeby Ústavu automatizace a informatiky Fakulty strojního inženýrství VUT v Brně. Součástí této práce je podrobný popis funkcí a ovládání zařízení.

2 PROBLEMATIKA IDENTIFIKACE OBJEKTŮ

2.1 Úvod k technologii RFID

RFID (Radio Frequency Identification) je zkratka pro radiofrekvenční identifikační systém, který pracuje na principu radiofrekvenčních vln. Umožňuje rychlejší, spolehlivější a jednodušší identifikaci a sledování objektů oproti dnes používaným čárovým kódům. Nabízí možnost nahrávat, ukládat a předávat základní údaje o výrobku, objektu nebo osobě. To vede ke zlepšení skladových, logistických a výrobních procesů, sledování pohybu objektů a jednodušší identifikaci osob.[1]

Informace jsou přenášeny prostřednictvím čipů (transpondérů, tagů), na které lze zapisovat, opakovaně přepisovat a číst z nich. Samotné čtení informací z transpondérů může probíhat hromadně. Současná zařízení dokáží přečíst až několik set transpondérů za minutu.

Technologie RFID je v současné době považována za nástupce čárových kódů, nicméně je pravděpodobně nenahradí úplně. Je však možné výhodně spojit fungování čárového kódu s RFID, například integrováním transpondéru do samolepky, na kterou se následně natiskne čárový kód.

S myšlenkou hromadné bezkontaktní identifikace objektů bez nutnosti přímé viditelnosti přišla maloobchodní firma WalMart, která kdysi stála i u zrodu čárových kódů. V dnešní době se tato technologie rychle rozvíjí do nejrůznějších oborů.[2]

V obchodním odvětví přináší několik výhod. Dnes se velmi často využívá pro ochranu hodnotnějšího zboží v obchodě. Pokud dojde ke krádeži, transpondér na zboží aktivuje bezpečnostní rám u východu z obchodu. RFID technologie však nabízí mnohem více. Oproti čárovým kódům lze rozlišit nejen druh zboží a výrobce, ale i konkrétně identifikovat každý kus. Lze zjistit informace o místě výroby, datu výroby a spotřebě, způsobu přepravy a další informace. Díky možnosti načtení několika transpondérů najednou lze také při placení u pokladny načíst téměř najednou jednotlivé výrobky bez nutnosti jejich vykládání z nákupního vozíku. Tím se snižuje inventurní difference na minimum.[3]

V logistickém odvětví se staly čárové kódy osvědčeným standardem a fungují spolehlivě již dlouhou řadu let. Nicméně i zde má RFID potenciál především v množství informací, které lze do transpondéru uložit, a čtecí vzdálenosti několika metrů. Dalším zajímavým přínosem může být sledování objektu v reálném čase pomocí aktivních transpondérů, které dokáží bezdrátově posílat informaci o své poloze. Aktivní transpondéry jsou schopny zaznamenávat během výroby nebo manipulace okolní teplotu, atmosférický tlak, vlhkost, otřesy a další fyzikální veličiny. Při spojení senzoru pádu a sledování osob v reálném čase lze využít tuto technologii pro pacienty v léčebnách dlouhodobě nemocných, kde může zachraňovat životy.[3], [4]

Tato technologie je stále více využívána při identifikaci osob. Za předpokladu, že oprávněná osoba bude mít svůj transpondér pro vlastní použití a bude si ho hlídat před odcizením, lze díky jedinečnosti každého transpondéru jednoznačně určit její totožnost. Pomocí jednoho jediného transpondéru lze na různých místech například rozpoznat majitele vozidla, využívat elektronickou jízdenku, bankovní účet nebo elektronickou peněženku, umožnit oprávněné osobě vstoupit do budovy. Může nahradit osobní doklady jako řidičský nebo občanský průkaz. Nachází uplatnění při identifikaci automobilů při placení elektronického mýtného, identifikaci zvířat a mnoha dalších místech.[2]

2.2 Komunikace mezi čtečkou a transpondérem

Hlavní části identifikačního systému jsou čtečka, transpondér (tag) a podpůrné systémy (řídící počítače, databáze, telekomunikační sítě).

Čtečka se skládá z vysokofrekvenčního modulu (vysílač a přijímač), řídící jednotky a antény. Dále může obsahovat prvky pro komunikaci s nadřazenými podpůrnými systémy (např. RS 232, RS 485, ...).

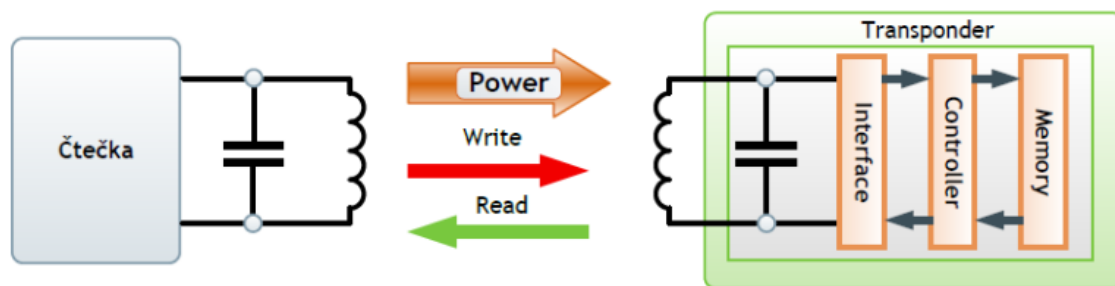
Každý transpondér se skládá z antény a mikročipu. Pokud transpondér neobsahuje vlastní zdroj napájení (baterii), musí být vybaven obvodem pro získávání energie z elektromagnetického

pole a jedná se o pasivní transpondér. Jestliže transpondér má vlastní zdroj napájení, jedná se o transpondér aktivní. [5]

Technologie RFID pracuje na principu radaru. Čtečka nepřetržitě, nebo v pravidelných intervalech, vysílá na svém nosném kmitočtu elektromagnetické vlnění. Pokud se v dosahu tohoto vlnění vyskytne transpondér, začne se pomocí elektromagnetické indukce nabíjet jeho kondenzátor. Ve chvíli, kdy množství energie postačuje k napájení logických a rádiových obvodů transpondéru, vyšle se odpověď čtečce. Ta je většinou realizována dvoustavovou ASK modulací (Amplitude Shifting Key) pomocí změny zakončovací impedance antény transpondéru. Odrazy, které tím vzniknou, jsou detekovány a vyhodnoceny čtečkou jako logické úrovně 0 a 1. [6]

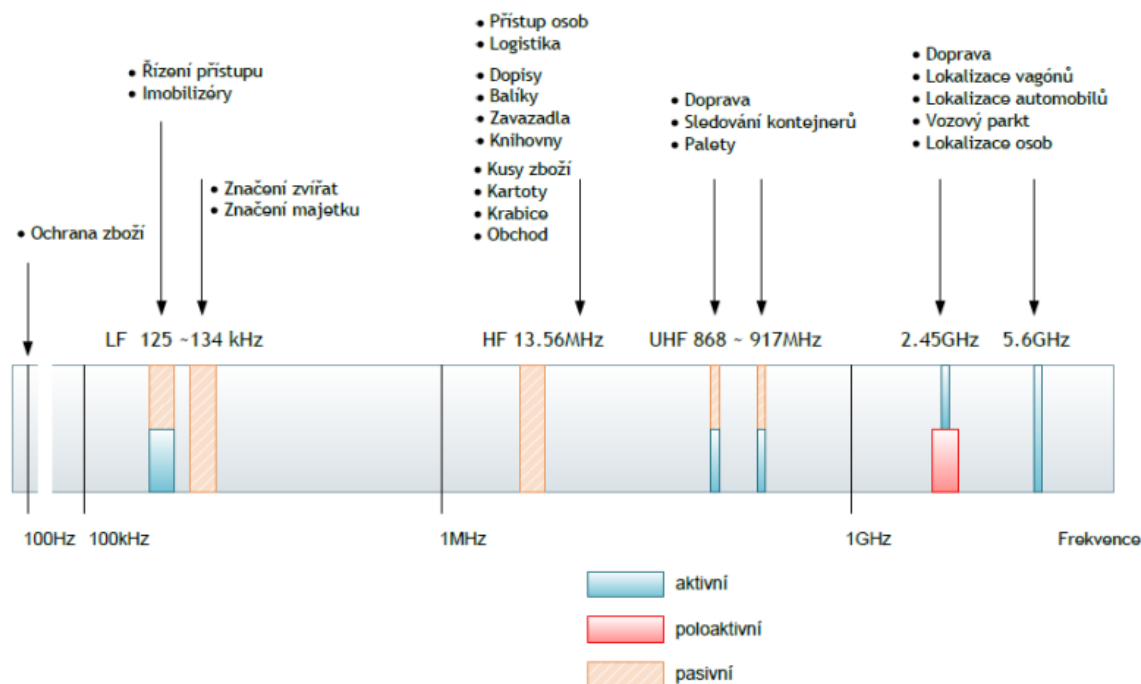
Řízení komunikace je definováno příslušnými normami:

- ČSN ISO/IEC 10536 - Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s těsnou vazbou,
- ČSN ISO/IEC 14443 - Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s vazbou na blízko,
- ČSN ISO/IEC 15693 - Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s vazbou na dálku.



Obrázek 1: Schéma komunikace RFID.[6]

2.3 Pracovní frekvence



Obrázek 2: Frekvence používané různými aplikacemi RFID. [6]

- Nízká frekvence (LF) 125 – 134 kHz

V tomto rozsahu se používají dvě frekvence. 125 kHz a pro identifikaci zvířat 134,2 kHz. Tyto 2 frekvence jsou celosvětově uznávané. Je to nejstarší technologie používaná od konce 80. let. Umožňuje snadnou a levnou výrobu čtečky. Má malou čtecí vzdálenost, která je určena velikostí cívky v transpondéru a konstrukcí čtečky. Běžnou ISO kartou lze dosáhnout čtecí vzdálenosti až 15 cm. Pomalá přenosová rychlost. Využívá pasivní i aktivní transpondéry. Pracuje dobře v prostředí s kovy, kapalinami a ve znečištěném prostředí. [7]

- Vysoká frekvence (HF) 3 MHz – 30 MHz

Standardně se používá celosvětově uznávaná frekvence 13,56 MHz. Poskytuje vyšší úroveň zabezpečení a větší přenosovou rychlost. Nákladnější a na výrobu čtečky složitější než LF technologie. [7]

- Velmi vysoká frekvence (VHF) 30 MHz – 300 MHz

Na velmi vysoké frekvenci nepracuje žádná RFID technologie. [7]

- Ultra vysoká frekvence (UHF) 200 MHz – 1 GHz

V Evropě se používá frekvence 868 – 928 MHz, v USA a Kanadě 902 – 928 MHz. Ve velké míře se využívá pro sledování zboží, a to hlavně díky větší čtecí vzdálenosti a levnější sériové výrobě oproti LF a HF transpondérům. Hlavní nevýhodou je rušení v blízkosti kovů a kapalin. Může také rušit citlivé elektronické přístroje, například ve zdravotnictví. Používá aktivní i pasivní transpondéry. [7]

- Mikrovlnná frekvence (MW) více než 1 GHz

Poměrně nová, rychle se rozvíjející, technologie pracující na frekvenci 2,45 GHz nebo 5,8 GHz. Obvykle se používají aktivní a semi-aktivní transpondéry, ale může pracovat i s pasivními. Za použití aktivní technologie dosahuje velké čtecí vzdálenosti (až 30 metrů) a vysoké rychlosti přenosu dat ze všech uvedených technologií. Problémem této technologie může být konflikt s bezdrátovými 802.11b/g (WiFi) sítěmi. [7]

- Ultra-Wideband (UWB)

Nejnovější technologie, kterou RFID využívá. UWB místo vysílání radiofrekvenčního vlnění na určité jmenovité frekvenci, využívá velmi široký rozsah frekvencí s malým vyzařovacím výkonem. Sloučením širokého rozsahu frekvencí je dosaženo poměrně silného signálu. V praxi se používá frekvenční rozsahy od 3,1 do 10,6 GHz. Velkou výhodou této technologie je dosahování velkých čtecích vzdáleností, teoreticky až 200 m. Díky slabému vyzařovacímu výkonu tato technologie neruší citlivá zařízení. Lze také číst skrze kovy a kapaliny. Donedávna byla nevýhoda v absenci pasivních transpondérů. V roce 2009 však společnost Tagent tyto transpondéry vyvinula. Nicméně tato technologie je stále v začátcích, spíše ve vývoji. Tomu odpovídá i její vysoká cena. [7], [8]

Pracovní frekvence	Pasivní čtecí vzdálenost
Nízká frekvence - LF	10-20 cm
Vysoká frekvence - HF	10-20 cm
Ultra vysoká frekvence - UHF	3 m
Mikrovlnná frekvence - MW	3 m
Ultra-Wide – UWB	10 m

Tabulka 1: Dosahované čtecí vzdálenosti s pasivními transpondéry.[7]

