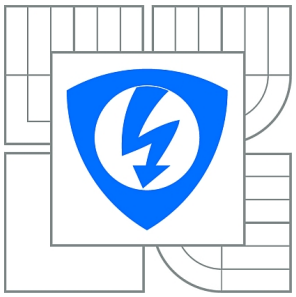
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV RADIOELEKTRONIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF RADIO ELECTRONICS

EMULÁTOR HF RFID TAGU

HF RFID TAG EMULATOR

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

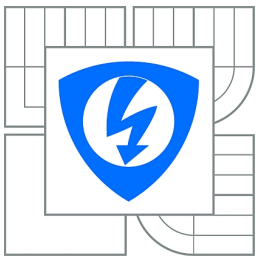
AUTOR PRÁCE — ONDŘEJ NEUŽIL

AUTHOR

VEDOUCÍ PRÁCE — Ing. JOSEF VYCHODIL

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav radioelektroniky

Bakalářská práce

bakalářský studijní obor
Elektronika a sdělovací technika

Student:	Ondřej Neužil	***ID:***	159150
Ročník:	3	***Akademický rok:***	2014/2015

NÁZEV TÉMATU:

Emulátor HF RFID tagu

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte způsoby a principy RFID komunikace v pásmu HF, například dle normy ISO 15693 nebo ISO 14443. Promyslete způsob realizace HW emulátoru RFID tagu včetně vhodné antény, analogové i digitální části, vyberte vhodný mikroprocesor. Navrhněte schéma zapojení a DPS zařízení s ohledem na celkovou velikost.

Zařízení zrealizujte a oživte. Naprogramujte firmware, který bude obstarávat základní funkce tagu. Proveďte praktickou zkoušku zařízení.

DOPORUČENÁ LITERATURA:

[1] KÜPPERS, S. RUHR UNIVERSITY BOCHUM. ChameleonMini [online]. 2014 [cit. 2014-05-09]. Dostupné z: https://github.com/emsec/ChameleonMini.

[2] ISO 15693. Identification cards - Contactless integrated circuit(s) cards - Vicinity cards. Dostupné z: http://www.openpcd.org/ISO15693.

Termín zadání:	9.2.2015	***Termín odevzdání:***	13.8.2015

Vedoucí práce: Ing. Josef Vychodil
Konzultanti bakalářské práce:

doc. Ing. Tomáš Kratochvíl, Ph.D.
Předseda oborové rady

UPOZORNĚNÍ:

Abstrakt

Tato bakalářská práce pojednává o základech technologie radiofrekvenční identifikace neboli RFID. Popisuje její princip a využití. Hlavním cílem je návrh emulátoru RFID tagu pro HF pásmo podle normy ISO 15693, který by měl simulovat bezkontaktní kartu s vazbou na dálku. Tento návrh v sobě zahrnuje výběr vhodných komponentů jako je mikroprocesor, který je jádrem celého emulátoru, výpočet vhodných rozměrů planární cívky na desku plošného spoje a software, který řídí komunikaci mezi RFID čtečkou a emulátorem.

Klíčová slova

RFID, tag, HF pásmo, mikroprocesor, emulátor, rezonanční obvod, planární cívka, deska plošného spoje, software

Abstract

This thesis contains the basic information about the Radio Frequency Identification (RFID) technology. It describes its main principles and usage. The main goal of this thesis is to design a RFID tag emulator for HF band according standard ISO 15693 that should emulate the long-range contactless smart card. The design includes the selection of the suitable components, such as a microprocessor - the core of the whole emulator, or calculation of the efficient integrated coil dimensions on a printed circuit and software for communication between the RFID reader card and the emulator.

Keywords

RFID, tag, HF zone, microprocessor, emulator, LC circuit, planar coil, PCB, software

NEUŽIL, O. Emulátor HF RFID tagu. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2015. 51 s., 2 s. příloh. Bakalářská práce. Vedoucí práce: Ing. Josef Vychodil

Prohlášení

Prohlašuji, že svoji bakalářskou práci na téma Emulátor HF RFID tagu jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

Poděkování

Chtěl bych touto cestou poděkovat vedoucímu mé práce panu Ing. Josefu Vychodilovi a především svému příteli Vojtěchu Jeřábkovi, za jejich užitečné rady a pomoc, které mi během práce poskytli.

Obsah

Seznam obrázků

Seznam tabulek

ÚVOD

RFID neboli Radio-frequency identification je automatická bezkontaktní identifikace, kde jsou informace ukládány do tzv. RFID tagů (transpondérů) využívajících elektromagnetické vlny, díky kterým tato technologie může přenášet, uchovávat a zaznamenávat informace o objektu, na němž je tento tag připevněn. RFID funguje tedy podobně jako čárový kód, ale má oproti čárovým kódům mnohem větší výhody, jako například:

- Není nutný přímý kontakt (má dosah až desítky metrů)
- Rychlost čtení
- Načítání více tagů najednou (až několik set tagů za 1 s)
- Velká odolnost

Historie RFID sahá do druhé světové války, kdy Britové využívali na podobném principu rádio-vysílače (radiomajáky) na letadlech, aby bylo možné rozeznat přátelská a nepřátelská letadla (systém IFF – Identification Friend and Foe). S myšlenkou na vznik technologie využívající bezdrátové zpracování informací přišla, však už před desítkami let, největší maloobchodní firma WallMart, a stála tak právě u zrodu čárového kódu. Základní myšlenkou bylo vyvinout takovou technologii, která by dokázala objekt identifikovat na větší vzdálenost, bez přímé viditelnosti tak, aby v reálném čase bylo možno zpracovat více produktů současně. To následně vedlo ke zvýšení přesnosti, rychlosti a efektivnosti obchodních, skladových, logistických a výrobních procesů [1]. Na začátku 70. let se začaly objevovat první patenty se vztahem k využití RFID a roku 1973 byl Mario W. Cardullovi v USA zapsán patent na aktivní RFID tag s přepisovatelnou pamětí. Ve stejném roce Charles Walton patentoval pasivní identifikátor uložený v plastové kartě, který sloužil k odemčení dveří bez klíče [2].

I přesto, že je RFID považováno za nástupce dosavadních čárových kódů, nepředpokládá se úplné nahrazení, ale spíše doplnění o další možnosti. Systém RFID je dnes používán v mnoha odvětvích průmyslu, kde je vyžadováno rychlé a přesné zpracování informací. Například: identifikace osob, identifikace zvířat (ať už jde o domácí mazlíčky nebo i velká stáda dobytku), automobilový průmysl, mobilní telefony, logistika, přístupové systémy, kontrola výrobních procesů, ve zdravotnictví a v mnoha dalších. Díky tomu se zvýší efektivita, kvalita i zabezpečení.

Technologie RFID se dnes používá téměř v každém průmyslu a i jeho využívání pro budoucnost je obrovské a možnosti téměř neomezené. Z tohoto důvodu jsem se o tuto technologii začal zajímat. Teoretická část v této bakalářské práci seznamuje s technologií RFID a s jejím běžným využitím ve světě případně s možnostmi budoucího využití. RFID tagy se běžně vyrábějí ve velkém množství na pásové výrobě řízené počítači, tím pádem jsou i jejich rozměry velmi malé. Praktická část této práce si dala za cíl navrhnout funkční emulátor RFID tagu pracující v pásmu HF a to podle standardu ISO 15693, s rozměry srovnatelnými nebo i menšími než běžná plastová platební karta pracující dle této normy.

1 SYSTÉM RFID

Základní komponenty RFID systému se dělí na tři části.

- na transpondér (tag)
- na čtečku (reader)
- řídicí software (middleware).

Každá část bude probrána podrobně.

1.1 Transpondér

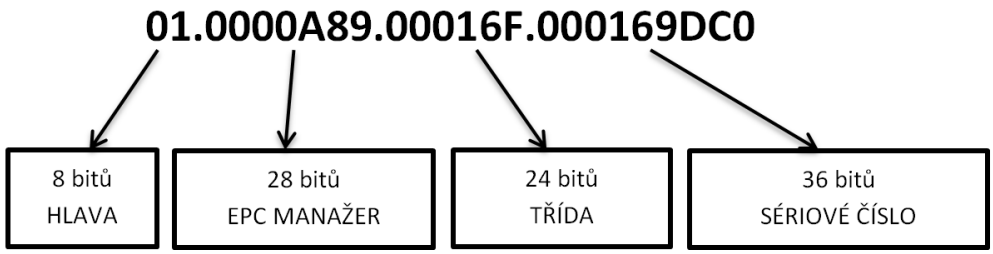
Transpondér neboli tag, je čip (elektronický paměťový obvod), jehož velikost je dnes již menší než 1 mm^2, který je umístěn na plastové nebo papírové podložce a spojen s cívkou nebo spirálovou anténou, díky které je schopen komunikovat se čtečkou. Velikost tagu přímo souvisí s velikostí antény. Podle účelu použití je možné přidat ještě další komponenty, např. různé senzory nebo dodatečné paměti. Cena tagu se tímto však zvýší, neboť je nutno přidat i zdroj energie.

1.1.1 EPC

EPC neboli Electronic Product Code, je identifikační číslo RFID tagu. Jednoznačně určuje konkrétní tag a tím pádem i konkrétní objekt, na němž je tag umístěn. Obvykle se skládá 96bitového čísla, které má hierarchickou strukturu. Ta je popsána v následující tabulce [1].

Název	Identifikace	Kapacita	Počet kombinací
Hlava	Identifikace verze EPC	8 bitů	256
EPC Manažer	Informace o firmě	28 bitů	268 milionů
Třída	Identifikace druhu výrobku	24 bitů	16 milionů
Sériové číslo	Identifikace konkrétního objektu	36 bitů	68 miliard

Tabulka 1 - Význam jednotlivých částí EPC kódu [1]



Obr. 1.1 – Struktura EPC [1]

1.1.2 Dělení podle zdroje energie

Tagy potřebují ke komunikaci se čtečkou nějakou energii. Podle způsobů, jak jim je tato energie dodávána, tagy rozdělujeme na tři základní skupiny:

Pasivní tagy

Jsou to takové tagy, které nemají žádný vlastní zdroj napájení. Jako energii potřebnou k přenosu dat, využívají část energie přijatého signálu ze čtečky, která periodicky vysílá pulsy do okolí. Tento signál nabije napájecí kondenzátor. Tag obvykle využívá metodu RTF (reader talks first), neboli tag nemůže sám vysílat informaci, dokud ho nenabije čtečka. Díky své nízké ceně, jednoduchosti a odolnosti, jsou však pasivní tagy využívány nejvíce. Dosah závisí na použité frekvenci a pohybuje se v rozmezí 0,1 – 20 m.

Aktivní tagy

Oproti pasivním tagům, mají aktivní svůj vlastní zdroj energie. Díky miniaturní baterii, jsou schopny vysílat informaci ke čtečce, aniž by se k ní museli přiblížit – často se využívá kromě RTF i metody TTF (tag talks first). Její největší výhodou je dosah. Díky vlastnímu zdroji jsou schopny vysílat až do vzdálenosti 100m. Také se k nim dají připevnit různé senzory (například kontrolovat teplotu při převozu masa) či dodatečné paměti. Velmi často se využívají v systémech pro lokalizaci v reálném čase, kde signál vyslaný z tagu je zachycen minimálně třemi anténami umístěnými kolem sledované oblasti. Nejčastěji se RTLS (Real-Time Location System) systémy používají ve venkovním prostředí na ploše distribučních center nebo rozlehlých výrobních provozech [2]. Jejich nevýhodou je samozřejmě podstatně vyšší cena, složitost, větší rozměry a menší odolnost. Životnost baterie tagu se pohybuje v rozmezí 1 – 5 let v závislosti na periodě vysílání.

Semipasivní tagy

Semipasivní či semiaktivní tagy jsou speciálním hybridem pasivních a aktivních tagů. Stejně jako aktivní tag mají také vlastní zdroj energie. Ten je ovšem využíván jen na některou z funkcí. Buď pouze zvyšuje dosah zařízení, nebo může sloužit jen k fungování senzoru, takže při získání energie ze čtečky přidá k informacím o identifikaci ještě navíc získané informace ze senzoru, apod.

1.1.3 Dělení podle frekvence

RFID systémy využívají široké spektrum frekvencí podle potřeby jejich nasazení a standardů. Volba vhodné frekvence je jedna z nejdůležitějších fází návrhu takovéhoto řešení. Různé pracovní kmitočty jsou určující pro čtecí dosah, rychlost čtení a zapisování, ale i pro citlivost na přítomnost problematických materiálů (kovy a kapaliny), které výrazně ovlivňují šíření rádiových vln.

Existují čtyři hlavní frekvenční pásma pro systémy RFID:

LF (Low Frequency) pásmo

LF tagy vysílají na nízkých frekvencích v rozsahu 125 – 134 kHz. Mají krátkou čtecí vzdálenost (do 0,5 m) a nízkou rychlost. Důležitá charakteristika tohoto pásma je, že dobře prochází skrz kovy, kapaliny, sníh, prach atd. Dobře funguje i ve velmi teplém či vlhkém prostředí nebo mlze. Další výhodou je relativně nízká cena výroby.

Využití: Docházkové karty, imobilizéry automobilů, čipování zvířat, dálkové ovladače,...