2.4 Transpondéry

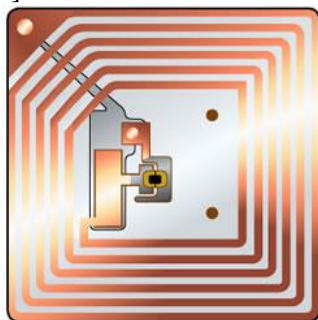
Někdy označované také jako tagy. Jsou to paměťové nosiče technologie RFID, na kterých jsou uloženy veškeré informace potřebné k daným účelům. Většinou se jedná o unikátní ID + rozšiřující paměť pro vlastní potřebu. Mohou být v provedení pouze ke čtení, ke čtení s možností jednorázového zápisu nebo ke čtení s možností přepisu. Tvarově se mohou velmi lišit, ale nejčastější použití je v samolepicích štítcích, ISO kartách a klíčenkách. [9]

2.4.1 Aktivní

Tyto transpondéry obsahují baterii, kterou používají pro komunikaci se čtečkou, ale zároveň mohou být vybaveny doplňujícími senzory a poskytovat tak informace o objektech, ke kterým jsou připevněny. Díky vlastnímu zdroji energie dosahují větších čtecích vzdáleností než transpondéry pasivní. Mohou pracovat v automatickém režimu a provádět měření nebo záznamy. Pokud se dostanou do čtecího pásma čtečky, informace předají. Využívají se spíše při lokalizaci. Nevýhodou oproti pasivní technologii je vysoká cena. [10]

2.4.2 Pasivní

Je to nejběžnější technologie. Pasivní transpondéry neobsahují žádný vlastní zdroj energie. Veškerou energii, kterou potřebují ke své činnosti, získávají elektromagnetickou indukci z pole vyzařovaného čtečkou. Dosahují malých čtecích vzdáleností. Jsou však velmi levné, a proto se dají použít i k jednorázovým účelům. [11]



Obrázek 3: Pasivní transpondér v samolepicím štítku. [12]

2.4.3 Semi-aktivní

Kombinuje výhody aktivních a pasivních transpondérů. Pracuje na stejném principu jako pasivní technologie. Narozdíl od ní však obsahuje baterii, díky které zlepšuje kvalitu vysílané odpovědi, a tím i čtecí dosah. Tohoto způsobu se využívá například u elektronického mýtného.

3 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU

3.1 Základní informace a požadavky

Při navrhování přístupového systému bylo třeba vyřešit několik problémů týkajících se samotné RFID technologie a instalace zařízení, které se odvíjely od prostředí, kde má být zařízení používáno. Zároveň bylo nutné zvolit cenově nejvýhodnější řešení.

Jedním z hlavních požadavků bylo, aby zařízení pracovalo bez nutnosti připojení k nadřazeným systémům, prostřednictvím kterých by získávalo informace o uživateli ze vzdálené databáze. V důsledku toho bylo voleno zařízení s interní pamětí o dostatečné velikosti, aby dokázalo uchovat informace o několika desítkách ID uživatelů. Zároveň bylo nutné tyto informace uchovat i při výpadku napájení. Jako nejvhodnější a nejjednodušší řešení se ukázalo využití interní EEPROM paměti mikrokontroléru ATmega. Disponuje velikostí 512 bajtů a možností 100 000 přepsání.[13] Nabízí možnost uložení až 127 transpondérů + 1 MASTER transpondér.

Dalším požadavkem byla snadná instalace zařízení. Proto byla konstrukce a rozměry zařízení navrhovány tak, aby se dalo umístit do běžných domovních elektroinstalačních krabic.

U zařízení nebyl kladen požadavek na funkčnost při výpadku elektrické energie. To především z toho důvodu, že bylo navrhováno jako alternativní možnost otevírání dveří uvnitř budov prostřednictvím spínání elektrického dveřního zámku. Tyto zámky nejsou obvykle elektricky zálohovány, a proto by funkčnost přístupového zařízení při výpadku neměla smysl.

3.2 Pracovní frekvence

Pro výběr vhodné pracovní frekvence muselo být přihlédnuto k několika aspektům, přičemž k nejdůležitějším patřila čtecí vzdálenost a cena.

K účelům identifikace osob se běžně používají pracovní frekvence 125 kHz nebo 13,56 MHz a pasivní transpondéry v podobě klíčenek nebo karet. Proto i při navrhování tohoto přístupového systému bylo vybíráno mezi těmito technologiemi.

Vzhledem ke skutečnosti, že zařízení mělo být umístěno v komplexu Vysoké školy VUT v Brně, kde v současné době funguje identifikace osob prostřednictvím ISIC, studentských a zaměstnaneckých karet na technologii HF (tj. 13,56 MHz), byly nejprve zkoumány možnosti využití této pracovní frekvence. Výhodou by bylo ušetření nákladů za transpondéry, které každý student i zaměstnanec VUT již vlastní. Další výhodou je zabezpečení radiové komunikace při komunikaci. Problémem ovšem byla čtecí vzdálenost. Ke spolehlivému čtení potřebuje RFID čtečka anténu naladěnou na 13,56 MHz. Kvůli minimalizování rozměrů antény se obvykle používají cívky vinuté na desce plošných spojů (DPS). Výroba této DPS musí být velmi přesná a kvalitní. Samotné ladění antény probíhá v několika krocích za pomoci generátoru pulzů, osciloskopu a měřiče impedance smyčky, nebo pomocí speciálních přístrojů a softwaru. Bohužel vybavení, které bylo pro vývoj k dispozici, nepostačovalo k výrobě a ladění takové antény. Jako další možnost se nabízelo zakoupit hotovou čtečku s již naladěnou anténou. Cena by však vysoce překročila hranici určenou pro tento projekt.

Následně byly zkoumány možnosti čtečky ID-12 od firmy ID Innovations na pracovní frekvenci LF (tj. 125 kHz) s udávaným dosahem 12 cm. Její výhodou byla příznivá cena za kompaktní čtečku s integrovanou anténou. Výstupem čtečky je přímo ID přiloženého transpondéru posílané v ASCII formátu přes RS 232 nebo pomocí dvou datových vodičů a protokolu Wiegand26. Tím odpadla výroba antény a celá realizace se tím značně zjednodušila. Čtečka podporuje formát karet EM 4001 a kompatibilní formáty.

S výběrem řešení na frekvenci 125 kHz však vyvstala nutnost zakoupit i transpondéry pracující na frekvenci 125 kHz. Náklady za 1 transpondér (Read Only) jsou v současné době na našem trhu 10-20 Kč ve formě ISO karty a 20-100 Kč ve formě klíčenky. [zdroj: SOS electronic] Cena závisí především na mechanické odolnosti a čtecí vzdálenosti transpondéru. Přesto jsou náklady za kompletní systém na této frekvenci při malém počtu transpondérů nižší než HF technologie.

Jednoduchost výroby zařízení a přívětivá cena byly hlavními důvody použití pracovní frekvence 125 kHz. Využita byla již zmíněná čtečka ID-12 od firmy ID Innovations podporující formát EM 4001 a formáty s ním kompatibilní.

3.3 Zabezpečení proti útokům

Zvolená RFID technologie LF využívá formát EM 4001, který se odvíjí od čipu integrovaného do transpondéru. Je to vlastně sériová paměť o velikosti 64 bitů s konstantním unikátním ID. Struktura této paměti je jednoznačně určena. Ve chvíli, kdy se čip dostane do pole čtečky, začne opakovaně vysílat binární řetězec, který je v něm uložený. Využívá se přitom kódování Manchester, avšak žádné šifrování. Transpondér odpoví jakékoli čtečce na jeho pracovní frekvenci. Toho využívají zařízení velikosti mobilního telefonu, které jsou schopny vybudit transpondér v okolí několika metrů a zaznamenat radiovou komunikaci. Poté stačí využít programovatelný čip Q5, zaznamenaný radiový signál do něj nahrát a naprogramovat výstupní kódér.[14], [15]

Lepší zabezpečení přináší frekvenční pásmo HF, které nabízí šifrování radiové komunikace. Na to spoléhá spousta aplikací typu elektronických peněženek a legitimací. Bohužel všechny tyto technologie již byly prolomeny. Nejpoužívanější z nich jsou:

- Mifare Classic – používá se ve dvou režimech. Režim unikátního ID, který není šifrovaný a funguje ekvivalentně jako LF transpondéry. Druhý používaný režim již využívá kryptografie Crypto1 a obousměrné autentizace čtečky a transpondéru. Byl však prolomen v letech 2007 – 2009. K samotnému prolomení hrubou silou jsou zapotřebí pouze 4 dotazy, ze kterých je na běžném PC během hodiny vypočítán tajný klíč. Dotaz může být proveden třemi způsoby. Interakcí útočníka se čtečkou, interakcí útočníka s čipem Mifare Classic nebo odposlechnutím komunikace během autorizovaného přístupu (možnost odposlechu až na desítky metrů daleko).
- Mifare DESFire – odstraňuje několik slabín Mifare Classic, ale několik nových zavádí.
- Mifare Plus – i tato technologie již byla prolomena, avšak forma útoku není zveřejněna, a proto je prozatím nejbezpečnější ze jmenovaných technologií.

Každá z těchto LF i HF technologií má několik známých bezpečnostních děr a je nutno s nimi počítat při nasazování do „ostrého“ provozu. Řada systémů pro zvýšení bezpečnosti kombinuje RFID technologii se zadáváním bezpečnostního PINu.[31]

3.4 Funkce

3.4.1 Správa uživatelů

Zařízení umožňuje snadnou správu uživatelů prostřednictvím MASTER transpondéru. Tím může být libovolný transpondér, který čtečka dokáže přečíst. Určit takový transpondér lze pouze pomocí sériové linky RS 232 přes piny Rx a Tx na desce plošných spojů nebo snadněji, pomocí vestavěného RS 232 <-> USB převodníku.

Nastavení MASTER transpondéru:

Označení MASTER transpondéru lze provést příkazem „mXXXXXX#“ poslaným v ASCII znacích prostřednictvím RS 232. Parametr „m“ označuje příkaz: „přiřadit MASTER transpondér“. 6 číslic reprezentovanými znaky „XXXXXX“ představuje samotné ID MASTER transpondéru v šestnáctkové soustavě. Jeho zjištění je popsáno níže. Poslední znak „#“ funguje jako potvrzení. Úspěšné uložení MASTER transpondéru do zařízení je signalizováno třemi krátkými tóny a blikáním zelené LED diody. Zároveň je přes RS 232 vypsána hláška: „MASTER transponder XXXXXX was successfully added.“

Zjistit ID transpondéru lze snadno, pomocí sériové linky RS 232. Při každém přiložení transpondéru vyšle zařízení načtené ID v desítkové soustavě přes sériovou linku RS 232 v ASCII znacích.

Přidávání nových transpondérů:

Pro přidávání nových uživatelů do přístupového systému se využívá MASTER transpondéru, který je nutno mít pro tuto funkci definován. Přidání nového transpondéru provedeme tak, že 3x krátce po sobě přiložíme MASTER transpondér a poté transpondér, který chceme do zařízení přidat. Pokud:

- je nový transpondér úspěšně uložen, zařízení tento stav signalizuje třemi krátkými tóny a blikáním zelené LED. Zároveň je přes RS 232 vypsána hláška: „New ID number XXXXXX was successfully added.“,
- přidávaný transpondér je již uložen z dřívějška, zařízení tento stav signalizuje jedním dlouhým tónem a svitem červené LED diody,
- je zaplněná paměť zařízení, tento stav je signalizován dvěma dlouhými tóny se současným rozsvícením červené LED diody.

Mazání transpondérů:

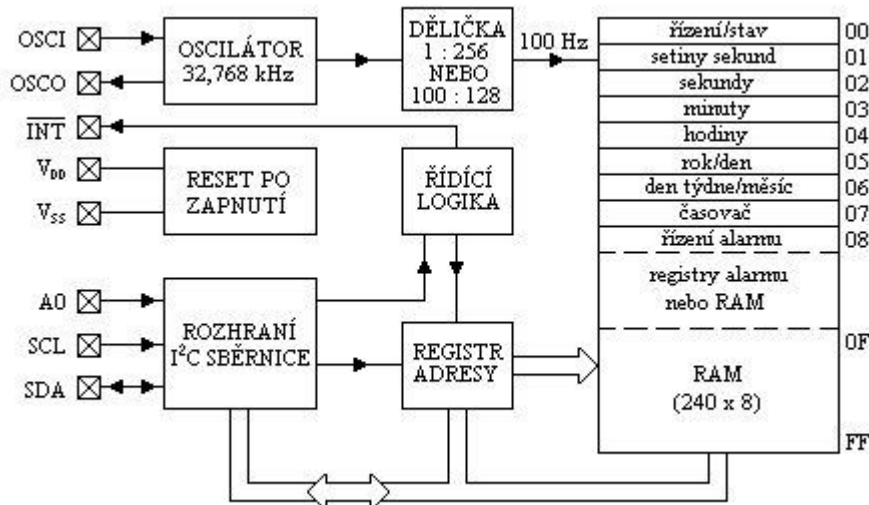
Pro mazání uživatelů z přístupového systému se využívá MASTER transpondéru, který je nutno mít pro tuto funkci definován. Transpondér smažeme tak, že k zařízení přiložíme MASTER transpondér po dobu alespoň 5 sekund a poté transpondér, který chceme smazat. Jediný transpondér, který nelze smazat je MASTER. Pokud:

- je transpondér úspěšně smazán, zařízení tento stav signalizuje třemi krátkými tóny a blikáním zelené LED. Zároveň je přes RS 232 vypsána hláška: „ID number XXXXXX was successfully removed.“,
- nebyl transpondér v zařízení uložen, není co mazat a zařízení tento stav signalizuje jedním dlouhým tónem a svitem červené LED diody.