HF (High Frequency) pásmo

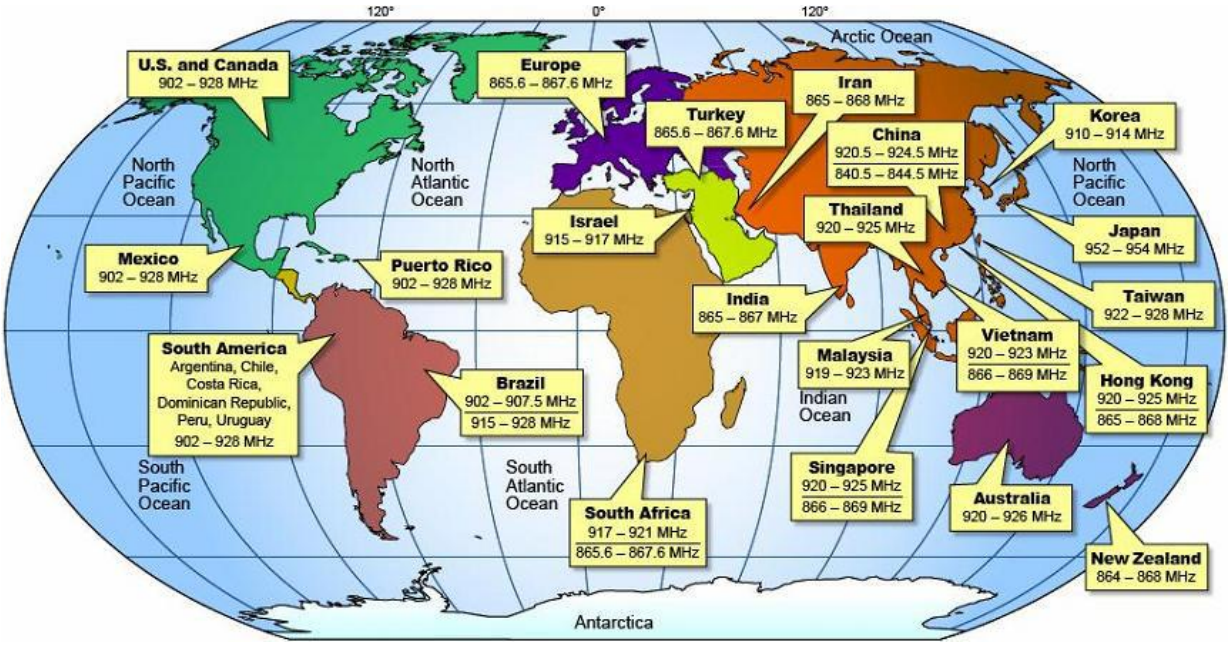
HF tagy vysílají na vysoké frekvenci 13,56 MHz, která je přijímána celosvětově. Čtecí vzdálenost je vyšší než u pásma LF (do 1,5 m) a stejně tak i přenosová rychlost. Jejich spolehlivost v prostředí s kovy či kapalinami je omezenější, ale stále relativně dobrá. HF RFID tagy jsou v dnešní době asi nejvíce využívané a proto jsou nejlevnější.

Využití: Přístupové a platební systémy (např. VUT karta), vstupenky, doprava, knihovní systémy, kontrola zboží, ...

UHF (Ultra High Frequency) pásmo

UHF tagy vysílají na ultra vysokých frekvencích v rozsahu 860 – 960 MHz. Rozsah je obrovský a mnoho světových zemí využívá jinou část tohoto rozsahu (Obr. 1.2). Čtecí vzdálenost u UHF tagů může dosahovat až několika metrů (v pasivním provedení) a mají vysokou přenosovou rychlost. Na rozdíl od pásem LF a HF nedovolují průchod kapalinou a jen velmi omezeně průchod kovy. Jsou velmi citlivé na vlhkost. V současné době jsou tagy, které využívají pásmo UHF, díky dosahu a rychlosti, nejvíce rozšiřujícími se tagy.

Využití: Průmysl, sklady (pro identifikaci zboží či palet), mýtné brány na dálnicích, identifikace vozidel…



Obr. 1.2 – Pásma UHF ve světě [5]

MW (Microwave) pásmo

MW tagy vysílají mikrovlny o celosvětově přijímané frekvenci kolem 2,45 GHz a 5,8 GHz. Jejich největší výhodou je čtecí vzdálenost, která může dosahovat za použití pasivního tagu až kolem 10 m. [24] Díky tomuto frekvenčnímu pásmu mají tyto tagy i největší přenosovou rychlost. To ovšem znamená i řadu nevýhod jako je pořizovací cena a složitost. Průchod skrz kapaliny či kovy je téměř nemožný a vzhledem k frekvenci blízké Wi-Fi, je tu i možnost kolize signálu.

Využití: Identifikace rychle se pohybujících objektů (auta), přepravní kontejnery, lokalizace, …

1.1.4 Dělení tagů podle výrobní technologie

Dělení tagů podle technologie určuje jejich budoucí využití. Podle toho je navržen tvar, přizpůsobena velikost a kladen důraz na určité vlastnosti. Např. tagy, které budou implantovány pod kůži, musí být odolné proti biologickému působení. U jiných je nutno zajistit vysokou odolnost proti vlhkosti, vysokým teplotám, působení chemikálií nebo UV záření a podobně. Z hlediska výrobní technologie tak existují desítky typů tagů, jako například:

Mince

Mají kruhový tvar, uprostřed něhož může být otvor na uchycení. Známá je forma „hodinky“, protože je připomínají tvarem. Používají se hlavně ve vlhkém prostředí (bazény, sauny,…). Obal bývá většinou tvořen plastem a díky tomu mají velkou mechanickou odolnost. Obvyklá forma je jak pasivní tak i aktivní tag. Využívají se v oblastech, kde je požadován vysoký stupeň bezpečnosti. Mají snadnou implementaci do jiných součástek.

Využití v praxi: klíčenky, imobilizéry do aut nebo znepřístupnění budov či místností.

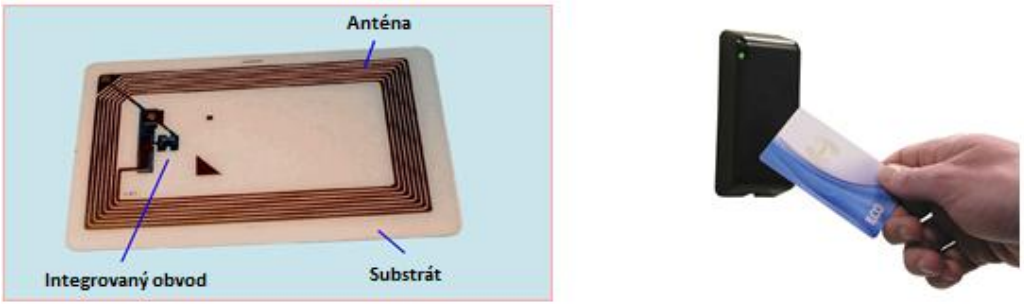
Obr. 1.3 – RFID tagy typu mince

Smart card

Smart card, neboli „chytrá karta“, má tvar klasické platební karty. Vzhledem k velikosti je v ní umístěna daleko větší anténa, díky čemuž je podstatně zvýšen dosah celého systému (0 – 1,5 m). Většina chytrých karet je vyrobena podle normy ISO 14443 nebo ISO 15693

s frekvencí 13,56 MHz. Výroba se provádí prostřednictvím laminace pasivního tagu mezi dvě vrstvy plastové folie.

Využití v praxi: Jako bezkontaktní platební karty nebo pro přístup do budov [5].



Obr. 1.4 – RFID typu Smart card

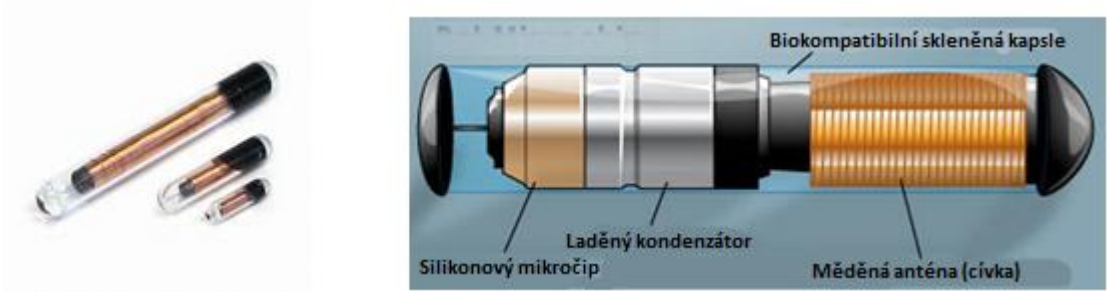
Smart label

Smart label neboli tzv. „chytrá etiketa“, je obvykle prostá papírová či plastová, tištěná etiketa s integrovaným pasivním tagem, která se jednoduše nalepí na produkt. Obvyklá kombinace je na jedné straně tag a na druhé klasický čárový kód. Ten obvykle funguje jako záložní identifikátor. Smart label je využíván nejčastěji, hlavně pro svou jednoduchost a nejnižší pořizovací cenu na trhu. Vzhledem k prosté papírové formě je však tento tag daleko náchylnější na mechanické poškození než například forma mince. Využití v praxi: v obchodech jako identifikace a ochrana před krádežemi, zatím převážně cennějších produktů, nebo k označení palet či kartónů ve skladech [5].

Obr. 1.5 – RFID typu Smart label

Skleněné tagy

Jak už napovídá název, jedná se o skleněnou trubičku dlouhou cca 10-30 mm. Uvnitř je čip, uchycený na plastovém nosiči s namotanou cívkou. Zbytek trubičky je zaplněn kapalinou pro lepší mechanickou odolnost. Tyto tagy jsou nejčastěji využívány v zemědělství pro kontrolu dobytka a jsou vhodné i pro další aplikaci v lékařství. Skleněné tagy se zavádějí zvířatům pod kůži, aby bylo možné např. v případě nemoci zvířete, kontrolovat, kolikrát dostalo léky. Anebo proto, aby se prodejem nekvalitního masa zabránilo přenosu nemoci na člověka. Tyto tagy byly vyrobeny již na začátku 80. let na žádost ministerstva zemědělství.



Obr. 1.6 – Skleněný tag

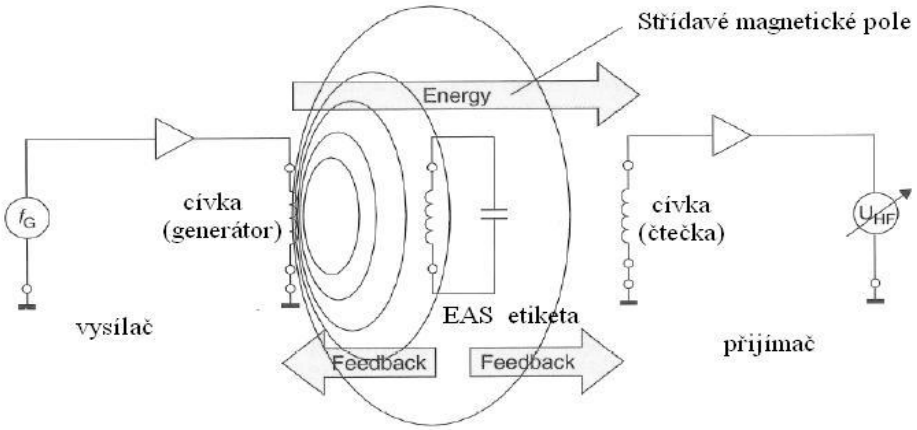
1.1.5 Dělení podle principu

Komunikace mezi čtečkou a tagem může probíhat různými způsoby. Důležité pro výběr principu přenosu informací je požadavek, kolik stavů by měl tag nabývat. Tagy mohou být buď dvoustavové tzv. jednobitové, nebo mohou mít N různých stavů tzv. N-bitové tagy. Podle toho se pak dále dělí na konkrétní princip komunikace [6].

Jednobitové (2 stavové)

Velmi často se využívají pro bezpečnostní systémy v obchodech (čtečky u pokladen). Mohou nabývat pouze dvou stavů – (zaplaceno/nezaplaceno). Výhodou je nízká cena.

a) Radiofrekvenční – Brána, kterou tvoří dvě čtečky. Jedna čtečka slouží jako generátor elektromagnetického pole. Pokud do tohoto pole vstoupí tag, který v tomto případě tvoří jen rezonanční obvod na stejné frekvenci, dojde k poklesu amplitudy, který zjistí druhá čtečka [6].

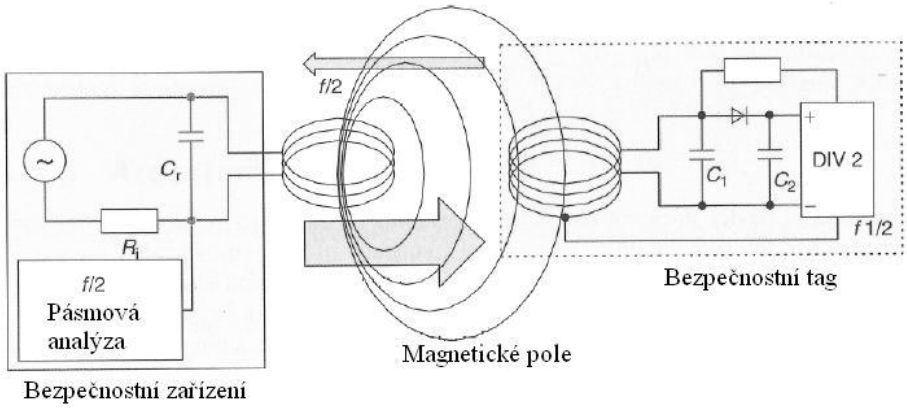


Obr. 1.7 – Princip radiofrekvenčního RFID tagu [6]

b) Mikrovlnné - Brána, kterou tvoří dvě čtečky. Jedna čtečka vysílá modulovanou nosnou vlnu. Tag tuto vlnu zachytí a pomocí varikapu vytvoří dvojnásobný kmitočet. Ten je zachytáván druhou čtečkou a identifikován [6].

Obr. 1.8 – Princip mikrovlnného RFID tagu [6]

c) Frekvenční dělič – Čtečka vytváří elektromagnetické pole (100 – 130 kHz). Tag tuto vlnu zachytí a vytvoří poloviční kmitočet Ten je opět, jako v předchozí metodě, zachytáván a identifikován [6].



Obr. 1.9 – Princip RFID tagu využívající frekvenční dělič [6]

d) Elektromagnetické – Čtečka vysílá silné elektromagnetické pole. Tag obsahuje magneticky měkký materiál, který je přemagnetováván. Díky tomu vzniknou vyšší harmonické, které jsou detekovány čtečkou [6].

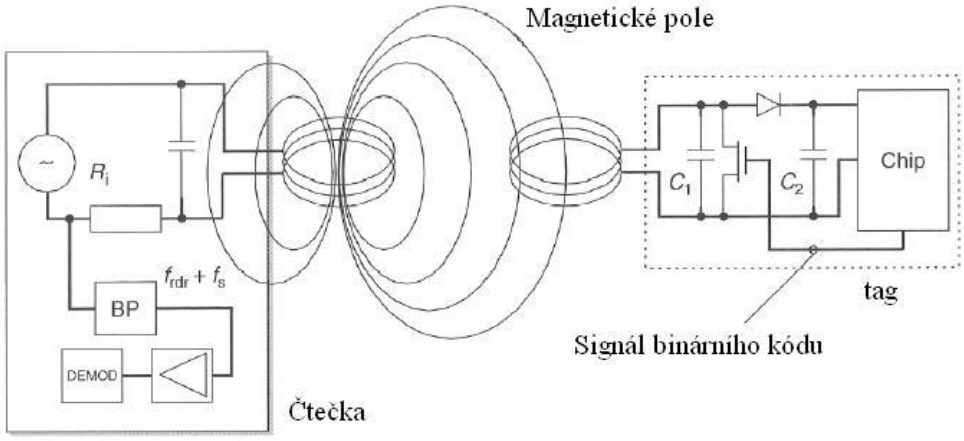
e) Akusticko-magnetické – Pracuje na principu magnetostrikce (schopnost feromagnetických materiálů měnit svoje rozměry). Tag obsahuje prvek, který je v magnetickém poli rozkmitán. Při vypnutí pole, dochází stále ke chvění prvku. Toto chvění je detekováno [6]

N-bitové

Mají N-počet různých stavů. Využívají čip – unikátní kód. Mají daleko větší rozsah využití. Jejich cena je vyšší než u tagů jednobitových.

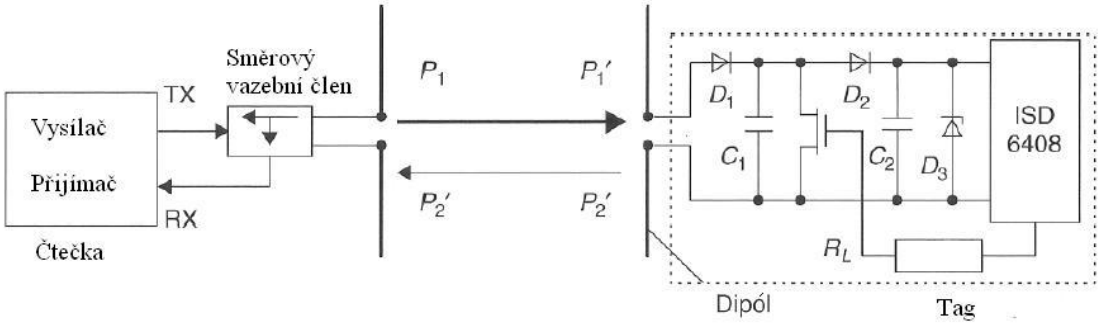
a) Induktivní vazba – Využívají ji tagy s frekvencí do 100 MHz. Základ čtečky i tagu je rezonanční obvod. Čtečka vysílá modulovanou nosnou vlnu (impulzy) o určité frekvenci (125 – 135 kHz, 13,56 MHz). Tato vlna je tagem přijata a usměrněna.

Následně je její část použita do napájecího kondenzátoru (v případě pasívního tagu), který slouží jako zdroj pro vysílání tagu. Další část vlny je zpracována čipem. Ten ze získaných informací začne ovládat řídicí tranzistor (modulátor), který mění parametry tagu a tím, se zpět do čtečky dostává kódovaná informace (ASK) [6].



Obr. 1.10 – Princip RFID tagu s induktivní vazbou [6]

b) Systémy s "backscatter" modulací = odrazová metoda – Využívají ji tagy s frekvencí nad 100 MHz. Systém využívá radiový přenos, jelikož vlnová délka je již srovnatelná s rozměry antény. Čtečka nepřetržitě vysílá spojitou modulovanou nosnou vlnu. Dále je princip stejný jak u induktivní vazby. Dle přijatého kódu mění čip impedanci antény (dochází k odrazu) a tím je vlna modulována [6].



Obr. 1.11 – Princip RFID tagu využívající odrazovou metodu [6]

1.1.6 Dělení podle interní paměti

Interní paměť je důležitou součástí tagu. Dle jednotlivých vlastností tagů a z finančního hlediska jsou využívány různé druhy pamětí. Podle použité paměti dělíme tagy do tří skupin:

Tagy RO (Read - Only)

Tagy RO jsou nejjednodušší a nejlevnější. Jak už napovídá název, tyto tagy lze pouze číst. Výrobce do nich jednou nahraje unikátní EPC číslo a dále do nich už nelze nic zapisovat (podobně jako CD-ROM). Pouze lze dalším přepisem informace v tagu znehodnotit a vyřadit tak tag z provozu (na pokladně po zaplacení zboží). Paměť těchto tagů je co do kapacity nízká. Většinou se pohybuje kolem 64 až 96 bitů. Z tohoto důvodu je ovšem jejich cena relativně nízká.

Tagy RW (Read / Write)

Na rozdíl od tagů RO, lze v RW uložená data vymazat a znovu přepsat na jiné, a to až tisíckrát. Další výhodou je veliká paměť. Ta se obvykle pohybuje kolem 256 bitů, a podle použití může být až 32kB v pasivním provedení. V aktivním může dosahovat až být až 2MB. Díky tomu stoupá cena a složitost.

Tagy WORM (Write Once / Read Many)

Tyto tagy jsou speciální kombinací předchozích dvou tagů. Narozdíl od tagů RO, jsou tyto tagy naprogramovány až u prodejce či dodavatele. Ten může na tyto tagy jednou zapsat potřebnou informaci a dále už slouží pouze ke čtení. Na trhu se lze setkat s WORM tagy, jejichž výrobce udává, že mohou být opakovaně přepsány, avšak bez záruky na spolehlivost (počet přepsání cca 100krát) [5]. Velikost paměti se pohybuje od 40 do 512 bitů.

1.2 Čtečka

Čtečka neboli reader je zařízení, které vysílá nebo přijímá elektromagnetické vlny a tím je schopna komunikovat s tagy. Obsahuje jednu nebo více antén, které mohou být integrované nebo i externí, díky kterým se zlepšuje směrovost a kvalita přenosu. Čtečka dále obsahuje řídicí jednotku, která zpracovává přijaté informace. Základním požadavkem na čtečku je schopnost zpracovat obrovské množství dat. Čtečky musí poznat již jednou přečtené tagy a detekovat (ignorovat) odrazy signálů tagů od pevných překážek (např. kovu) a musí zvládnout současně načíst velký počet tagů. S tím souvisí schopnost paralelně načítat tagy v relativně krátkém časovém intervalu [3].

RFID čtečky se dělí na dva druhy – Mobilní a stacionární.

Stacionární čtečky

Jsou pevně vestavěné v určitém identifikačním bodu. Využívají se na místech, kudy pravidelně prochází zboží, které chceme identifikovat (průchod ve skladu, počátek výrobní linky, jedoucí auta na dálnici apod.). Proto je u těchto čteček kladen nárok na rychlost zpracování a na počtu zpracovaných tagů najednou. Stacionární čtečku lze vidět na Obr. 1.12 vpravo

Mobilní čtečky

Jak už říká jejich název, mohou být přenášeny z místa na místo – fungují bezdrátově. Jsou menší a mají menší nároky na počet zpracovaných tagů i na rychlost, zato větší nároky na odolnost (fyzické poškození, vlhkost, velké teploty, prach). Získaná data jsou buď přenášena rovnou do centrální databáze prostřednictvím Wi-Fi nebo Bluetooth, nebo je čtečka připojena k PC pomocí kabelu. Mobilní čtečku lze vidět v následujícím Obr. 1.12 vlevo

Obr. 1.12 – Mobilní a stacionární RFID čtečka

1.3 Middleware

Je to softwarová vrstva, která řídí datový tok mezi hardwarem a aplikacemi informačního systému. U middleware jsou zpravidla charakterizovány čtyři základní funkce: sběr dat, směřování dat, řízení procesů, nástroj managementu. Middleware je tedy zodpovědný za přijatá data, jejich následnou filtraci a zařazení. Dalo by se říci, že v případě funkce sběru dat middleware plní úlohu jakéhosi síta, které filtruje obrovské množství dat získaného ze čteček. Tato filtrace se provádí zejména proto, že IT programy potřebují pro svoji práci pouze zlomek získaných informací [4]. Většinou to bývají informace o detekci tagu, identifikaci a čase. Vzhledem k potřebě se k nim ovšem můžou přidat i informace o baterii, informace ze senzoru, informace o stavu paměti, lokalizace apod.

1.4 Standardy

Když se systém RFID začal rozmáhat po celém světě, bylo naprosto klíčové, aby jednotlivé výrobky jednotlivých firem byly navzájem kompatibilní (aby se dovedly spolu „domluvit“). Proto byly definovány standardy ve formě norem, které zajišťují správnou funkci a kompatibilitu pro jednotlivé aplikace RFID [7]. RFID normy se většinou věnují jedné z různých oblastí. Tyto oblasti mohou být:

1. Komunikační protokol – předepisuje způsob komunikace mezi čtečkou a tagem
2. Formát dat – popisuje způsob organizace a formátování dat na tagu
3. Shoda se standardem – testuje plnění předepsaného standardu
4. Aplikace normy – upravuje, jakým způsobem jsou normy v praxi využity [2]

Název	Účel
ISO 7816	Standard pro kontaktní čipové karty
ISO 7816-1	Standard popisuje elektrické a mechanické vlastnosti karty
ISO 7816-2	Standard popisuje velikost, pořadí, umístění a funkčnost kontaktních oblastí karty
ISO 14443	Standard pro bezkontaktní karty pracující na frekvenci 13,56 MHz se čtecím rozsahem do 15 cm
ISO 15693	Standard pro bezkontaktní karty pracující na frekvenci 13,56 MHz se čtecím rozsahem od 1m do 1,5m
ISO 18000	Standard pro použití RFID v letectví
ISO 18000-1	Standard popisuje obecné parametry RFID
ISO 18000-2	Standard popisuje obecné parametry pro rozhraní <135 kHz
ISO 18000-3	Standard popisuje obecné parametry pro rozhraní 13,56 MHz
ISO 18000-4	Standard popisuje obecné parametry pro rozhraní 2,54 MHz
ISO 18000-5	Standard popisuje obecné parametry pro rozhraní 5,8 MHz
ISO 18000-6	Standard popisuje obecné parametry pro rozhraní 860 až 930 MHz
ISO 18000-7	Standard popisuje obecné parametry pro rozhraní 433 MHz (ve vývoji)
ISO 11784	Standard pro RFID identifikaci zvířat. Popisuje strukturu kódu v tagu
ISO 11785	Standard pro RFID identifikaci zvířat. Popisuje přenosový protokol

Tabulka 2 - Platné standardy pro RFID technologii [5]

Technologie RFID se stále vyvíjí. Díky tomu přicházejí i další požadavky na vznik nových mezinárodních standardů.

1.5 Využití

Využití RFID technologie je v dnešní době opravdu obrovské. V praxi je snad více omezené lidskou představivostí než možnostmi technologie. Čím více se tato technologie bude využívat, tím více bude klesat její cena a bude dostupnější i pro menší firmy. Různé druhy využití jsou popsány v následujících odstavcích.

Výroba a logistika

V logistice nacházejí RFID asi největší uplatnění. Velké množství na sebe navazujících procesů sebou nese i požadavek na kontrolu, evidenci a rychlost zpracování. Monitorování jednotlivých operací, hlášení stavu zakázek, pozice jednotlivých palet či kontejnerů, počet vyrobených a přepravených kusů, počet zmetků, třídění, značení, příjem apod. to vše v dnešní době usnadňuje systém RFID.

Dalším z faktorů, na který je kladen důraz během celého logistického řetězce a zároveň důvod pro zavedení RFID technologie jsou náklady. Snížení nákladů závisí zejména na možnosti umístit tagy na vizuálně nepřístupné místo. Ten proto není vystavován povětrnostním a jiným mechanickým vlivům. Další možností jak snížit náklady je použít transpondér opakovaně, po přehrání dat. Způsob práce s informacemi zahrnuje i eliminaci chyb způsobených lidským faktorem. Dalším důvodem častého využití je velká odolnost, obnovitelnost, a přesná evidence jednotek dodávky [4]. Čtecí zařízení lze umístit do průchodů ve skladu, slouží tedy jako brána, kterou projíždí zboží na dopravním pásu. Může být připojeno na paletě či na vysokozdvižném vozíku nebo může být využita mobilní čtečka a za jednotlivým zbožím docházet.