Druhou možnost smazání nabízí RS232 a požití příkazu „rXXXXXX#“ poslaným v ASCII znacích. Parametr „r“ označuje příkaz: „smazat transpondér“. 6 číslic reprezentovaných znaky „XXXXXX“ představuje konkrétní ID transpondéru v šestnáctkové soustavě, který chceme smazat. Poslední znak „#“ funguje jako potvrzení. To je také jediná možnost jak smazat ID transpondéru z databáze pokud nedisponujeme transpondérem, který chceme smazat. Pokud je třeba smazat z databáze hromadně všechny transpondéry (mimo MASTERu), lze použít příkaz „r*#“.

3.4.2 Reálný čas

Zařízení disponuje obvodem reálného času pro možnost uchování časové informace o přístupech uživatelů. Pro tento účel byl zvolen integrovaný obvod PCF8583 s externím hodinovým krystalem o frekvenci 32 768 kHz. Obvod je vybaven 2048 bity statické CMOS RAM paměti uspořádanou jako 256 slov po 8 bitech. Prvních 8 bajtů se používá pro uchování hodin a data. Dalších 8 bajtů může být naprogramováno jako alarmy nebo libovolně využito jako volná RAM paměť. Komunikace obvodu s mikrokontrolérem probíhá pomocí sběrnice I2C.



Obrázek 4: Blokové schéma PCF8583.

V prvním bajtu na adrese 00 se nachází stavový registr. Prostřednictvím něho se nastavují všechny funkce a volby obvodu. Na adresách 01 až 06 je uložen čas a datum v BCD formátu. Registr na adrese 07 slouží jako čítač počítající od 0 do 99. Poté může vyvolat přerušení a resetuje se. Od adresy 08 po 0F jsou nastavení alarmů. [16]

Pro správnou funkci zařízení musí být tento obvod trvale napájen, a proto je jeho zdroj energie zálohován 3V knoflíkovou baterií typu BR1216, CR1216, BR1220, CL1220, CR1220 nebo BR1225.

Nastavení času:

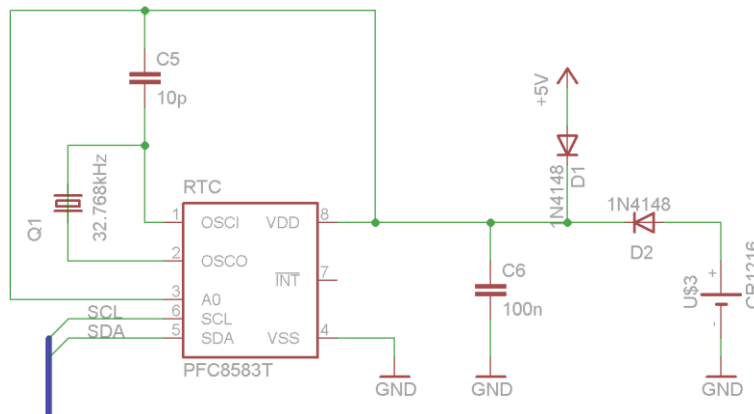
Pro správnou funkci logování přístupů je nutné nastavit správný čas. K tomu je nutné zaslání příkazu „sth:mm:ss,DD.MM.YYYY#“ přes sériovou linku RS 232. Parametr „s“ označuje příkaz SET (nastav); parametr „t“ označuje TIME (čas). Bezprostředně za těmito znaky následuje nastavování času:

1. „hh“ – nastavení hodin ve 24-hodinovém formátu,
2. „mm“ – nastavení minut v rozmezí 00 až 59,
3. „ss“ – nastavení sekund v rozmezí 00 až 59,
4. „ , “ – následuje oddělovací čárka (bez mezer),
5. „DD“ – nastavení dne včetně úvodních nul v rozmezí 01 až 31,
6. „MM“ – nastavení měsíce včetně úvodních nul v rozmezí 01 až 12,
7. „YYYY“ – nastavení roku v plném formátu např. 2012.
8. „#“ – potvrzovací znak.

Pokud je čas správně nastaven, zobrazí se informativní hláška.

Zjištění času:

Pro kontrolu nastaveného času slouží příkaz „gt“ zaslaný přes RS 232. Parametr „g“ označuje příkaz GET (vrat); parametr „t“ označuje TIME (čas).



Obrázek 5: Schéma zapojení PCF8583.

3.4.3 Logování přístupů

Pro možnost zpětné kontroly ukládá zařízení více než 7 000 posledních uskutečněných přístupů. Pokud se paměť pro logovací soubor zaplní, začnou se nejstarší záznamy automaticky mazat. Ukládají se pouze autorizované (tj. uskutečněné) vstupy. Přidávání a odebírání transpondéru z paměti a neautorizované přístupy logovány nejsou.

Logovací soubor je uložen v externí sériové EEPROM paměti typu 24LC512 o velikosti 512K bitů uspořádanou jako 65 536 slov po 8 bitech. Tento integrovaný obvod má 16-ti bitové adresování a komunikuje s mikrokontrolérem pomocí sběrnice I2C.

3.4.4 Přenos logovacího souboru na microSD kartu

Aby bylo možné přečíst informace z logovacího souboru, je nutný jeho přenos do zařízení schopného zobrazit textový soubor txt, např. PC. K přenosu je nutné mít microSD kartu naformátovanou pro souborový systém FAT32. Pokud bude naformátována pro jiný souborový systém, není zaručen úspěšný přenos.

1. MicroSD karta se vkládá do slotu umístěného pod bílým krytem zařízení, který je nutné odcvaknout pomocí plochého šroubováku.
2. Po vložení microSD karty se trvale rozsvítí červená LED dioda.
3. Nyní je nutno přiložit MASTER transpondér. Tím zařízení provede kontrolu souborového systému na kartě.
4. Proběhne-li kontrola úspěšně, LED dioda změní barvu na zelenou, čímž signalizuje, že je vše připraveno k přenosu souboru.
5. Pokud v tuto chvíli znovu přiložíme MASTER transpondér, zařízení zahájí přenos, který je signalizován blikáním zelené LED diody.
6. Po přenesení souboru zařízení vydá krátký zvukový signál, komunikace s microSD kartou se ukončí a LED zhasne. Tím je přenos úspěšně ukončen a soubor je ze zařízení odstraněn.
7. Opatrně nacvakněte kryt zařízení zpět.

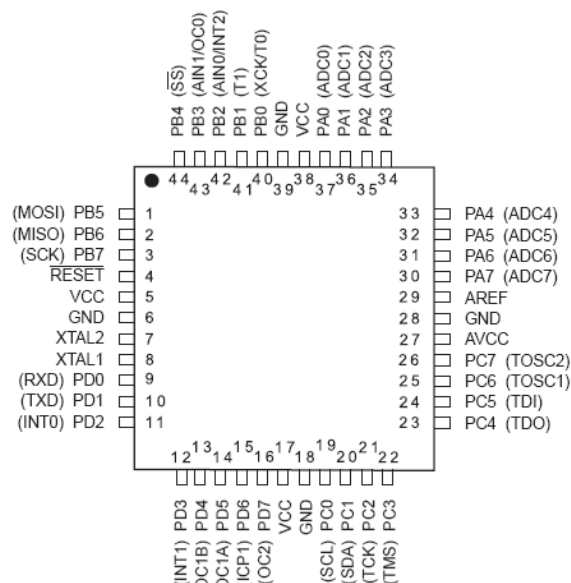
Logovací soubor naleznete v kořenovém adresáři microSD karty pod názvem YYMMDD_X.txt, kde YY představuje rok, MM měsíc, DD den, X pořadové číslo přenosu souboru.

3.5 Mikrokontrolér

Celé zařízení je řízeno mikrokontrolérem ATmega32 firmy ATMEL. Stará se o komunikaci mezi všemi integrovanými obvody a čtečkou. Využívá:

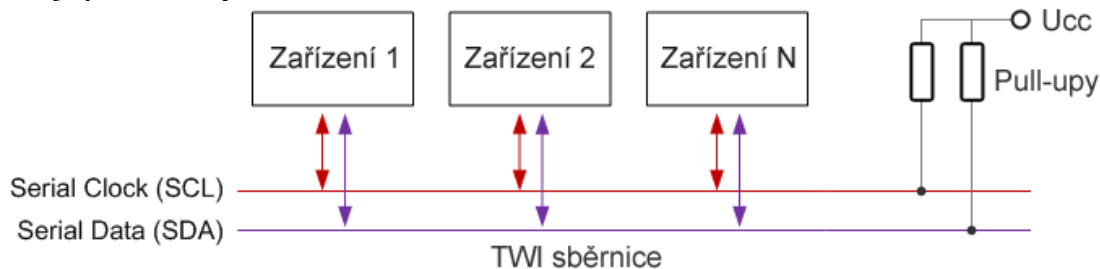
- rozhraní TWI pro komunikaci s externí EEPROM pamětí a obvodem reálného času,
- rozhraní SPI ke komunikaci s microSD kartou a k programování samotného mikrokontroléru,
- rozhraní UART pro komunikaci s RS 232 převodníkem,
- 2 externích přerušení INT0 a INT1 pro komunikaci s RFID čtečkou,
- interní EEPROM paměti pro ukládání uživatelských ID.

Na základě těchto požadovaných funkcí byl vybírán mikrokontrolér řady ATmega, který tyto funkce nabízí, je snadno dostupný, malých rozměrů a za výhodný poměr cena/výkon. Kvůli velikosti programu musela být zvolena varianta s alespoň 32Kb FLASH pamětí. Těmito parametry nejlépe odpovídal mikrokontrolér ATmega32, kterým je zařízení osazeno.



Obrázek 6: Schéma mikrokontroléru ATmega32.[13]

TWI (Two-wire Serial Interface) rozhraní je typ sériového rozhraní, známější pod pojmenování I2C. Pomocí dvou linek SCL (hodiny) a SDA (data) umožňuje komunikovat až se 128 zařízeními na sběrnici. Každé z těchto zařízení musí mít svoji unikátní 7-bitovou adresu. Dosahuje přenosové rychlosti až 400 kHz.



Obrázek 7: Připojování zařízení na TWI sběrnici.

SPI (Serial Peripheral Interface) rozhraní je vysokorychlostní full-duplexní sběrnice, dosahující přenosové rychlosti až 8Mb/s. Propojuje mikrokontrolér s periferními zařízeními. Využívá 4 linek, MISO (Master In Slave Out), MOSI (Master Out Slave In), SCK (hodinový signál) a SS (Slave Select – výběr Slave zařízení).

UART je flexibilní univerzální sériový přijímač a vysílač. Podporuje full-duplex, disponuje snadným a rozsáhlým nastavením přenosové rychlosti, detekcí ztráty znaku a chyby rámce. Vysílač obsahuje jeden zapisovací buffer, sériový posuvný registr, generátor parity a řídicí jednotku pro obsluhu rámců. Buffer zajišťuje kontinuální přenos dat bez zpoždění mezi rámci. Přijímač obsahuje jednotku pro rekonstrukci hodin a dat, detektor parity, řídicí logiku, posuvný registr a přijímací buffer. [17]

3.6 Převodník USB – UART

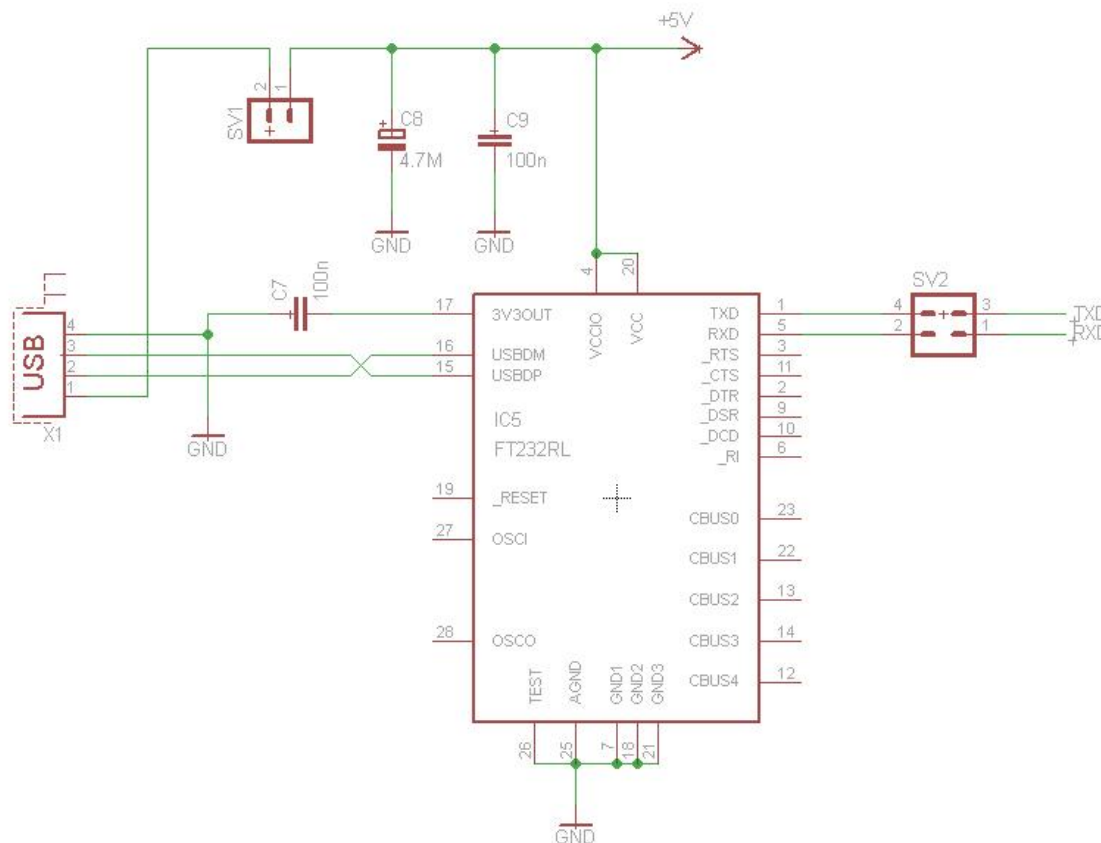
Pro snadné připojení k současným osobním počítačům je zařízení vybaveno USB konektorem typu B. Bohužel mikrokontrolér nemá hardwarovou podporu USB standardu, a proto byl do obvodu zařazen USB – UART převodník. Obvod FT232RL je plnohodnotný USB – UART konvertor s možností vyvedení externích hodin o frekvenci 6MHz, 12MHz, 24MHz nebo 48MHz a napětí 3,3V o maximální zatížitelnosti 50 mA. Jeho zapojení je velmi snadné

a provoz spolehlivý díky technologii TDIChip-ID™, která zaručuje rozpoznání v operačních systémech:

- Windows 98, 98SE, ME, Vista, XP 64-bit, XP Embedded, CE.NET 4.2 & 5.0
- MAC OS 8 / 9, OS-X
- Linux 2.4 a novější

Pro propojení s PC je nutné nastavit parametry komunikačního rozhraní na 19200, N, 8, 1 (tj. přenosová rychlost 19 200, žádný paritní bit, 8-bitová data, 1 stop bit).

Obvod vyžaduje DC napájení v rozmezí 3,3V – 5,25V a má již integrovaný obvod pro filtraci tohoto napětí. [18]

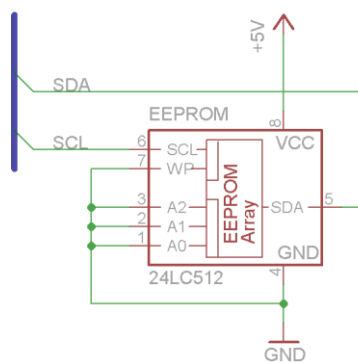


Obrázek 8: Schéma zapojení FT232RL.

3.7 Sériová EEPROM paměť

Paměť EEPROM (Electrically Erasable Programmable Read Only Memory) je velmi podobná paměti EPROM s tím rozdílem, že se maže elektricky a umožňuje smazání pouze určitých bajtů. Není nutné ji mazat celou. Velkou výhodou oproti paměti RAM je uchování dat i v případě odpojení od napájení. Naopak oproti RAM je pomalejší, má menší kapacitu, větší výkonovou ztrátu a je dražší. Z těchto důvodů se používá pro ukládání dat, které je nutno zachovat i při vypnutém zařízení jako jsou parametry firmwaru elektronických zařízení. Paměť komunikuje pomocí dvou nebo tří vodičů a data se do ní posílají bit po bitu. Díky tomu má paměť malé pouzdro většinou s 8 piny. [19], [20]

Paměť zvolená pro navrhovaný přístupový systém je 24LC512 o velikosti 512kB. Využívá se pro uložení záznamů logovacího souboru. Jeden záznam obsahující informaci o čase, datu a uživateli a zabírá v paměti 9 bajtů. Celkem je teda zařízení schopno uložit 7281 záznamů. Pokud nastane případ, že se celá paměť zaplní, začnou se nejstarší záznamy automaticky přepisovat novými.



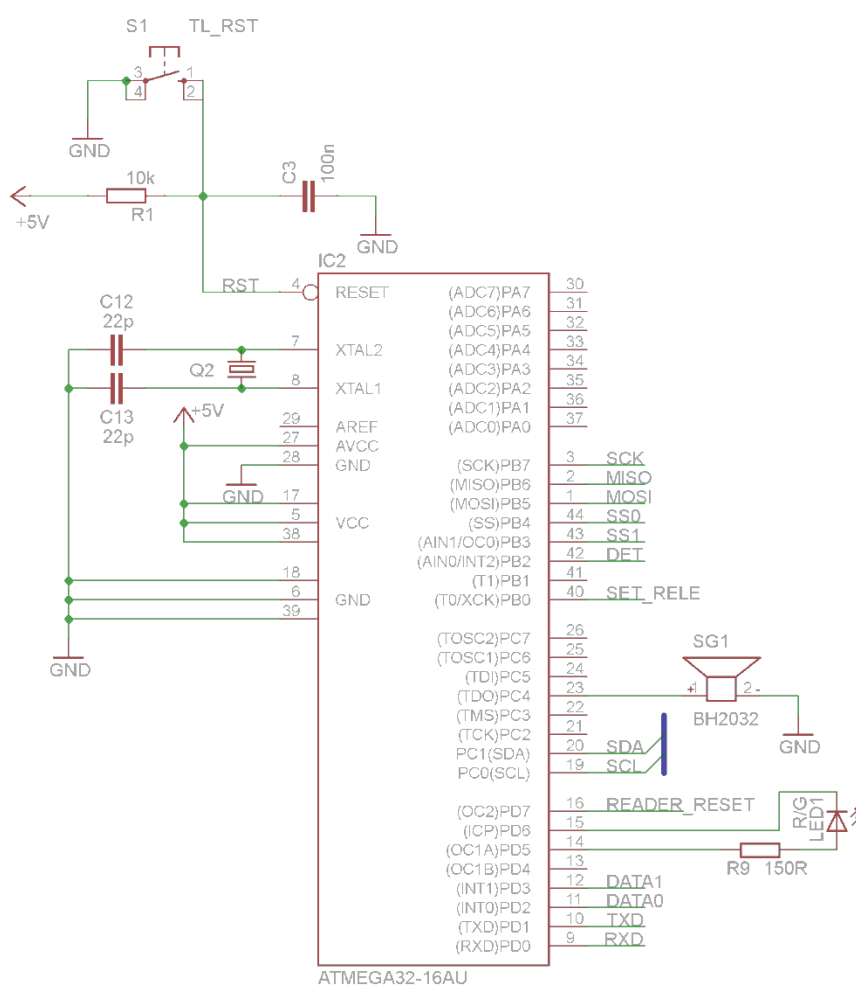
Obrázek 9: Schéma zapojení 24LC512.

4 REALIZACE

4.1 Schéma

4.1.1 Mikrokontrolér

Hlavní částí celého zařízení je mikrokontrolér ATmega32, který komunikuje se všemi ostatními integrovanými obvody přístupového systému. Kvůli požadavkům na malé rozměry byla použita varianta mikrokontroléru v pouzdru TQFP pro povrchovou montáž. Jako zdroj hodinového signálu je použit externí krystal o frekvenci 14 745,6 kHz, který se dobře hodí pro UART komunikaci s různými přenosovými rychlostmi. Ke snadnému restartování programu je k RESET pinu mikrokontroléru připojen mikrosplínač. Stiskem tohoto tlačítka si zařízení uchová informace o všech uložených transpondérech, MASTER transpondéru, nastavení času a data a údajích z logovacího souboru.



Obrázek 10: Schéma zapojení mikrokontroléru ATmega32.

4.1.2 Napájení

Jednoduchý způsob stabilizace napětí na požadované napěťové úrovni lze provést lineárním stabilizátorem. Jeho použití je nutno ověřit výpočtem ztrátového výkonu, aby se nadměrně nezahříval.

Výpočet ztrátového výkonu stabilizátoru 7805:

- Na vstup stabilizátoru je přivedeno napětí, které odpovídá zvýšenému napájecímu napětí o 10%.

$$U_{IN} = 24V$$

$$U_{IN\ MAX} = U_{IN} \cdot 1,1 = 24 \cdot 1,1 = 26,4V$$

- Na výstupu stabilizátoru je napětí:

$$U_{OUT} = 5V$$

- Předpokládaný maximální odebíraný proud:

$$I_{OUT} = 120mA$$

- Rozdíl napětí mezi vstupem a výstupem:

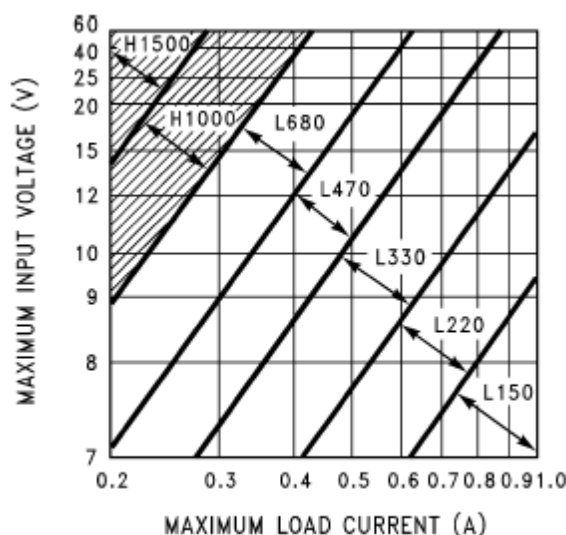
$$\Delta U = U_{IN\ MAX} - U_{OUT} = 26,4 - 5 = 21,4V \quad (1.1)$$

- Ztrátový výkon stabilizátoru napětí:

$$P_Z = \Delta U \cdot I_{OUT} = 21,4 \cdot 0,12 = 2,6W \quad (1.2)$$

Volba lineárního stabilizátoru napětí např. KIA7805AP se neukázala jako vhodná, kvůli velkému ztrátovému výkonu při připojení maximálního napětí. Ten může být bez chladiče maximálně 1,9 W [21]. Kvůli nedostatku prostoru však chladič nelze použít.

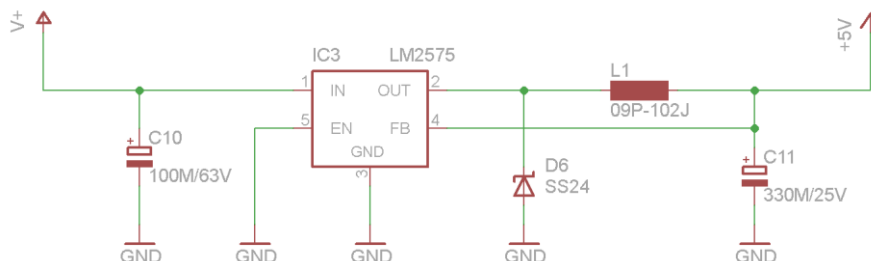
Další možností ke snížení vstupního napětí na požadované pracovní bylo použití spínaného regulátoru napětí LM2575T-5. Jeho základní zapojení vyžaduje volbu tlumivky a Schottkyho diody, která ovlivňuje účinnost. Tlumivka se určí z diagramu z *obrázku 11*, dle maximálního vstupního napětí a maximálního odebíraného proudu na výstupu. Zařízení bylo navrhováno tak, aby mělo nejvyšší účinnost spínaného regulátoru při 12V. Skutečná maximální proudová zatížitelnost je 0,12A. Nejbližší odpovídající hodnota v diagramu je 0,2A. Na základě těchto hodnot z diagramu vyplývá volba tlumivky H1000 (tj. indukčnost $L = 1mH$). Výběr diody se odvíjí od maximálního požadovaného vstupního napětí (tj. 24V), proto byla zvolena Schottky dioda SS24 s maximálním dopředným napětím 40V. [22]



Obrázek 11: Diagram pro výběr hodnoty indukčnosti tlumivky.[22]

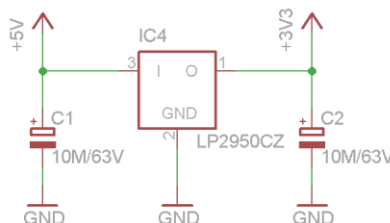
Volba spínaného regulátoru napětí LM2575T-5 do zatížitelnosti 1A se ukázala jako vhodná a byla použita. Na vstup zařízení lze ke svorkovnici CON2 (viz. *Obrázek 27*) připojit stejnosměrné napětí v rozmezí 9 - 24V. Na polaritě nezáleží, jelikož je zařízení vybaveno usměrňovacím můstkem. Napájení vnitřních obvodů je zajištěno stejnosměrným napětím 5V od spínaného zdroje

napětí nebo pomocí USB, které se dá volitelně pomocí jumperu odpojit. Pro bezproblémový chod by zařízení mělo být napájeno pouze jednou ze dvou jmenovaných možností.



Obrázek 12: Schéma zapojení spínaného regulátoru napětí 5V.