Obr. 1.13 - Možnosti umístění čtečky [1]

EAS systémy

EAS neboli Electronic Article Surveillance je elektronická ochrana proti krádežím [5]. Nejčastěji se využívají jednobitové RFID identifikátory (dva stavy – zaplaceno/nezaplaceno), které byly popsány v kapitole 1.1.5 Dělení dle principu. Čtecí zařízení se využívají jako brána u pokladen v obchodech, aby v případě nezaplaceného zboží mohla spustit alarm (pokud zákazník za zboží zaplatí, měl by mu být tag u pokladny ihned deaktivován). Tento systém je ovšem kvůli ceně zatím využíván spíše u dražšího zboží jako je oblečení, sportovní potřeby, drogerie, elektronika, a podobně [5].

Další využití: v knihovnách proti krádežím knih.

Zdravotnictví

Hlavním důvodem zavádění RFID do nemocničních zařízení je prevence chyb zdravotnického personálu, které by mohly být fatální. Každý pacient při příjmu dostane plastový náramek, ve kterém je tag RFID s pamětí, do něhož budou uloženy základní údaje o pacientovi, případně i jeho chorobopis. Ten bude aktualizován podle stavu pacienta. Mohou zde být zaznamenány podstoupené zákroky, podávané léky a všechny další informace o pacientově stavu. Sníží se i riziko chyb, které by mohly vznikat při přepisování

informací o pacientovi do centrální databáze. V čipu může být uložena i krevní skupina pacienta. Krevní konzervy jsou také opatřeny čipy, tudíž nemůže dojít k záměně a použití jiné krevní konzervy [3]. Dalším důvodem je uvažováno i o identifikaci předmětů (zejména chirurgických nástrojů) a omezení rizika jejich absence [8].

Docházkové, přístupové a platební systémy

Toto jsou další, velmi využívané systémy. Docházkové systémy pracují stejně jako dřívější tzv. píchačky, ovšem místo označení docházkové papírové karty, se přiloží RFID tag ke čtečce, ta ho identifikuje a zaznamená čas příchodu či odchodu. Přístupové systémy, jak už napovídá název, slouží ke zjištění oprávnění přístupu osoby do určitého místa firmy, školy apod. Budou zde zaznamenány i informace o pokusu o přístup a ukládány do centrální databáze. Nakonec platební systémy, které určitě každý zná z obchodů, dnes již jako bezkontaktní platební karty nebo jako čipy ve školních jídelnách. Tyto systémy se často spojují pro jeden tag, například Studentská karta či ISIC, využívaných na škole pro přístup či docházku a stejně tak v menzách pro platby jídla.

Budoucnost

Využití RFID je obrovské a už jsou vytvářeny i koncepty dalších technologii, které ovšem často vyžadují RFID tagy na každém produktu. Příklady takových konceptů jsou:

Inteligentní ledničky - Již existují tzv. inteligentní ledničky, které dokážou evidovat obsah pomocí optiky a čárových kódů na obalech zboží. Ovšem, vzhledem k nutnosti přímé viditelnosti a tím pádem i představitelné nespolehlivosti, nejsou moc rozšířené. Naopak lednice opatřená RFID čtečkou by dokázala během chvíle informovat o celém obsahu – „co máme a jak je to tam dlouho“, případně i co můžeme uvařit k večeři [3].

Automatické pokladny – Každý jistě zná situace v obchodech, kdy čeká v obrovské frontě, až přijde na řadu s placením. Místo toho by zákazník mohl pouze projít s nákupem skrz RFID bránu, která veškeré jeho zboží eviduje, sečte cenu a zákazník již pouze zaplatí.

Čipování lidí - obavy

Po úspěšných implantacích čipů pod kůži dobytku, přišly i návrhy na implantaci čipů pod lidskou kůži. První experiment provedl britský profesor Kevin Warwick roku 1998 [9]. Takový RFID tag by mohl sloužit jak přístupový tak i platební systém, proto by člověk sebou již nemusel nosit klíče od domu ani platební kartu a vyhnul by se tak případné ztrátě či krádeži. Na druhou stranu implantace čipu, který by mohl (kdekoliv, kde budou umístěny čtečky) odhalit naši přesnou pozici se ne každému zamlouvá. Je to považováno za omezování osobní svobody. Na obavy z této tzv. čipové totality, hodně upozorňují např. různé křesťanské kulty (Andělé světla).

2 ISO/IEC 15693

Komunikace mezi čtečkou a tagem probíhá za pomocí přesně definovaných norem. Pro tento emulátor byla zvolena norma ISO 15693 pro karty s vazbou na dálku. Všechny následující informace z této kapitoly byly vyčteny z normy ISO 15693 [22]. Přenosový protokol pro tuto normu definuje mechanismy pro výměnu instrukcí a dat mezi čtečkou a tagem v obou směrech. Celý přenosový protokol je založen na pravidle „VCD talks first“, tedy že čtečka vysílá vždy jako první. To znamená, že tag nikdy nezačne komunikaci, dokud nebude vložen do vysílacího pole čtečky a nedostane ze čtečky žádost, teprve poté může na žádost odpovědět.

V následujících podkapitolách bude popsána komunikace mezi čtečkou a tagem, za pomocí formátu:

- žádost
- odpověď

Každá „žádost“ i „odpověď“ jsou vysílány v přesně definovaných rámcích a jsou ohraničené SOF a EOF tedy tzv. Start of Frame (začátek rámce) a End of Frame (konec rámce).

2.1 UID

UID neboli Unikátní Identifikátor, je 64-bitové číslo, které obsahuje každý RFID tag, aby bylo možné tagy od sebe odlišit. Je využíván v antikolizní smyčce nebo k adresování žádosti pro konkrétní tag.

Nejvíce významný bit — Nejméně významný bit

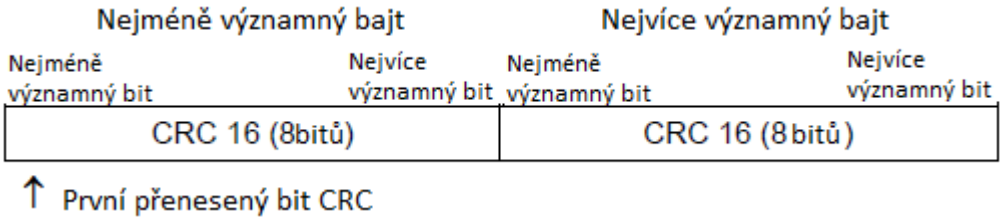
64 57	56 49	48 1
'E0'	Kód výrobce	Sériové číslo dané výrobcem

Obr. 2.1 – Unikátní identifikátor (UID) [22]

UID je tvořen hexadecimálním číslem 'E0', které je vždy na pozici nejvýznamnějšího bajtu a udává začátek UID. Dále je tvořen 8-bitovým kódem výrobce RFID tagu (např. Texas Instruments = '07') a nakonec 48-bitovým sériovým číslem.

2.2 CRC

Cyklický redundantní součet neboli CRC je speciální detekční kód využívaný pro detekci chyb vzniklých při přenosu. Dva bajty CRC jsou připojeny před EOF, ke každé žádosti nebo odpovědi přicházející v obou směrech mezi čtečkou a tagem. K výpočtu CRC se využívají veškerá data, která rámec obsahuje od konce SOF po začátek CRC. Po přijetí žádosti, tag musí nejprve ověřit, zda je hodnota CRC platná nebo ne. Pokud není, tak nesmí odpovídat (modulovat) a vyčká, až se žádost bude opakovat. Při přenosu CRC se nejprve přenáší nejméně významný bajt a to nejméně významným bitem na prvním místě. Počáteční obsah registru CRC musí obsahovat hodnotu 'FFFF'.

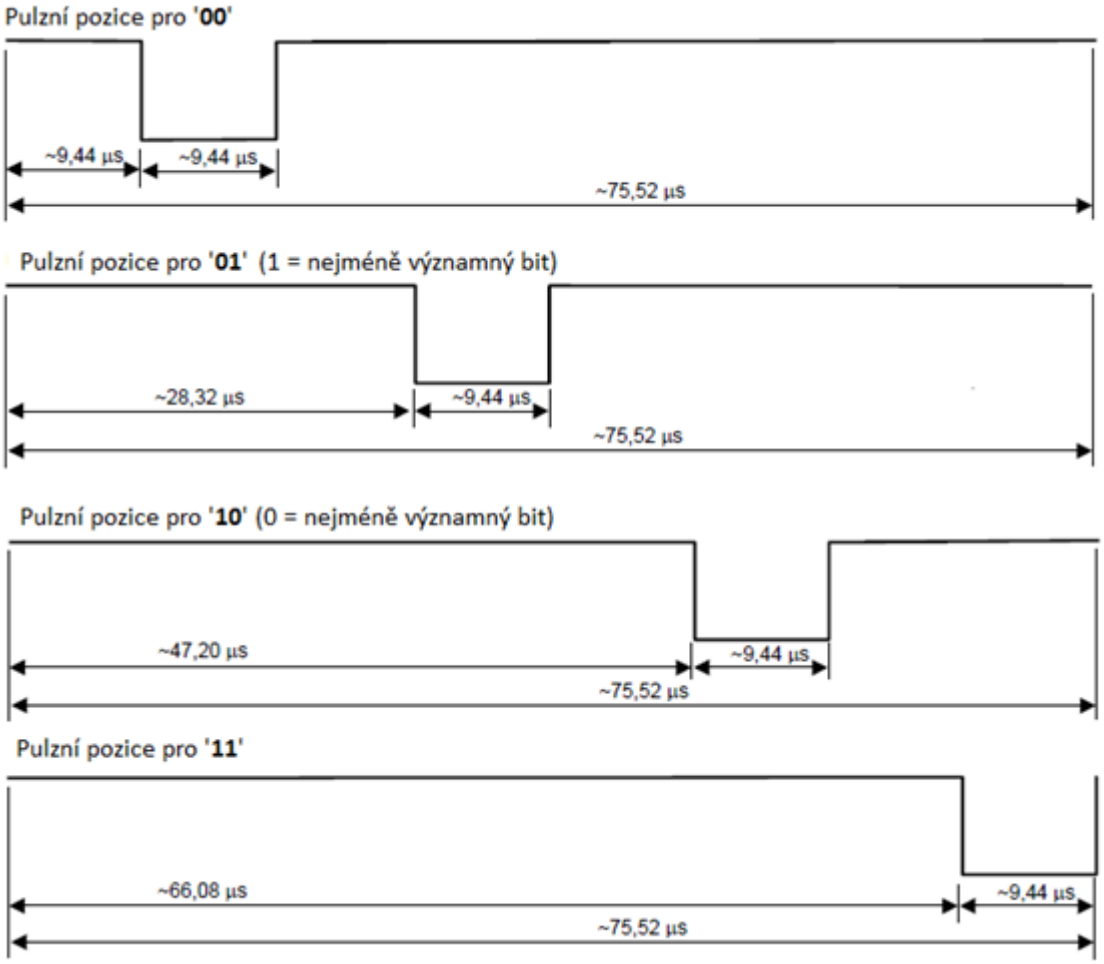


Obr. 2.2 – CRC kód [22]

2.3 Kódování žádosti a odpovědi

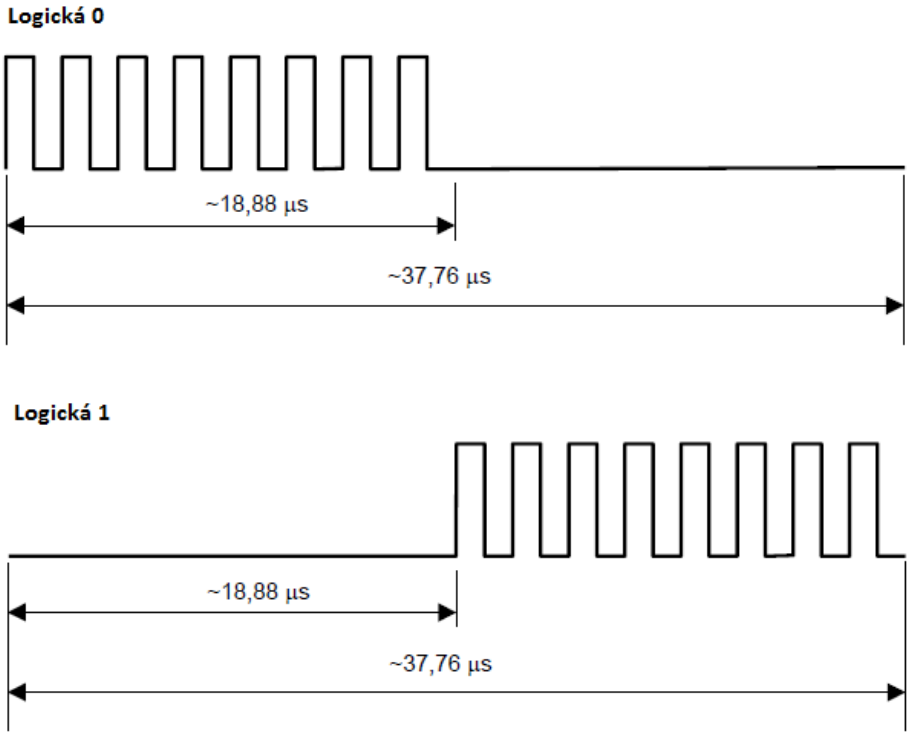
Kódování žádosti

Pro kódování žádosti se využívá pulzně poziční modulace. Žádost se může kódovat dvěma způsoby a to buď 1/4 nebo 1/ 256. Oba typy kódování by měli být podporovány každou kartou fungující dle normy ISO 15693. Typ kódování určuje SOF žádosti. Pokud SOF je kódováno například typem 1/4, bude celá zpráva kódována tímto typem. Typ kódování 1/4 spočívá v určování polohy pro dva bity najednou (Obr. 2.3). Čtyři po sobě jdoucí dvojce bitů tvoří celý bajt, při jehož přenosu se dvojce nejméně významných bitů přenáší jako první. Nejmenší časová jednotka je zde ~9,44 µs. Výsledná datová rychlost je 26,48 kbit/s.



Obr. 2.3 – Typ kódování žádosti 1/4 [22]

K odpovědi se využívá kódování Manchester podle Obr. 2.4. K vyslání odpovědi se může využívat jedna sub-nosná s modulační frekvencí 423,75 kHz, anebo, dvě sub-nosné s frekvencemi 423,75 kHz a 484,28 kHz. Kolik jich bude použito, se určuje v poli Flags. V případě použití jedné sub-nosné, logická 0 začíná nejprve 8 pulzy s celkovou dobou trvání ~18,88 µs a následované stejnou nemodulovanou dobou, ve které je signál na nízké úrovni. Logická 1 je přesně obráceně, tedy začíná nemodulovanou dobou s nízkou úrovní signálu a pokračuje 8 pulzy. Doba trvání jednoho pulzu je 1,18 µs.



Obr. 2.4 – Bitové kódování s použitím jedné sub-nosné [22]

2.4 Rámec - Žádost

Každý rámec **žádosti** musí obsahovat:

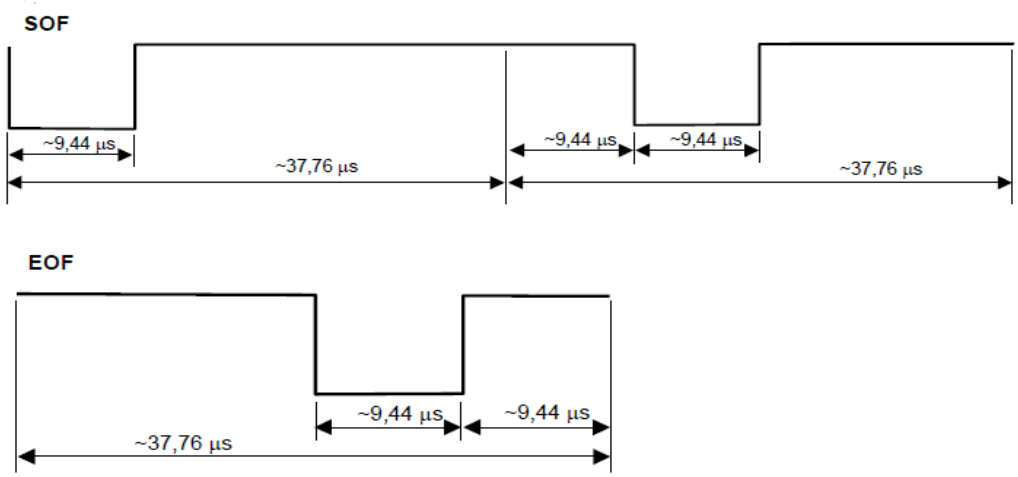
- SOF (začátek rámce)
- Flags
- Příkaz
- Povinné a nepovinné parametry pole podle příkazu + Data
- CRC
- EOF (konec rámce)

SOF	Flags	Příkaz	Parametry	Data	CRC	EOF

Obr. 2.5 – Obecný rámec žádosti [22]

2.4.1 SOF a EOF pro žádost

„Začátek rámce“ a „Konec rámce“ má přesně definovanou podobu. Ta se musí dodržovat, aby mohl tag rozpoznat, kdy přichází rámec, na který má reagovat a kdy se jedná pouze o parazitní signál, který má ignorovat. Stejně tak musí vědět, kdy rámec skončil. Tag musí být schopný přijmout rámec začínající SOF nejpozději 1ms po vložení tagu do pole čtečky. Na Obr. 2.6 lze vidět SOF a EOF pro kódování 1/4, které je v práci použito. Druhá možnost kódování je 1/256, která ovšem využita nebyla, kvůli její příliš dlouhé době trvání a zpracování.



Obr. 2.6 – Formát SOF a EOF [22]

2.4.2 Flags pro žádost

Pole „Flags“ je nastavení daného rámce. Určuje, které akce mají být kartou provedeny. Je tvořeno 8 bity, přičemž každý bit určuje nastavení a parametry komunikace.

Číslo bitu	Nastavení	Stav	Popis
1 bit	Sub-nosná	0	Jedna sub-nosná využívané tagem
		1	Dvě sub-nosné využívané tagem
2 bit	Datová rychlost	0	Nízká datová rychlost
		1	Vysoká datová rychlost
3 bit	Inventory	0	Parametry 5-8 podle tabulky 3
		1	Parametry 5-8 podle tabulky 4
4 bit	Protokol rozšíření	0	Bez rozšířeného protokolu
		1	Rozšíření protokolu (budoucnost)

Tabulka 3 – Nastavení žádosti 1 – 4bitu [22]

Číslo bitu	Nastavení	Stav	Popis
5 bit	Vybraný tag	0	Žádost je provedena každým tagem
		1	Žádost je provedena pouze vybraným tagem
6 bit	Adresování	0	Žádost neobsahuje UID určitého tagu
		1	Žádost obsahuje UID určitého tagu
7 bit	Volba	0	Není-li speciálně definováno příkazem
		1	Je-li speciálně definováno příkazem
8 bit	Pro budoucnost	0	Rezervováno pro budoucnost

Tabulka 4 – Nastavení žádosti 5 – 8bitu pokud je bit Inventory nastaven na ‘0‘ [22]

Číslo bitu	Nastavení	Stav	Popis
5 bit	Určení přednosti	0	Určení přednost není použito
		1	Určení přednost je použito
6 bit	Počet slotů	0	16 slotů
		1	1 slot
7 bit	Volba	0	Není-li speciálně definováno příkazem
		1	Je-li speciálně definováno příkazem
8 bit	Pro budoucnost	0	Rezervováno pro budoucnost

Tabulka 5 - Nastavení žádosti 5 – 8bitu pokud je bit Inventory je nastaven na ‘1‘ [22]

2.4.3 Příkaz pro žádost

Norma ISO 15693 definuje čtyři typy příkazů, které musí, či může karta pracující podle této normy umět. Jsou to příkazy:

1. **Povinné** ('01'až '1F') – musí je podporovat všechny karty podle normy ISO 15693
2. **Volitelné** ('20' až '9F') – nadstandartní, ale normou definované příkazy. Karty je nemusí podporovat
3. **Osobní** ('A0' až 'DF') – jsou to speciální příkazy definované výrobcem karet
4. **Uzavřené** ('E0' až 'FF') – speciální příkazy využívané výrobcem k testování

Kód příkazu	Typ	Příkaz
'01'	Povinné	Inventory
'02'	Povinné	Stay Quiet
'03' - '1F'	Povinné	Rezervováno pro budoucnost
'20'	Volitelné	Přečti jeden blok
'21'	Volitelné	Zapiš jeden blok
'22'	Volitelné	Uzamči blok
'23'	Volitelné	Přečti vícenásobný blok
'24'	Volitelné	Zapiš vícenásobný blok
'25'	Volitelné	Výběr tagu
…	…	…
'2D' - '9F'	Volitelné	Rezervováno pro budoucnost
'A0' - 'DF'	Osobní	Speciální příkaz výrobce
'E0' - 'FF'	Uzavřené	Speciální příkaz výrobce

Tabulka 6 – Tabulka příkazů [22]

Inventory ('01')

Je to základní a nejdůležitější povinný příkaz. Je to v podstatě příkaz „identifikuj se“. Čtečka ho po určité periodě opakovaně vysílá a čeká na odpověď. Karta, která tento rámec s tímto příkazem zachytí, pošle svůj UID, čímž se identifikuje.

SOF	Flags	Inventory	Přednost	Délka masky	Hodnota masky	CRC	EOF
	8 bitů	8 bitů	8 bitů	8 bitů	0 – 64 bitů	16 bitů	

Obr. 2.7 – Rámec příkazu Inventory [22]

Pouze v případě příkazu Inventory, je v poli Flags nastaven třetí bit na hodnotu 1, takže pro bity 5-8 se dále využívá tabulka 4. V případě, že je šestý bit nastaven na hodnotu 0, bude po přijetí příkazu tagem spuštěna antikolizní sekvence. V jiném případě je Délka masky nastavena na '00' a Hodnota masky neobsahuje žádný bit.

Stay Quiet ('02')

Tento příkaz je další z povinných příkazů pro každou kartu využívající vazbu na dálku. Pokud zná čtečka UID konkrétní karty, může vysílat adresované příkazy určené pouze pro danou kartu. Karta zachytí rámec, který obsahuje kromě příkazu a Flags i požadovaný UID,

to porovná se svým UID. Jestli souhlasí, karta vykoná daný příkaz (přejde do stavu Quiet). Pokud UID nesouhlasí, karta příkaz ignoruje. Pokud karta přejde do stavu Quiet, neodpovídá na příkazy typu Inventory, ale odpovídá už pouze na příkazy adresované.

SOF	Flags	Stay quiet	UID	CRC	EOF
	8 bitů	8 bitů	64 bitů	16 bitů	

Obr. 2.8 – Rámec příkazu Stay Quiet [22]

Další povinné příkazy s kódem '03' - '1F', jsou ponechány pro budoucí využití. Všechny ostatní příkazy jsou již pouze volitelné a formu jejich rámců lze najít v normě. Většina z nich využívá adresování pro konkrétní kartu. Rámce odpovědí budou popsány a zobrazeny v další kapitole.

2.5 Rámec – Odpověď

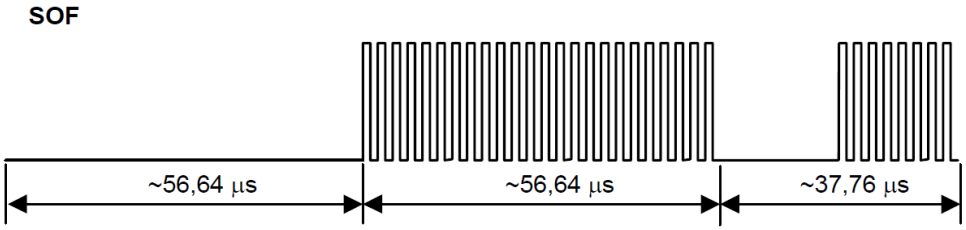
Každý rámec **odpovědi** musí obsahovat:

- SOF
- Flags
- Povinné a nepovinné parametry pole podle příkazu
- Data
- CRC
- EOF

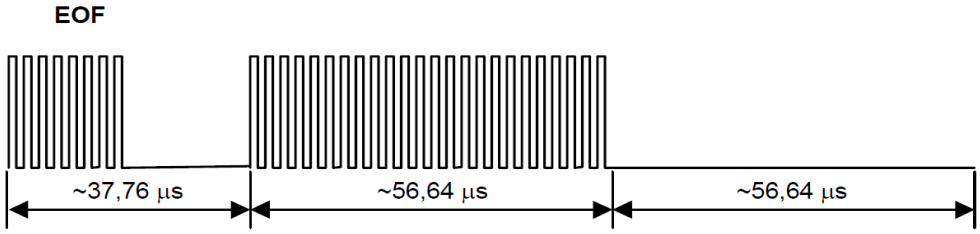
SOF	Flags	Parametry	Data	CRC	EOF

Obr. 2.9 – Obecný rámec odpovědi [22]

2.5.1 SOF a EOF pro odpověď



Obr. 2.10 – SOF s užitím jedné sub-nosné [22]



Obr. 2.11 – EOF s užitím jedné sub-nosné [22]

SOF i EOF s užitím jedné sub-nosné pro odpověď se skládá ze tří částí rozložených podle Obr. 2.10 a Obr. 2.11:

- nemodulovaný čas, ve kterém je signál na nízké úrovni (~56,64 µs)
- 24 rychlých pulzů (~56,64 µs)
- v případě SOF logická 1 (~37,76 µs), v případě EOF logická 0 (~37,76 µs)

2.5.2 Flags pro odpověď

Pole „Flags“ v odpovědi, obsahuje, jaké akce byly kartou provedeny. Nejdůležitější je prozatím pouze bit 1, který indikuje, zda nastala nebo nenastala chyba. Ostatní bity jsou rezervovány pro budoucí využití.

Číslo bitu	Nastavení	Stav	Popis
1	Chyba	0	Bez chyby
		1	Byla zjištěna chyba
2	Pro budoucnost		Nastaveno na 0
3	Pro budoucnost		Nastaveno na 0
4	Protokol rozšíření	0	Bez rozšířeného protokolu
		1	Rozšíření protokolu (budoucnost)
5	Pro budoucnost		Nastaveno na 0
6	Pro budoucnost		Nastaveno na 0
7	Pro budoucnost		Nastaveno na 0
8	Pro budoucnost		Nastaveno na 0

Tabulka 7 – Pole „Flags“ pro odpověď [22]

V případě, že by během přenosu nebo při příjmu nastala chyba, musí karta poslat zpět rámec, ve kterém popisuje, o jakou chybu se jedná. Pokud karta danou chybu nezná, vypíše kód chyby '0F' (neznámá chyba).