K napájení obvodu čtečky microSD karet je vyžadováno snížené napětí 3,3V. Pro tento účel by se pro většinu microSD karet dal využít výstup 3V3OUT USB – UART převodníku, který nabízí možnost vyvedení napětí 3,3V k jinému obvodu s maximálním odběrem 50mA. Na trhu však existují i karty, které udávají odběr 100mA, i pro ně bylo nutno zajistit funkčnost. Byl proto použit obvod s napěťovým stabilizátorem LP2950CZ-3.3 s nízkým úbytkem napětí a filtrační kondenzátory. [23]



Obrázek 13: Schéma stabilizátoru napětí 3,3V.

4.1.3 Spínání kontaktu relé

Spínací kontakty relé jsou vyvedeny na svorkovnici SV2 a jsou určeny ke spínání elektromagnetického dveřního zámku. Pokud je přístup oprávněný je relé sepnuto na 2s. Maximální zatížitelnost spínaných kontaktů je 5A při 250V AC nebo 5A při 30V DC. To spolehlivě postačuje obvyklým elektromagnetickým dveřním zámky, které odebírají maximálně 2,1A DC. [25]

Sepnutí relé je realizováno nepřímo přes NPN tranzistor BC817-16. Aby došlo k sepnutí tranzistoru, musela být vypočítána hodnota rezistoru R10.

- Nominální napětí a odpor vinutí cívky relé:

$$U = 5V$$

$$R = 125\Omega$$

- Proud protékající cívku relé:

$$I = \frac{U}{R} = \frac{5}{125} = 0,04A$$

- Minimální proudový zesilovací činitel tranzistoru:

$$hFE = 100$$

- Proud protékající bází tranzistoru nutný k sepnutí relé:

$$I_{b\ MIN} = \frac{I}{hFE} = \frac{0,04}{100} = 0,0004A \quad (1.3)$$

- Pro bezpečné sepnutí relé minimální protékající proud 5x zvýšíme:

$$I_b = I_{b\ MIN} \cdot 5 = 0,0004 \cdot 5 = 0,002A \quad (1.4)$$

- Napětí mezi bází a emitorem v sepnutém stavu:

$$U_{BE} = 1,2V$$

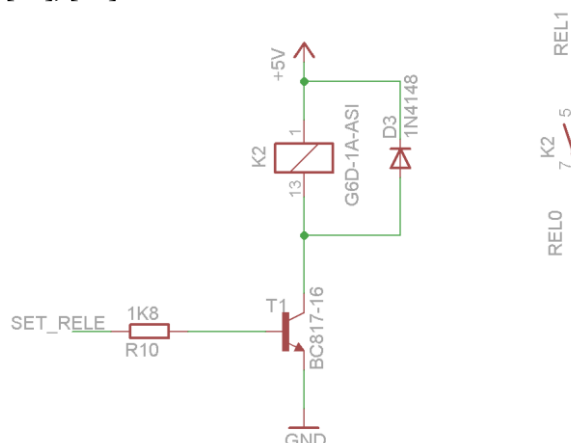
- Rozdíl výstupního napětí mikrokontroléru a U_{BE} , který protéká přes rezistor:

$$\Delta U = U_{MCU} - U_{BE} = 5 - 1,2 = 3,8V \quad (1.5)$$

- Maximální hodnota odporu rezistoru nutná k protečení I_b :

$$R_{R10} = \frac{\Delta U}{I_b} = \frac{3,8}{0,002} = 1900\Omega \quad (1.6)$$

Nejbližší běžně dostupná hodnota rezistoru je 1K8, a proto byla zvolena. Jako ochrana proti napěťovým špičkám při rozpínání relé je do obvodu zařazena rekuperační dioda 1N4148 v závěrném směru. [24], [25], [26]



Obrázek 14: Schéma zapojení spínacího relé.

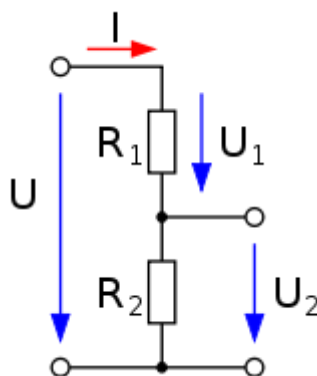
4.1.4 Čtečka microSD karet

MMC, SD a microSD karty ke komunikaci používají protokol SPI. Jeho logika pracuje s napěťovou úrovní 3,3V, na rozdíl od 5V logiky mikrokontroléru. Proto bylo nutné 5V logiku snížit pomocí odporového děliče napětí.

Dělič napětí je založen na Ohmově zákoně a používá se pro rozdělení nebo snížení napětí. Jeho základní zapojení se skládá ze dvou rezistorů R_1 a R_2 . Pro výpočet napětí platí vztahy:

$$U_1 = U \cdot \frac{R_1}{R_1 + R_2} \quad (2.1)$$

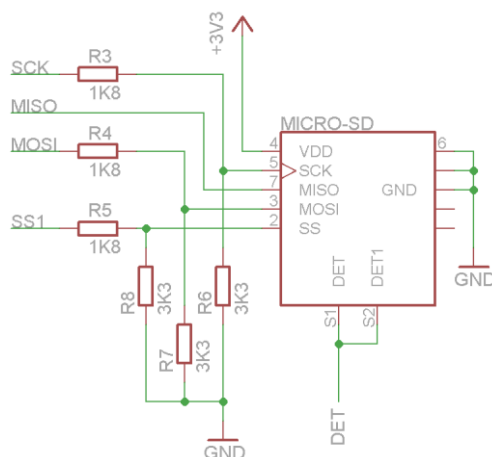
$$U_2 = U \cdot \frac{R_2}{R_1 + R_2} \quad (2.2)$$



Obrázek 15: Schéma odporového děliče napětí.

V našem případě potřebujeme rozdělit 5V ideálně na 3,3V a 1,7V. Použít budeme pouze větve s napětím 3,3V. Využito bylo již ověřené funkční zapojení vývojového modulu GOTRONIK verze 2, na kterém byla čtečka navrhována a laděna. Dosazením do vzorce 3.2 byla pouze ověřena napěťová úroveň.

$$U_2 = U \cdot \frac{R_2}{R_1 + R_2} = 5 \cdot \frac{3300}{1800 + 3300} \doteq 3,2V$$

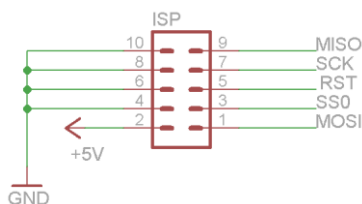


Obrázek 16: Schéma zapojení čtečky microSD.

Výstupy označené DET a DET1 jsou bez vložené karty uzemněny. Při vložení karty se tyto výstupy odpojí, díky tomu lze snadno rozpoznat vloženou kartu.

4.1.5 ISP programovací konektor

Pro možnost ladění a aktualizování firmwaru zařízení pomocí běžných programátorů firmy ATMEL, byl na DPS přidán 10-ti pinový ISP konektor.

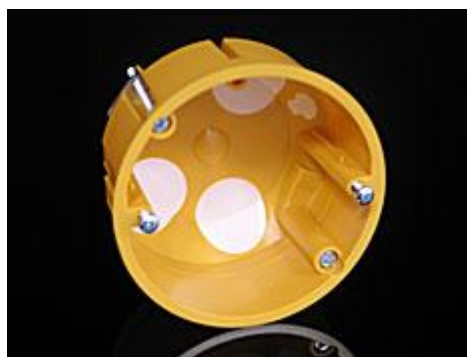


Obrázek 17: Zapojení ISP programovacího konektoru. [27]

4.2 Výběr pouzdra

Původním záměrem bylo umístit zařízení na vnitřní stranu dveří, kde by bylo chráněno před krádeží i mechanickým poškozením cizí osobou. Na venkovní straně dveří by bylo pouze označeno místo přiložení transpondéru a čtení by probíhalo skrze dveře. Toto řešení bylo nakonec zavrženo z důvodu malé univerzálnosti instalace v inteligentních budovách, především z hlediska složitého vedení vodičů k zařízení.

Aby bylo možné zařízení snadno instalovat v budovách a zároveň esteticky nevybočovalo od standardního elektroinstalačního vybavení jako vypínače, zásuvky, anténní a síťové přípojky a další, bylo voleno umístění pod omítku do kulatých elektroinstalačních krabic. Vnitřní hloubka krabice musí být alespoň 45 mm. Díky tomu je celé zařízení ukryto ve zdi a viditelná část je pouze rámeček se záslepkou pro vypínač s indikační dvoubarevnou LED diodou. Bohužel toto řešení nezaručuje odolnost proti mechanickému vniknutí, a proto se hodí pouze na místa, kde je jeho zabezpečení řešeno jiným (např. kamerovým) systémem.



Obrázek 18: Elektroinstalační krabice do dutých zdí.

Vrchní viditelný díl tvoří bílý rámeček s vypínačovou záslepkou firmy ABB. Do krytu bylo vyříznuto několik děr, aby vyhovoval našim potřebám, například pro připevnění DPS, umístění indikační LED diody nebo otvor pro microSD kartu. Vrchní kryt je s elektromontážní krabicí spojen dvěma vruty.



Obrázek 19: Vrchní kryt zařízení.

4.3 Návrh DPS

DPS byla navržena pomocí programu EAGLE. Tento program je určen pro navrhování schémat, navrhování spojů a exportování vytvořených návrhů do postscriptových souborů nebo pro plotry.

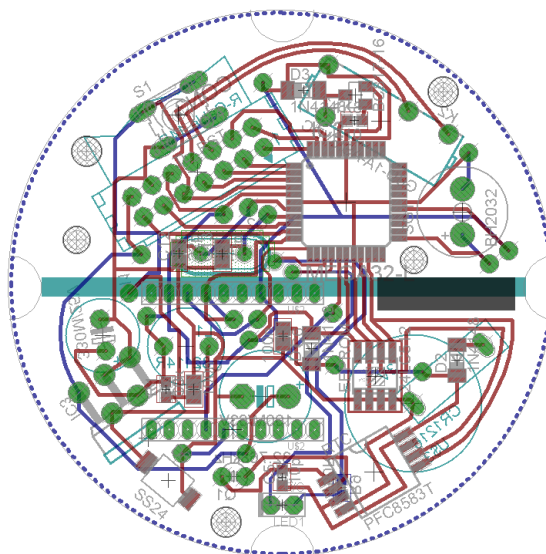
EAGLE disponuje velkou knihovnou součástek, která obsahuje většinu použitých součástek v zařízení. Přesto bylo nutno součástky upravit zvětšením pájecích plošek pro snadnější ruční pájení. Některé součástky, například držák baterie nebo slot microSD karty, bylo nutno navrhnout kompletně celé, včetně schématické značky a pouzdra.

Program je v Lite verzi volně ke stažení pro studentské a nekomerční účely. Oproti placené verzi je omezen následujícími vlastnostmi:

- Použitelná plocha desky je omezena na 100 x 80 mm (4 x 3,2 palce).
- Mohou být použity jen dvě signálové vrstvy spojů (vrchní a spodní strana).
- Editor schématu může vytvořit schéma pouze na jednom listu.[28]

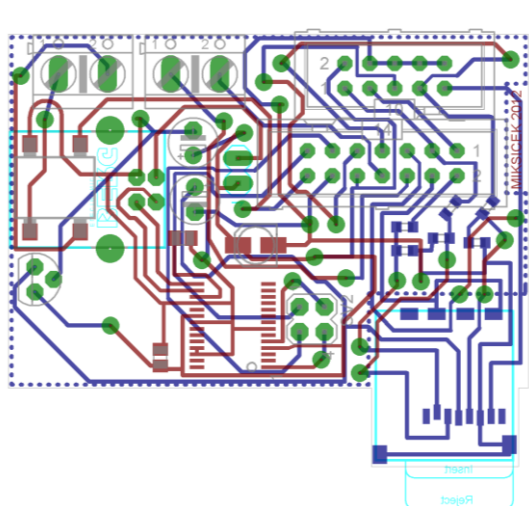
Vzhledem ke stísněnému prostoru uvnitř elektroinstalační krabice, mohla být maximální velikost DPS 53 mm ve tvaru kruhu. Tak malý prostor nestačil k osazení všech součástek, a proto bylo nutno udělat dvě DPS. Základní a přídatnou, které jsou k sobě připevněny dvěma šrouby M2. Obě dvě jsou oboustranné s minimální šířkou cest 12 mil.

Základní deska obsahuje mikrokontrolér, externí EEPROM, obvod reálného času, slot pro RFID čtečku, RESET tlačítko a další součástky vyjmenované v příloze č. 12. Je instalována rovnoběžně s vrchním krytem, k němuž je přišroubována třemi šrouby. S druhou (přídavnou) deskou je propojen pomocí plochého 14-ti žilového kabelu. Navíc je v desce vyříznut otvor obdélníkového tvaru, kterým je ze zadní strany prostrčena přídatná DPS se slotem pro microSD kartu.



Obrázek 20: Návrh základní desky.

Na přídatné desce je osazen slot microSD karty, USB konektor, ISP programovací konektor, svorkovnice pro externí připojení a další součástky vyjmenované v příloze č.12. Kvůli microSD slotu musela být umístěna kolmo na hlavní desku, aby šlo kartu do zařízení jednoduše vložit bez nutnosti demontáže celého zařízení ze zdi. Pro spojení se základní deskou byly na dvě místa s rozlitou mědí připájeny speciální kusy měděného plechu ve tvaru písmene „L“. Ty mají na jedné stěně vyvrtaný otvor pro šroub M2 a na stěně kolmé jsou plné, aby šly snadno připájet.