Kód chyby	Popis
'01'	Příkaz není podporován tzv. neznámý příkaz
'02'	Příkaz není rozpoznán, například: došlo k chybě formátu
'03'	Volba není podporována
'0F'	Neznámý příkaz
…	…
'11'	Specifikovaný blok je již uzamčen, nelze byt uzamčen znovu
'12'	Specifikovaný blok je uzamčen a nelze již měnit
'A0' - 'DF'	Osobní chybová hlášení (definováno výrobcem)
všechny ostatní	Rezervováno pro budoucnost

Tabulka 8 – Kódy a popis chyb, které mohou při přenosu nastat [22]

2.5.3 Odpověď na Žádost

Na každý příkaz poslaný v rámci žádosti může existovat specifický typ rámce odpovědi. Základem je odpověď na rámec s příkazem Inventory.

SOF	Flags	DSFID	UID	CRC16	EOF
	8 bits	8 bits	64 bits	16 bits	

Obr. 2.12 – Odpověď na příkaz Inventory [22]

Pokud nenastane žádná chyba, kterou by signalizoval 1bit v poli Flags, vyšle karta zpět rámec strukturovaný podle Obr. 2.12. Pole UID představuje vyslaná Data a pole DSFID představuje parametr rámce odpovědi a popisuje, jak jsou data v paměti tagu strukturována. Pole DSFID se používá spíše pro složitější karty, které podporují více než jen základní příkazy. Pokud karta pole DSFID nepodporuje, zapíše se v tomto poli jen '00'. Na další povinný příkaz „Stay Quiet“, pokud nenastala chyba, tag neodpovídá.

3 KONSTRUKCE EMULÁTORU

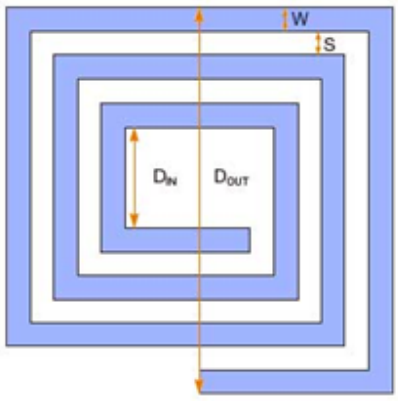
Tato část se zabývá návrhem a konstrukcí emulátoru RFID tagu pracující v pásmu HF. Emulátor je zařízení, které je schopné simulovat RFID tag. Konstrukce emulátoru se dělí na čtyři podkapitoly. Jsou to:

- Návrh antény
- Návrh analogové části
- Výběr mikroprocesoru
- Konstrukce

3.1 Návrh antény

Pro RFID tagy využívající HF pásmo se ke komunikaci mezi čtečkou a tagem využívá místo antény, která by pro HF musela být 22,12 m dlouhá, což není realizovatelné, paralelní rezonanční obvod naladěný na frekvenci 13,56 MHz, tvořený planární cívkou, kondenzátorem a rezistorem. Bylo nutné nejprve spočítat rozměry planární cívky a k tomu podle známého kmitočtu dopočítat, pomocí Thompsnova vzorce příslušnou kapacitu kondenzátoru.

Pro výpočet rozměrů a hodnot planárních cívek se nejčastěji využívají tři metody. První je tzv. Wheelerova modifikovaná metoda, druhá metoda je odvozena z elektromagnetických principů a třetí metoda je odvozená z jednočlenného vyjádření hodnoty z veliké databáze cívek [20]. Všechny tři metody jsou přesné s typickými chybami kolem 2-3% a jsou velmi jednoduché, proto se k návrhu planární cívky hodí nejvíce. Tloušťka má na indukčnost jen velmi malý vliv, proto je u všech metoda zanedbána. Rozměry cívky byly zvoleny:



Počet závitů (N)	13
Šířka spoje (W)	0,42 mm
Šířka mezery mezi spoji (S)	0,42 mm
Vnější délka cívky (D_{OUT})	42 mm
Vnitřní délka cívky (D_{IN})	21 mm

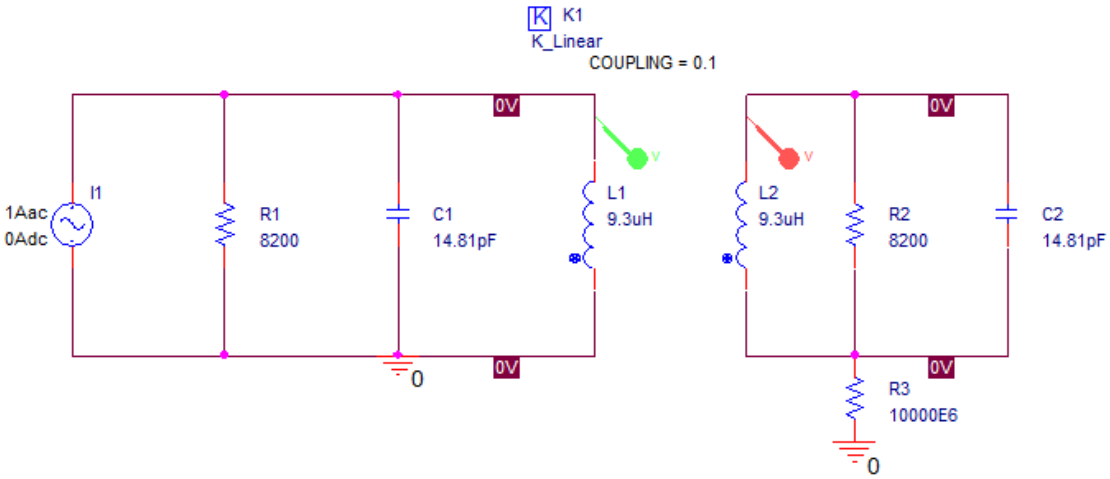
Obr. 3.1 – Planární čtvercová cívka a tabulka zvolených hodnot [20]

Podle zvolených hodnot a využití všech tří výpočetních metod, vyšla průměrná hodnota indukčnosti 8,25 µH. Pro výpočet těchto hodnot byla použita internetová kalkulace [20]. K této hodnotě indukčnosti se pomocí Thompsnova vzorce (1.1) dále dopočítala i potřebná kapacita rezonančního obvodu, která vyšla C=16,69 pF.

$$f_0 = \frac{1}{2\pi \times \sqrt{LC}} \qquad (1.1)$$

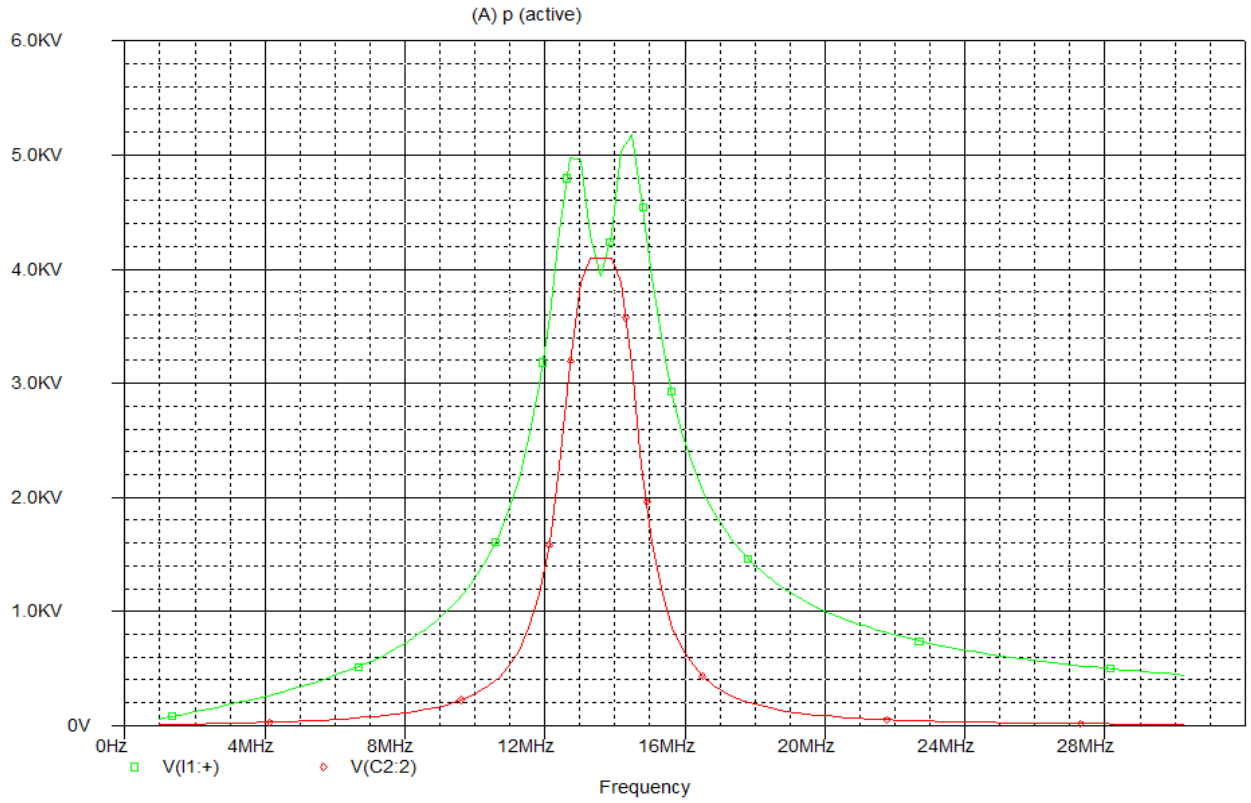
Předem se ovšem předpokládalo s výrobními odchylkami a tedy jistou nepřesností v konečném výsledku, a také proto byl zde navržen místo kondenzátoru s pevnou hodnotou kapacity, kapacitní trimr s proměnnou hodnotou 3-50 pF. Po vyrobení cívky byla její hodnota indukce přibližně 9,3 uH a její odpor R=2Ω. Potřebná nastavená kapacita v tom případě byla 14,81 pF [10].

S těmito hodnotami rezonančního obvodu byla provedena simulace, u které se zkoumala přenosová charakteristika signálu na 13,56 MHz. Tato simulace byla nutná především k vyřešení dvou existujících problémů. Za prvé byla potřeba, krom dostatečné přenosové charakteristiky, i dostatečná šířka pásma signálu, aby byla dobře zachytitelná i odpověď z emulátoru, pracující na sub-nosné s frekvencí ±423,75 kHz. Emulátor pro jednoduchost využívá pouze jednu sub-nosnou, jejíž úroveň signálu by neměla mít větší pokles než 3dB. Tato šířka pásma se nastavovala rezistorem, který také spolu s cívkou a kondenzátorem tvořil paralelní rezonanční obvod. K simulaci byl využit obvod zobrazený na Obr. 3.2, který představuje vazbu dvou rezonančních obvodů, které jsou, pro jednoduchost identické [21].



Obr. 3.2 - Vzájemná vazba dvou paralelních rezonančních obvodů

Druhý problém je ve vznikajícím nežádoucím efektu. Pokud pomocí R2 zvyšujeme maximální přenos signálu pro tag a zužujeme šířku pásma, vzniká mezi čtečkou a emulátorem těsná vazba (nadkritická), který místo jedné špičky maximálního přenosu na naladěné frekvenci 13,56 MHz vytváří dvě, které se od sebe oddalují a u požadované frekvence, která se nachází mezi nimi, nastává pokles. Čím víc se tedy zvyšuje úroveň maximálního přenosu pro tag na frekvenci nosné, tím více klesá hodnota přenosu pro čtečku [21]. Proto byla zvolena optimální hodnota rezistoru 8.2 kΩ, kde maximální přenos nosné ze čtečky je přibližně na stejné úrovni jako maximální přenos nosné tagu, jak lze vidět na Obr. 3.3 a úrovně sub-nosných na frekvencích 13,136 MHz a 13,983 MHz nebudou mít pokles větší než 3dB.

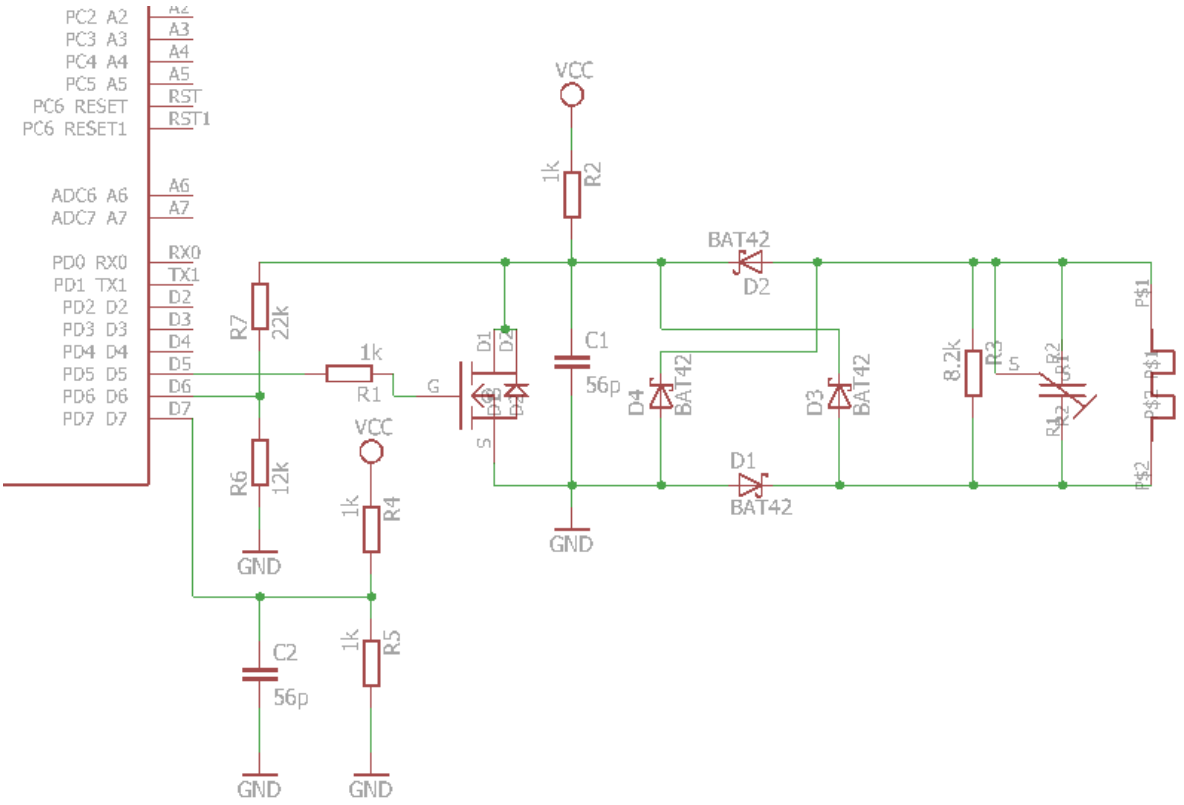


Obr. 3.3 – Přenosová charakteristika paralelních rezonančních obvodů čtečky a tagu

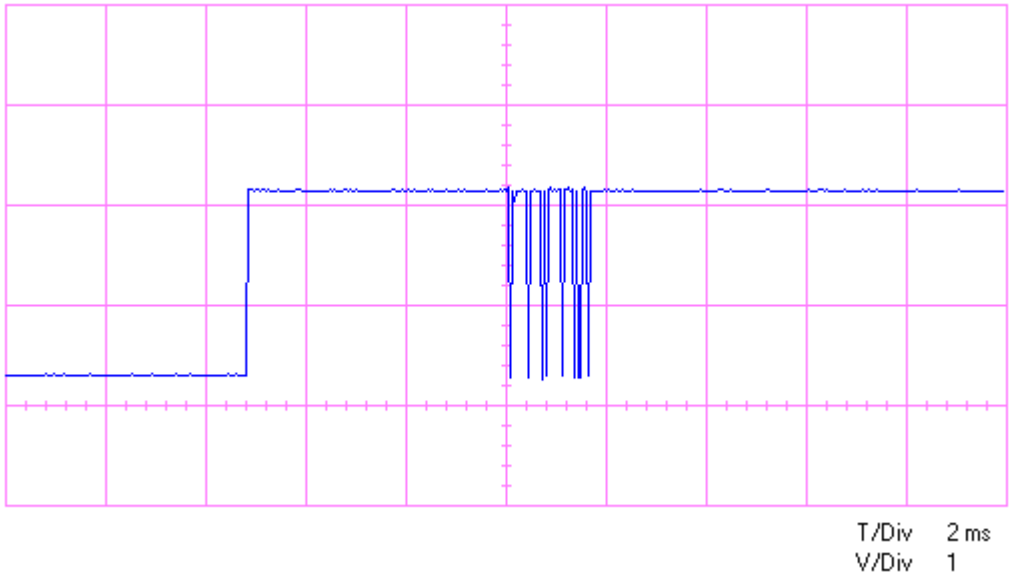
3.2 Návrh analogové části

Po přijetí modulovaného signálu pomocí rezonančního obvodu je potřeba tento signál nejprve dvojcestně usměrnit a následně demodulovat. Demodulovaný signál poté vstupuje do komparátoru, kde je porovnáváno, zda je na vysoké nebo nízké úrovni a zjišťováno zda jde o datový rámec vyslaný ze čtečky, anebo o parazitně naindukovaný signál.

Magnetické pole indukované čtecím zařízením musí nabývat hodnot od 150 mA/m do 5 A/m. Při nízké hodnotě bude transpondér málo vybuzen a naopak při vysoké hodnotě hrozí riziko zničení čipu [10]. Na Obr. 3.4 je zobrazena analogová část emulátoru. Jako dvoucestný usměrňovač je zde použit Graetzův můstek tvořený čtyřmi Schottkyho diodami typu BAT42, který usměrňuje střídavý signál z rezonančního obvodu. Schottkyho diody BAT42 jsou využity kvůli případné ochraně proti přepětí a taky z důvodu vysoké frekvence. U obyčejných usměrňovacích diod by při frekvenci 13,56 MHz, vznikl nežádoucí jev, kdy se po změně vstupního napětí do záporné půlvlny oblast PN přechodu nestihne dostatečně rychle vyprázdnit a ještě nějakou chvíli vede proud i v závěrném směru [12]. Za graetzovým můstkem je využit kondenzátor C1, který slouží jako filtr a zároveň, spolu s rezistorem R2 zapojeným za Vcc slouží jako demodulátor, který nám z krátkého sledu vysokofrekvenčních pulzů vytvoří obdélníky s vysokou úrovní. Napájení Vcc zde slouží jako tzv. Pull-up, který v případě, že nepřichází žádný signál, udržuje vstup PD6 trvale na vysoké úrovni. Demodulovaný signál je přiveden přes napěťový dělič na komparátor v čipu (PD6) a je porovnáván s referenční hodnotou vstupu PD7. Podle toho zda je příchozí signál větší nebo menší než referenční, se určuje, zda přišla hodnota 1 nebo 0. Kondenzátor C2 je zde pro případ parazitního vysokofrekvenčního rušení.

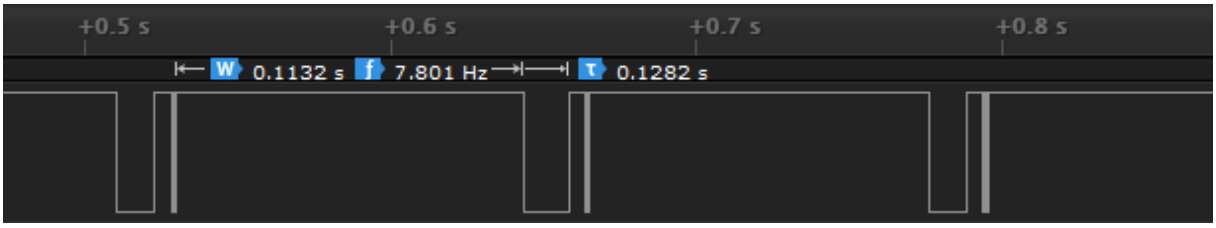


Obr. 3.4 – Analogová část emulátoru



Obr. 3.5 – Žádosti Inventory přijímané emulátorem

Žádost Inventory se neustále opakuje s nastavitelnou periodou. Příjem žádosti Inventory měřený emulátorem lze vidět na Obr. 3.5. Čtečka nejprve po dobu přibližně 13 ms nachází ve stavu logické nuly, poté následuje náběžná hrana, která je po čase 5,19 ms přerušena SOF tedy začátkem rámce žádosti ze čtečky. Po skončení celého rámce by do maximální doby 300µs měl tag začít odpovídat.



Obr. 3.6 – Žádosti Inventory přijímané emulátorem s měřítkem 0,1s (analyzátor)

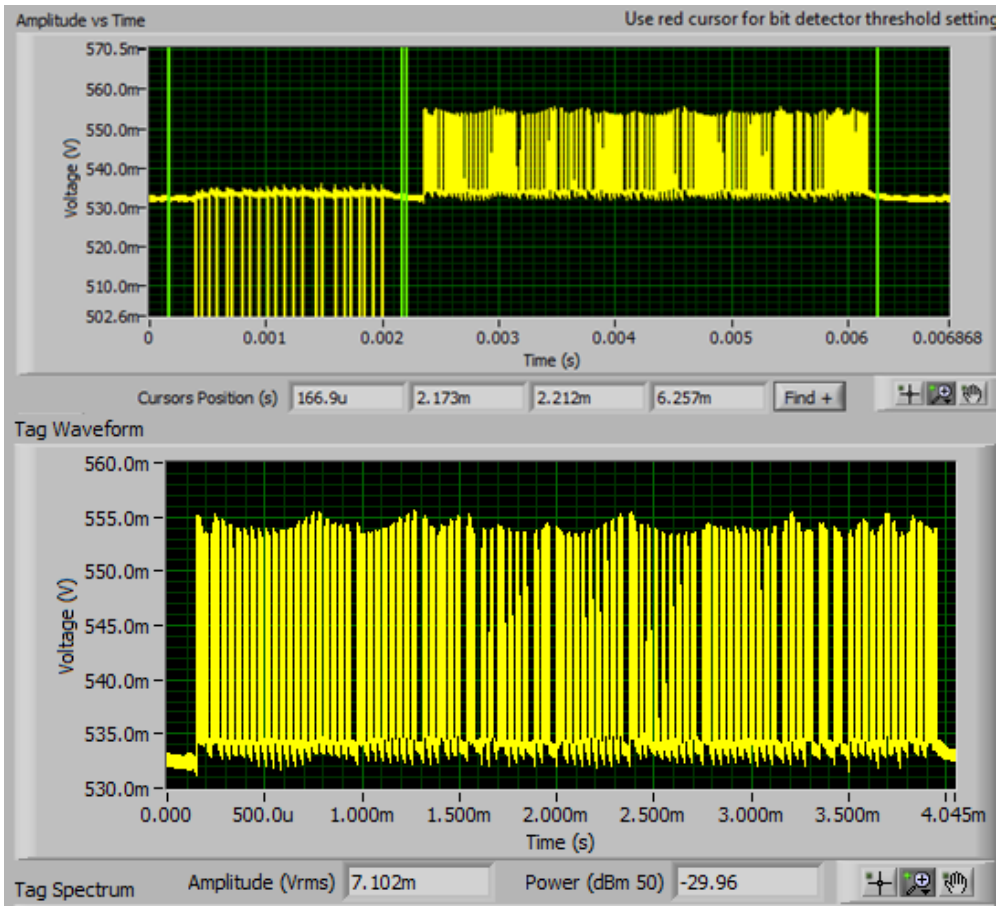
Obr. 3.7 – Žádost Inventory přijímané emulátorem s měřítkem 0,1ms (analyzátor)

Na Obr. 3.6 a Obr. 3.7 je zobrazena žádost Inventory měřená logickým analyzátorem SaleaeLogic 24MHz a s použitím programu Saleae Logic. Tento program umožňuje detailní nahlédnutí do měřeného průběhu a lze snadno zkontrolovat přijímaná a vysílaná data včetně délky konkrétních pulzů a mezer mezi nimi. Při práci byla použita stolní čtečka RFID karet ID CPR30-USB od firmy FEIG electronic (Obr. 3.12). Bylo možné zjistit, že vysílaná zpráva z čtečky používá kódování ¼ a má tyto parametry:

- Flags – ‘26‘
- Příkaz – ‘01‘ (Inventory)
- Maska – ‘00‘
- CRC16 – ‘F60A‘

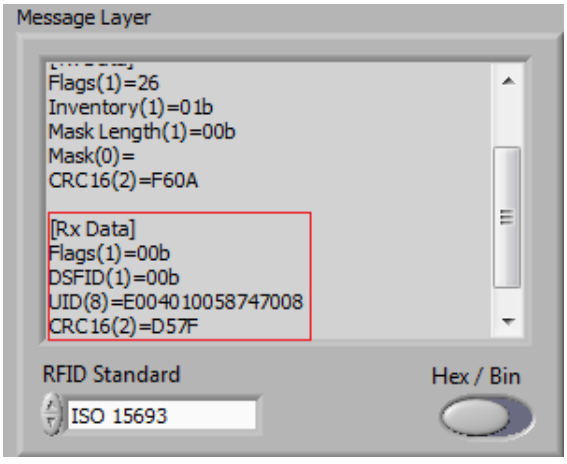
Pokud by se dalo předpokládat, že CRC16 vždy dojde ve správném tvaru, je možné brát tyto parametry jako ty, na které má emulátor odpovídat svým UID. Ostatní žádosti ze čtečky jsou již volitelné výrobcem, a tudíž nejsou nutně podporovány všemi čtečkami pracujícími podle normy ISO 15693.

Tranzistor Q3 je v emulátoru použit jako modulátor. Podle řídicího napětí z čipu (PD5) se otevírá a zavírá, čímž mění zatížení rezonančního obvodu, což zaregistruje čtečka, do které se tím pádem dostává amplitudově kódovaná (ASK) informace. Spínací vlastnosti klasického bipolárního tranzistoru, řízeného asymetrickým vstupním napětím se ukázaly být nedostatečné pro frekvenci pomocné nosné 423,75 kHz [3], a právě proto byl použit unipolární tranzistor IRFD110. Tento typ se obecně využívá u prací s RFID emulátory nejvíce. Maximální odpor tranzistoru v sepnutém stavu je $R_{DS(on)}$=0,54Ω, což zajišťuje jeho zanedbatelný ztrátový výkon. Při U_{GS} = 5V, může tranzistorem protékat proud o velikosti až I_c = 1A [13].