Obrázek 21: Návrh přídavné desky.

Pomocí CAM procesoru byly vygenerovány soubory postscriptu pro další zpracování programem Adobe Illustrator. Ten umožňuje snadno vytvořit jeden PDF soubor s několika obrázky plošných spojů.

4.4 Výroba a osazení DPS

Výroba plošného spoje v neprofesionálních podmínkách nabízí 2 schůdné cesty k přenesení vzoru plošného spoje na desku s rozlitou mědí (cuprextit) s přijatelnou kvalitou výsledku. Liší se jak cenou, tak složitostí a kvalitou dosaženého výsledku. Proto je nutné zvážit, pro jaké účely a za jakou cenu má být deska vyrobena.

4.4.1 Metody přenesení obrazce na DPS

První způsob výroby je metoda nažehlováním toneru. Je jednoduchá, levná a rychlá. Je založena na možnosti přenesení tonerové barvy za tepla na desku s rozlitou mědí. Obrazec plošného spoje vytiskneme zrcadlově převrácený na speciální folii nebo nesavý papír. Tento obrazec položíme tiskem k DPS a přiložíme žehličku. Po prohřátí celé desky žehličku odstraníme a necháme volně na vzduchu nebo lépe pod vodou vychladnout. Potom by měl jít vzor volně odstranit a deska je tím připravena k leptání.

Lze ji snadno použít v domácích podmínkách, protože vyžaduje pouze běžně dostupné dostupné věci jako:

- barevné lepicí papíry nebo speciální fólii určenou k přezhlování toneru,
- laserovou tiskárnu,
- lepicí pásku,
- žehličku,
- vodu. [29]

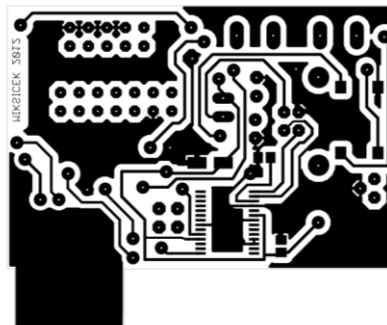
Druhý způsob, který byl zvolen pro výrobu prototypu zařízení, je metoda přenesení obrazce plošného spoje fotocestou na cuprextit se speciální fotocitlivou vrstvou. Tuto vrstvu lze nanést na běžný cuprextit nástřikem emulze Pozitiv 20 nebo již zakoupit desku, která je touto vrstvou opatřena z výroby. Nástřik vrstvy je proces velice citlivý na čistotu prostředí. Následuje vytvrzení emulze 24 hodin při pokojové teplotě nebo 15 minut při teplotě 70°C.

Samotné přenesení obrazce vyžaduje předlohu vytištěnou na kancelářský papír, pauzovací papír, fólii nebo vysvícenou na film. Ideální předloha má mít tyto vlastnosti:

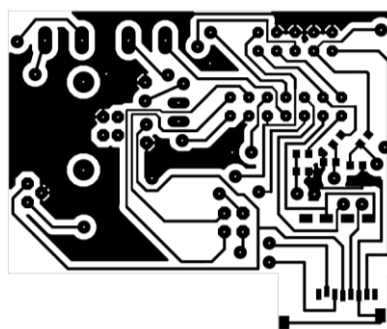
- vysoký kontrast v UV spektru,
- vysokou ostrost a dostatečné rozlišení,
- tvarovou stálost a přesnost,

- motiv vytištěný zrcadlově převrácený, aby se dal položit tiskem přímo na desku a nevznikaly tak stíny. [30]

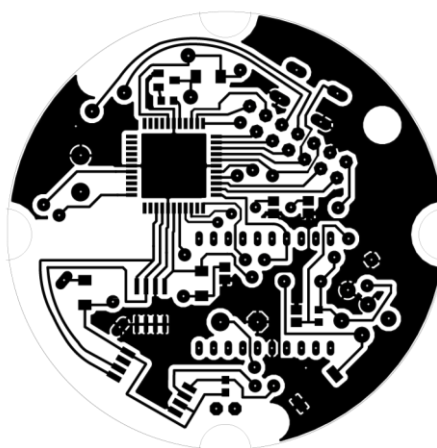
Těmto požadavkům dokonale vyhovuje předloha vysvícená na film, kterou dosahujeme nejlepších výsledků, a proto byla pro výrobu vybrána. Osvit předlohy na film se zhotovuje na osvitových jednotkách, kterými většinou disponují grafická studia nebo tiskárny. Soubory pro osvitovou jednotku musí být ve formátu PDF v měřítku 1:1. Její velkou výhodou je vícenásobné použití a precizní přesnost.



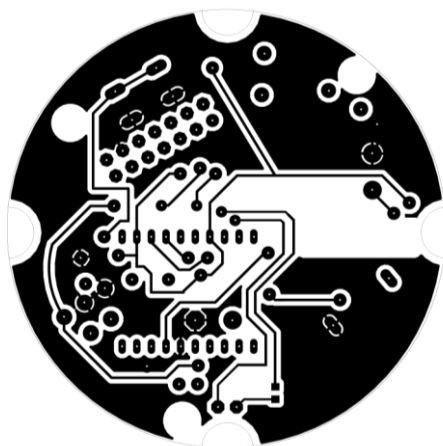
Obrázek 22: Vrchní strana předlohy pro přídavnou desku.



Obrázek 23: Spodní strana předlohy pro přídavnou desku.



Obrázek 24: Vrchní strana předlohy pro základní desku.



Obrázek 25: Spodní strana předlohy pro základní desku.

Pokud jsou DPS oboustranné je nutno napasovat předlohy tiskem k sobě a přilepit ze tří stran lepicí páskou tak, aby vznikla kapsa, do které se vloží fotocitlivý cuprextit. Takto připravenou desku s předlohami vložíme mezi dvě očištěná skla, která k sobě přitiskneme, například kuličky, aby se předloha mezi skly nepohnula.

4.4.2 Osvit a vyvolání

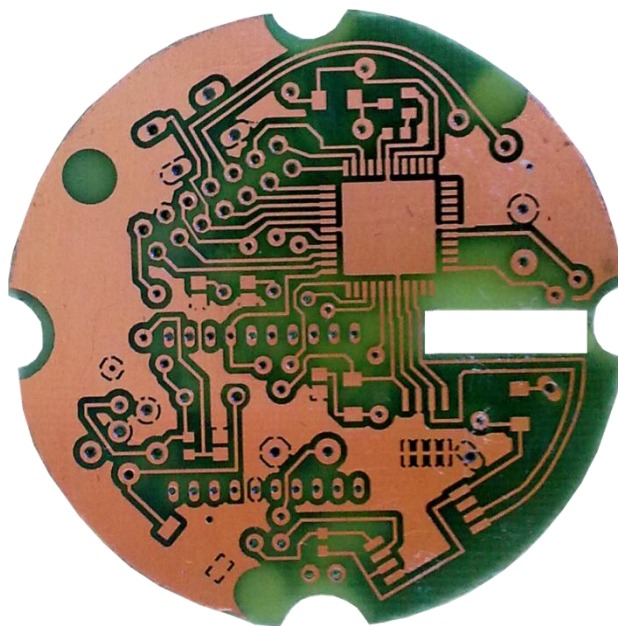
Samotný osvit předlohy na desku probíhá pod UV-A světlem. K tomuto účelu mohou být použity různé zdroje výbojek, zářivek a UV LED diod. K našemu účelu byl použit UV LED panel s několika desítkami UV LED diod, které vyzařují velmi měkké UV záření. K osvitu desky stačí přibližně 4 minuty z každé strany. Pokud je předloha dostatečně kontrastní, delší osvit nevádí.

Po osvitu je nutné desku vyvolat v roztoku NaOH při koncentraci 10 g/l. Vyvolává se při pokojové teplotě v misce, ve které s plošným spojem pohybujeme a obracíme, pokud je DPS oboustranná. Jednostranné desky se neobracují a vyvoláváme je fotoemulzí nahoru. Při práci s vývojkou je nutné používat pinzetu, aby se zamezilo kontaktu s kůží, kterou může poleptat. Vyvolání je ukončeno, pokud plocha, která má být odleptána, je zbavena fotocitlivé emulze a je vidět čistá měď. [30]

Pokud je třeba motiv na DPS upravit, lze to snadno provést lihovým fixem.

4.4.3 Leptání

K leptání používáme roztok chloridu železitého. Do misky nalijeme dostatečné množství tohoto roztoku. Pro rychlejší leptání je dobré ho zahřát alespoň na teplotu 30°C ponořením uzavřené nádoby s roztokem do teplé vody. Poté položíme DPS opatrně na hladinu, aby se deska neponořila a zároveň aby pod ní nevznikly vzduchové bubliny. Leptání jedné strany trvá v závislosti na koncentraci a teplotě roztoku od 10 do 45 minut, proto je třeba průběžně kontrolovat, zda již není DPS vyleptána. Při kontaktu s chloridem železitým je dobré používat ochranné pomůcky, jelikož zanechává obtížně smývatelné skvrny na kůži i na oblečení. Zároveň také naleptává kovové povrchy. Po leptání musíme desku důkladně omýt vodou a mýdlem, aby se smyl všechny leptací roztok.



Obrázek 26: Vrchní strana vyrobené základní desky.

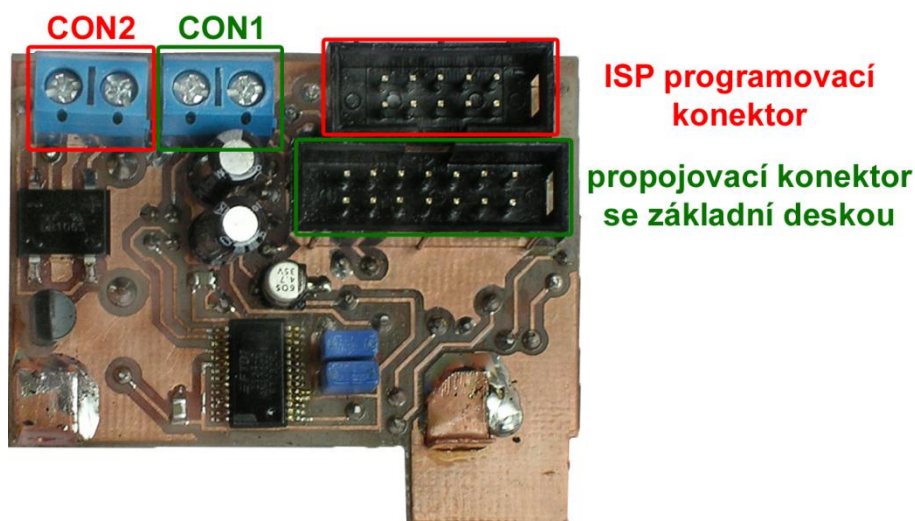
4.4.4 Dokončovací výroba a osazení

K vrtání byla použita stojanová vrtačka. Všechny díry pro prokovy a nožičky integrovaných obvodů byly vrtány vrtákem o průměru 0,8 mm. Pokud byl otvor pro součástku příliš malý, lze ho snadno převrtat na větší. Součástky by do DPS měly jít zamáčknout přiměřenou silou. Nakonec byly zabroušeny otřepty po vrtání.

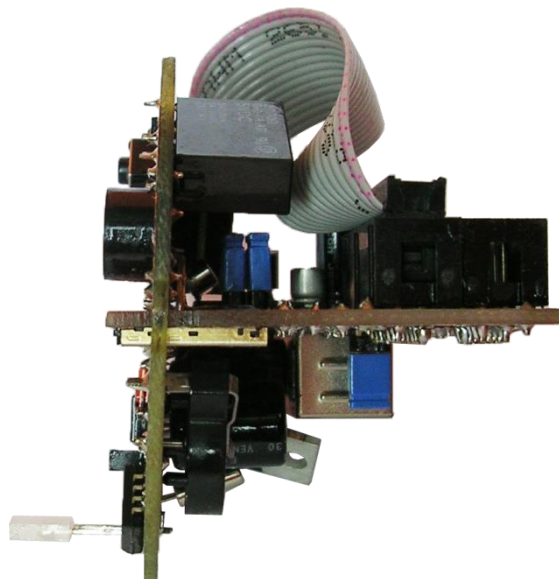
Ke snadnému pájení a ochraně DPS před korozí je nutná povrchová úprava. Nejdříve je nutno odstranit zbylou emulzi malým množstvím acetonu nebo líhu naneseného na kus látky, kterým desku pečlivě utřeme. Postup opakujeme, dokud deska není dokonale čistá.

Okamžitě po umytí byl na desku nanesen ochranný pájitelný lak, aby nedošlo k oxidaci mědi. V laku je rozpuštěno tavidlo, takže při pájení již není nutné používat kalafunu a práce se tím velmi ulehčí.

Pájení oboustranných desek vyrobených neprofesionálním způsobem začíná osazením všech prokovů. Následují SMD součástky, malé vývodové součástky a velké vývodové součástky. Nakonec bylo nutné připojit ploché kabely k samořezným konektorům, a tím desky propojit.



Obrázek 27: Popis konektorů přídavné desky.



Obrázek 28: Boční pohled na složené finální řešení.

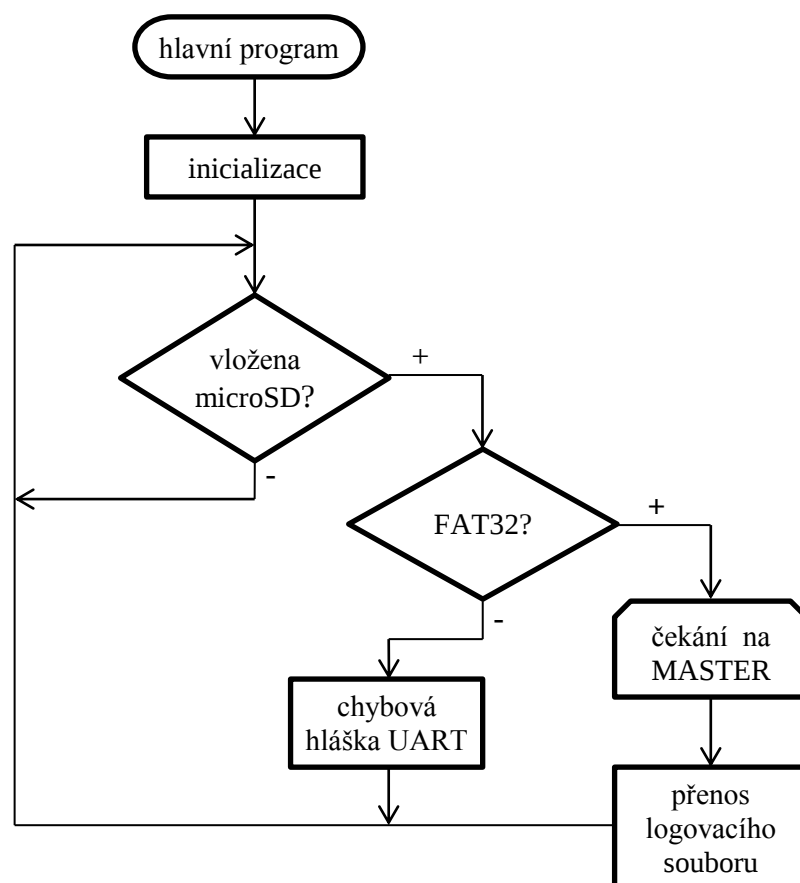
4.5 Programování firmwaru

Pro mikrokontrolér ATmega32 bylo nutno vyvinout vlastní firmware, který se stará o veškerou datovou komunikaci. K vývoji byl využit software firmy Atmel, AVR Studio 4. Ten umožňuje psaní zdrojového kódu v assembleru nebo v jazyce C. V našem případě byl zdrojový kód psán v jazyce C s využitím volně šiřitelného nástroje WinAVR, který obsahuje i kompilátor AVR GCC.

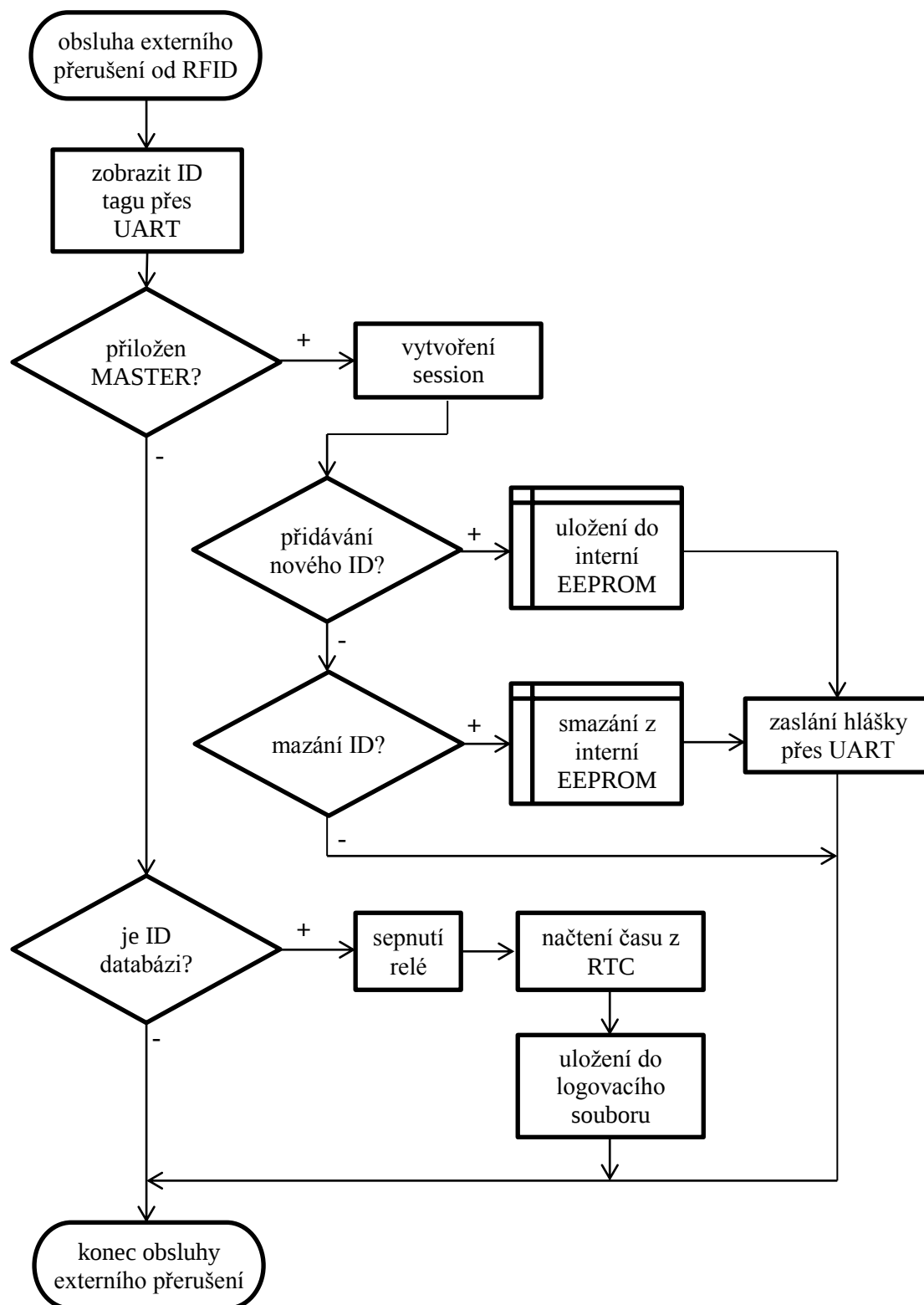
Zdrojový kód má téměř 2500 řádků a je rozčleněn na 9 souborů. Každý z nich obsahuje funkce pro jinou část nebo funkci zařízení. Jmenovitě například funkce pro správu uživatelů, přijímání příkazů přes RS 232, I2C komunikace, SPI komunikace, rutiny pro práci s SD kartou nebo rutiny pro práci se souborovým systémem FAT32. Pro komunikaci s RFID čtečkou je využito externího přerušení. Zkompilovaný soubor v mikrokontroléru využívá 54% paměti určené pro program a 86% paměti určené pro proměnné. Právě velikost paměti pro proměnné byla v několika ohledech limitující. Například pro přenos logovacího souboru bylo nutné zvolit vhodně velké buffery, aby bylo možno přenést několik tisíc záznamů do jednoho souboru a zároveň nedošlo k přetečení paměti pro proměnné.

Přenesení zkompilovaného *.hex souboru bylo provedeno pomocí programátoru pro rozhraní STK500. To umožňuje nahrávat data přímo z vývojového prostředí AVR Studia do mikrokontroléru. Programátor se k zařízením připojuje pomocí 10-ti pinového ISP konektoru, který je umístěn na přídatné desce (viz. Obrázek 27). Během programování je nutné, aby byl mikrokontrolér napájen.

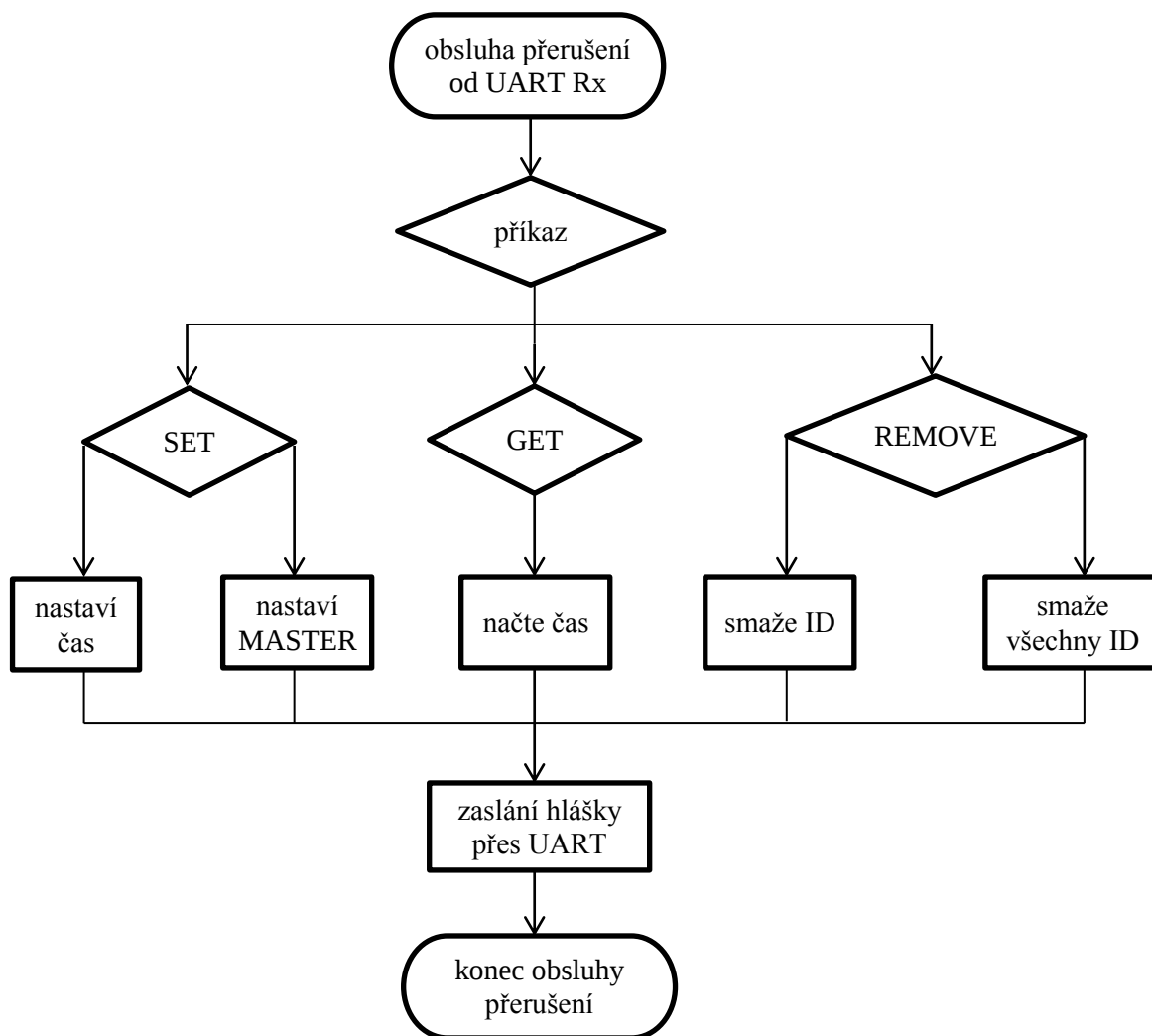
Následující vývojové diagramy popisují základní strukturu programu. V samotném hlavním programu (main) se pouze zjišťuje, zda byla vložena microSD karta. Ostatní podprogramy jsou spouštěny přerušeními.



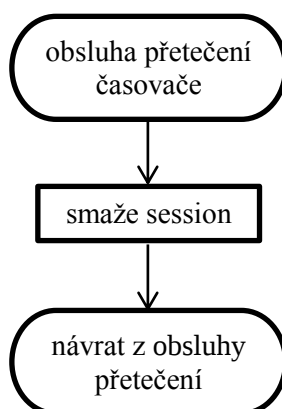
Obrázek 29: Vývojový diagram hlavního programu.



Obrázek 30: Vývojový diagram zpracování dat od modulu RFID čtečky.

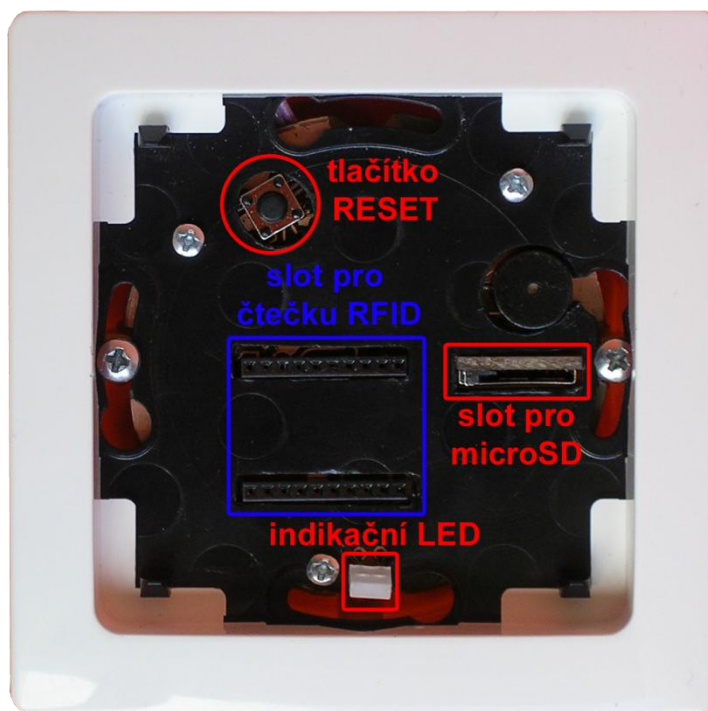


Obrázek 31: Vývojový diagram obsluhy přerušení od UART jednotky při zadávání příkazů.



Obrázek 32: Vývojový diagram obsluhy přetečení čítače.

4.6 Funkčnost hotového zařízení



Obrázek 33: Popis zařízení po odcvaknutí vrchního krytu.

Byla testována funkčnost zařízení jako celku, včetně všech jeho funkcí. Z hlediska vyvinutého firmwaru, zařízení pracuje spolehlivě a za dobu testovacího provozu nebyly nalezeny žádné problémy.

Objevily se však nedostatky v přesnosti běhu času, který se mírně předbíhá oproti skutečnosti. Předbíhání se pohybuje v řádu jednotek sekund za týden. To lze řešit změnou velikosti kondenzátoru C5. Bohužel testování trvalo příliš krátkou dobu na to, aby se dala blíže určit nepřesnost a provést korekce. Další nedostatek byl nalezen v použitém slotu microSD karet, který je vyroben z tenkého plechu, a jeho mechanické části jsou velmi citlivé na čistotu prostředí. V důsledku toho došlo několikrát k chybnému detekování karty nebo karta nešla do slotu zacvaknout.

Další zjištěný nedostatek se týká opět obvodu reálného času a to konkrétně změny roku. Pokud dochází k přelomu nepřestupného roku na přestupný je nutno ručně změnit datum. Je to způsobeno tím, že obvod uchovává informace o roce pouze ve tvaru 0 až 3, dle toho zda je přestupný či nikoli. O jeho transformaci do plného tvaru se stará mikrokontrolér. Ten ovšem sám o sobě není schopen zjistit, kdy dojde k přelomu roku. Tento problém by vyžadoval aktivaci přerušení od obvodu reálného času při změně roku. Bohužel pin externího přerušení nebyl při návrhu DPS propojen s mikrokontrolérem, a proto by tento problém musel být řešen úpravou DPS.

4.7 Návrhy na zlepšení

Na základě testování zařízení vzniklo několik návrhů pro vylepšení zařízení do budoucna.

- Kvůli snadnému vniknutí k samotnému zařízení a případnému zneužití spojením správných kontaktů, a tím i k obejití procesu autorizace, by měl být do zařízení integrován alarm, který by se spustil při neoprávněném vniknutí.
- Pro použití ve školách a firmách s přetržitým provozem vytvořit funkci, která by umožňovala nastavit časové rozmezí pro povolení přístupu, například na dobu školního vyučování nebo během pracovních směn.
- Vytvořit funkci pro přenos logovacího souboru po RS232.

5 ZÁVĚR

Tato práce se zabývala návrhem a uplatněním technologie RFID v praxi na funkčním zařízení. Bylo nutno seznámit se s principem této technologie, základními zapojeními elektrotechniky, programem EAGLE na návrh schémat a desek plošných spojů a programem AVR Studio pro programování mikrokontroléru ATmega32 v jazyku C.

Pro zařízení byly navrženy funkce zajišťující správu uživatelů, logování přístupů, přenos logovacího souboru na microSD karty a nastavení parametrů zařízení pomocí RS232. K tomu bylo nutné seznámit se s protokoly I2C, SPI a UART rozhraním.

Kapitola 2 Problematika identifikace objektů se zabývá použitím RFID v současnosti a jeho možným rozvojem do nových oblastí v budoucnu. Popisuje základní princip pasivní komunikace, pracovní frekvence, které jsou ve většině případů celosvětově uznávané a hlavní rozdíly mezi aktivní a pasivní technologií.

Kapitola 3 Návrh přístupového systému popisuje různé možnosti řešení, zdůvodňuje volbu použitého řešení, zabývá se otázkou zabezpečení komunikace a riziky zneužití. Podrobně popisuje funkce a ovládání zařízení, použité komunikační protokoly, volbu paměti pro ukládání logovacího souboru a obvod reálného času.

Kapitola 4 Realizace rozebírá volbu konkrétních součástek použitých ke stabilizaci napětí, volbu mikrokontroléru a relé. Zabývá se výběrem vhodného pouzdra pro zařízení, návrhem a výrobou prototypu zařízení. Je zde uvedeno několik vývojových diagramů, dle kterých byl naprogramován firmware. Závěrečná část této kapitoly shrnuje poznatky získané během testování zařízení a navrhuje několik vylepšení pro budoucí vývoj.

SEZNAM POUŽITÉ LITERATURY

- [1]: What is RFID?. AIM. *The global trade association for automatic identification* [online]. [2011] [cit. 2012-05-17]. Dostupné z: http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp
- [2]: PROJECT INVEST. *RFID portál* [online]. [2009] [cit. 2012-05-17]. Dostupné z: <http://www.rfidportal.cz/>
- [3]: Informační systémy v logistice. In: *IT řešení pro logistiku* [online]. 2012 [cit. 2012-05-17]. Dostupné z: <http://www.systemonline.cz/it-pro-logistiku/informacni-systemy-v-logistice.htm>
- [4]: Výhody RFID a použití v praxi. *Combitrading* [online]. [2010] [cit. 2012-05-17]. Dostupné z: <http://www.combitrading.cz/technologie/vyhody-rfid.html>
- [5]: About RFID. *RFID-Handbook* [online]. 1.5.2012 [cit. 2012-05-17]. Dostupné z: <http://www.rfid-handbook.de/rfid/index.html>
- [6]: VOJTĚCH, L. RFID - technologie pro internet věcí. *Access server* [online]. Praha, 12.2.2009 [cit. 2012-05-17]. Dostupné z: <http://access.fel.cvut.cz/view.php?cisloclanku=2009020001>
- [7]: WEIS, Stephen A. *RFID (Radio Frequency Identification): Principles and Applications* [online]. Cambridge, 2006 [cit. 2012-05-17]. Dostupné z: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.5224>. MIT Computer Science and Artificial Intelligence Laboratory.
- [8]: SWEDBERG, Claire. Chip-size Passive RFID Tag Promises Long Range. *RFID Journal* [online]. 3.2.2009, s. 3 [cit. 2012-05-18].
- [9]: PATÁKOVÁ, Jitka. *Návrh evidence docházky s využitím RFID čipů*. Brno, 2008. Bakalářská práce. VUT v Brně. Vedoucí práce Ing. JIŘÍ KRÍŽ, Ph.D.
- [10]: Active RFID Tag. In: *Technovelgy* [online]. [2005] [cit. 2012-05-18]. Dostupné z: <http://www.technovelgy.com/ct/technology-article.asp?artnum=21>
- [11]: Passive RFID Tag In: *Technovelgy* [online]. [2005] [cit. 2012-05-18]. Dostupné z: <http://www.technovelgy.com/ct/technology-article.asp?artnum=47>
- [12]: Asteroid Navigation. BURTON, Roland. *Stanford University* [online]. 30.7.2011 [cit. 2012-05-18]. Dostupné z: <http://www.stanford.edu/group/ar/rl/projects/asteroid-navigation>
- [13]: *Datasheet Atmel: ATmega32*. 2011, 346 s. [cit. 2012-05-18]. Dostupné z: <http://www.atmel.com/Images/doc2503.pdf>
- [14]: Jak pašáci aplikují RFID. *Sdělovací technika* [online]. 2008, č. 2 [cit. 2012-05-18]. Dostupné z: http://crypto.hyperlink.cz/files/ST_2008_02_x_x.pdf
- [15]: Kladivo na pašáky – Q5. *Sdělovací technika* [online]. 2008, č. 3 [cit. 2012-05-18]. Dostupné z: http://crypto.hyperlink.cz/files/ST_2008_03_x_x.pdf
- [16]: NXP. *Datasheet PCF8583* [online]. 2010, 37 s. [cit. 2012-05-18]. Dostupné z: http://www.nxp.com/documents/data_sheet/PCF8583.pdf
- [17]: MATOUŠEK, David. *Práce s mikrokontroléry ATMEL AVR: [měření, řízení a regulace pomocí několika jednoduchých přípravků]*. 1. vyd. Praha: BEN - technická literatura, 2006, 319 s. ISBN 80-730-0174-8.
- [18]: FTDI. *Datasheet FT232R*. 38. vyd. 2012, 43 s. [cit. 2012-05-18]. Dostupné z: http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT232R.pdf
- [19]: Learn about EPROMs and more. *Andromeda Research Labs* [online]. ©2010 [cit. 2012-05-18]. Dostupné z: <http://www.arlabs.com/help.htm>
- [20]: Připojení sériové paměti EEPROM. *DH servis* [online]. © 2002-2012 [cit. 2012-05-18]. Dostupné z: <http://www.dhservis.cz/eprom.htm>
- [21]: NATIONAL SEMICONDUCTOR. *Technical data: KIA7805AP*. [online]. 2010, 20 s. [cit. 2012-05-18]. Dostupné z: <http://www.gme.cz/dokumentace/330/330-001/dsh.330-001.1.pdf>
- [22]: NATIONAL SEMICONDUCTOR. *LM1575/LM2575/LM2575HV: Simple switcher*. [online]. 2004, 27 s. Dostupné z: <http://www.gme.cz/dokumentace/330/330-086/dsh.330-086.1.pdf>
- [23]: NATIONAL SEMICONDUCTOR. *LP2950/LP2951: Series of Adjustable Micropower Voltage Regulators* [online]. 2009 [cit. 2012-05-18]. Dostupné z: <http://www.gme.cz/dokumentace/331/331-047/dsh.331-047.1.pdf>
- [24]: BEZSTAROSTI, Jiří. Tranzistor jako spínač. *RoboDoupě* [online]. 9.3.2012 [cit. 2012-05-18]. Dostupné z: <http://robodoupe.cz/2012/tranzistor-jako-spinac/>

- [25]: OMRON. *PCB Power Relay – G6D* [online]. 4 s. [cit. 2012-05-18]. Dostupné z: <http://www.gme.cz/dokumentace/634/634-649/dsh.634-649.1.pdf>
- [26]: DISCRETE SEMICONDUCTORS. *BC817: NPN general purpose transistor* [online]. 1.6.1999, 8 s. [cit. 2012-05-18]. Dostupné z: <http://www.gme.cz/dokumentace/912/912-005/dsh.912-005.1.pdf>
- [27]: ATMEL. *Application Note: Atmel AVR042: AVR Hardware Design Considerations* [online]. 2011, 16 s. [cit. 2012-05-18]. Dostupné z: <http://www.atmel.com/images/doc2521.pdf>
- [28] Freeware. CADSOFT COMPUTER GMBH. *Eagle online* [online]. © 2001 [cit. 2012-05-18]. Dostupné z: <http://www.eagle.cz/freeware.htm>
- [29]: Výroba DPS nažehlením toneru. *HW.cz: Vše o elektronice a programování* [online]. 17.5.2005 [cit. 2012-05-18]. Dostupné z: <http://www.hw.cz/Teorie-a-praxe/Dokumentace/ART1286-Vyroba-DPS-nazehlenim-toneru.html>
- [30]: Výroba plošných spojů fotocestou. KÁKONA, Jakub, Jan LAFATA a Milan HORKEĽ. *Modulární elektronická LABORATOR* [online]. © 2011 [cit. 2012-05-18]. Dostupné z: http://www.mlab.cz/Articles/HowTo/How_to_make_PCB/DOC/HTML/How_to_make_PCB.cs.html
- [31]: ROSA, Tomáš. *Vybrané aspekty bezpečnosti RFID: prezentace* [online]. 17.5.2010 [cit. 2012-04-30]. Dostupné z: http://secreg.utko.feec.vutbr.cz/sites/default/files/RFID_rosa_v2.pdf

SEZNAM PŘÍLOH

- Příloha 1: Schéma zapojení mikrokontroléru ATmega32.
- Příloha 2: Schéma zapojení spínaného stabilizátoru napětí.
- Příloha 3: Schéma zapojení obvodu reálného času.
- Příloha 4: Schéma zapojení sériové externí EEPROM.
- Příloha 5: Schéma zapojení konektorů na základní desce.
- Příloha 6: Schéma zapojení relé.
- Příloha 7: Schéma zapojení USB – RS232 převodníku.
- Příloha 8: Schéma zapojení slotu microSD čtečky.
- Příloha 9: Schéma zapojení šroubovacích konektorů na přídatné desce.
- Příloha 10: Schéma zapojení stabilizátoru napětí 3,3V.
- Příloha 11: Schéma zapojení konektorů pro plochý kabel na přídatné desce.
- Příloha 12: Seznam součástek + orientační cena vč. DPH k 20.3.3012.