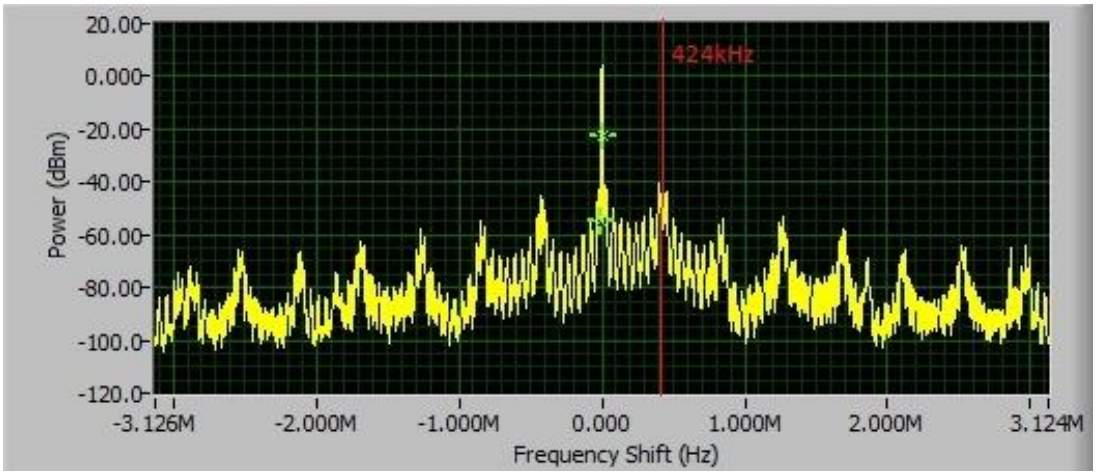


Obr. 3.8 – Modulovaná odpověď z emulátoru

Na Obr. 3.8 je zobrazena modulovaná odpověď obsahující UID emulátoru reagujícího na příchozí žádost ze čtečky, změřená a zobrazená pomocí programu LabView. Z obrázku lze vidět, že ačkoli přímo na pinu D5 bylo naměřeno cca 3V, tak ve výsledku je modulovaná zpráva velmi slabá cca 25mV. Přesto bylo možné dekódovat tuto zprávu (Obr. 3.9) pomocí programu LabView a potvrdit správnost vysílané zprávy. Co se týče časových přesností, na Obr. 3.10 lze vidět, že odchylka od požadovaných 423,75kHz je méně než 0,06%.

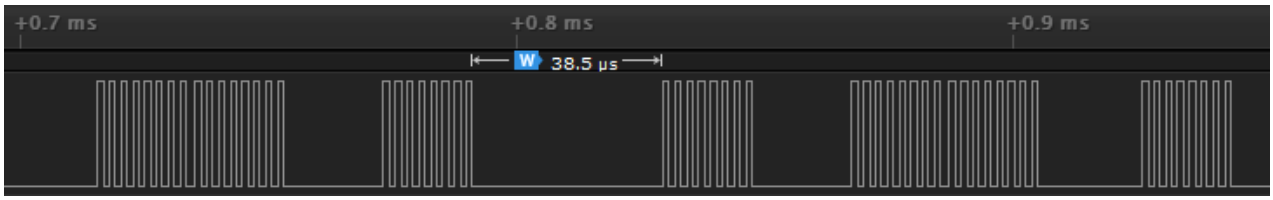


Obr. 3.9 – Dekódovaná odpověď z emulátoru



Obr. 3.10 – Spektrum signálu – odpověď z emulátoru

Detailní zobrazení modulované odpovědi emulátoru měřené logickým analyzátorem, lze pozorovat na Obr. 3.11. Jak bylo popsáno v kapitole 2.3 je u odpovědi použito kódování Manchester, kde se logická 1 a 0 skládá z rychlých pulzů, jejichž délka trvání je 1,18µs. Tímto způsobem je zakódována celá zpráva obsahující Flags, DSFID, UID, CRC16 a samozřejmě SOF a EOF udávající začátek a konec odpovědi.



Obr. 3.11 – Odpověď emulátoru na příchozí Inventory žádost

Obr. 3.12 – RFID čtečka ID CPR30-USB[25]

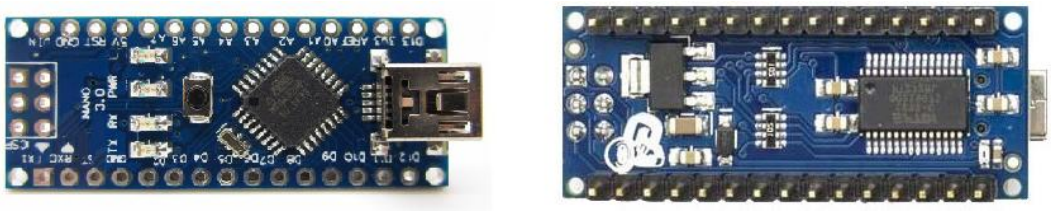
3.3 Výběr mikroprocesoru

Vybraný mikroprocesor byl zvolen z důvodu využívání platformy Arduino, což je Open-Source platforma pro snadný návrh a vývoj elektronických programovatelných zařízení. Konkrétně využívané Arduino Nano je minimalizovaná vývojová deska s mikroprocesorem

AVR ATmega328P. Má 14 digitálních vstupně-výstupních pinů (z toho 6 s podporou PWM) a 8 analogových vstupů [15]. Využívá krystalový oscilátor 16 MHz. Dále se na desce nachází komparátor, který je využíván k porovnání demodulovaného signálu vstupujícího do mikroprocesoru s referenčním signálem. K programování využívá ISP rozhraní na propojení s počítačem přes programátor STK500. Napájení probíhá přes mini USB kabel.

Co se týče mikroprocesoru ATMega328P, je to osmi bitový procesor obsahující 32k-bitovou programovatelnou FLASH paměť. Má dva 8-bitové a jeden 16-bitový čítač [16]. Je schopný pracovat s hodinovým signálem až 20 MHz.

Celý modul Arduino Nano byl zvolen hlavně kvůli jeho malým rozměrům, dobré pověsti, velké komunitě uživatelů, jednoduchosti zapojení a programování, nízké ceně a dobré podpoře ze strany výrobce.



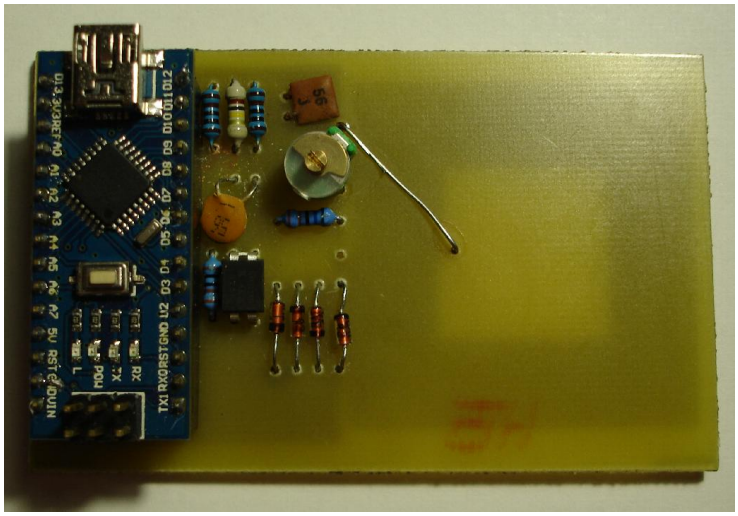
Obr. 3.13 – Platforma Arduino Nano – přední a zadní strana [23]

3.4 Výroba

Pro tvorbu schématu a planární cívky byl využit program Eagle verze 7.2.0, což je jednoduchý a zdarma dostupný software na návrh desek plošných spojů. V tomto programu bylo navrženo schéma i osazení desky. Tyto návrh byly vyexportovány ve formátu, podle kterého byla deska plošných spojů již chemickým způsobem vyrobena. Deska byla následně vyvrtána a osazena. Nakonec se k ní byl zapojen modul Arduino Nano, který se přes ISP rozhraní mohl programovat. Hotová deska má rozměry 82 x 50 mm, což je přibližně stejné jako rozměry klasické plastové platební karty či studentského průkazu. Deska byla schválně navržena tak, aby přibližně odpovídala rozměrům klasické plastové platební karty, jinak by mohla být vyrobena i menší, což by ovšem bylo finančně náročnější.

Na Obr. 3.14 lze vidět vyleptanou desku s vodivými cestami a planární cívkou. Na druhé straně (Obr. 3.15) lze vidět jednotlivé osazené součástky na desce, včetně mikroprocesoru. Propojení mezi středem cívky a kapacitním trimrem je realizováno drátovou propojkou. K emulátoru byl dodatečně připájen na zadní stranu paralelně k rezistoru další rezistor pro snížení jeho hodnoty a dále byly ke vstupu ke komparátoru připájeny dva SMD rezistory pro snížení vstupní úrovně.

Obr. 3.14 - Vyrobený a osazený emulátor HF RFID tagu – zadní strana



Obr. 3.15 - Vyrobený a osazený emulátor HF RFID tagu – přední strana

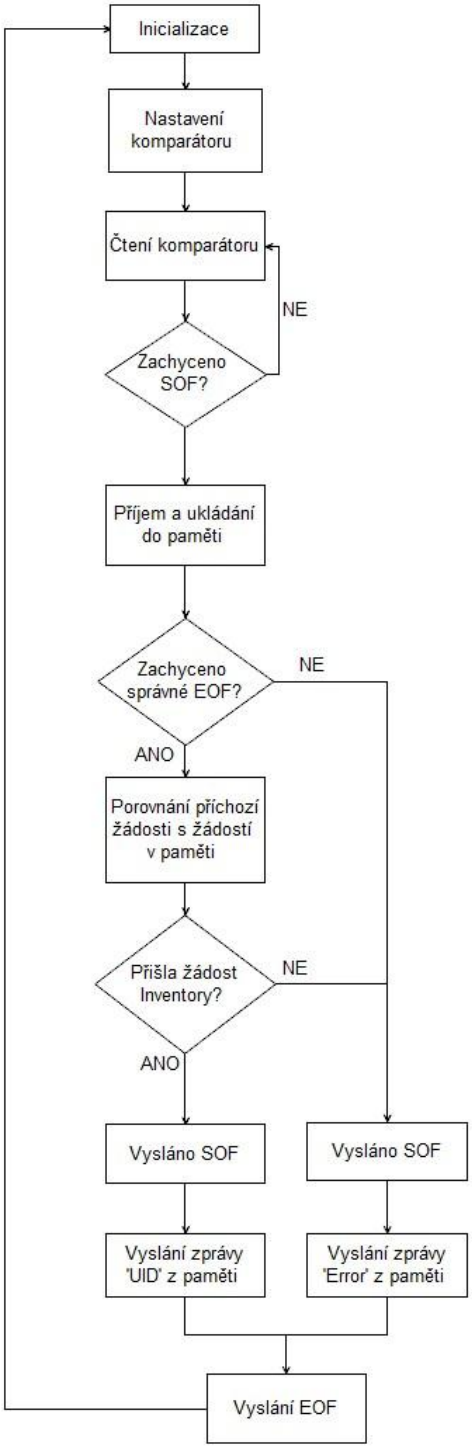
4 NÁVRH SOFTWARU

Návrh programu je založen na znalosti přesného rámce žádosti, který je vysílán čtečkou a přijímán emulátorem. Ten je znám nejen díky normě, ale také měřením žádosti přes logický analyzátor, který lze vidět na Obr. 3.6 a Obr. 3.7. Díky této znalosti je software vytvořen na jednoduchém principu - pokud přijde konkrétní žádost, emulátor odpoví konkrétní, předem definovanou odpovědí uloženou v paměti emulátoru. Vzhledem k tomu, že čtečka v základním nastavení posílá pouze žádost Inventory, který je znám a po dekódované odpovědi pošle příkaz Stay Quiet na který emulátor nereaguje, může být program realizován s myšlenou, že pošle svoje UID pouze když dostane žádost Inventory a ta se bude shodovat s žádostí uloženou v paměti, jinak emulátor nedělá nic. Program je možné ještě vylepšit tak, že v případě neznámé žádosti odpoví zprávou Chyba ‘0F‘ čímž dá najevo, že daná žádost není podporována. Za daného řešení není nutná případná kontrola CRC16, jelikož očekávané Inventory bude mít tento kód vždy stejný a v případě chybného přenosu se nebude shodovat celá zpráva.

4.1 Popis programu

Na Obr. 4.1 je zobrazen jednoduchý vývojový diagram použitého programu. Ten je zde detailněji popsán. Na začátku programu se provede inicializace vstupu a výstupu a nastavení komparátoru. Komparátor je tedy schopen rozlišovat vysokou a nízkou úroveň, která do něj přichází. V případě, že na komparátor přijde logická jednička, na emulátoru se rozsvítí LED dioda. Tím je zajištěna kontrola zda se emulátor nachází v dostatečně silném poli. Pokud se v tomto poli nachází, začne vykonávat funkci, kdy čeká na příchozí SOF. Během příchozího SOF se kontroluje každá nízká úroveň, zda jde opravdu o SOF, v jiném případě bude funkce ukončena s návratovou hodnotou 0x00, a program bude čekat na další SOF. Pokud je celý SOF přijat dobře, začne se kontrolovat pozice logické nuly v každém bytu následující zprávy. Tato logická nula se nachází v každém bytu na jedné ze čtyř pozic. Tato pozice je kontrolována programem tím způsobem, že pokud se nízká úroveň nenachází na první pozici, počká 18,88µs a zkontroluje druhou pozici, nenachází-li se ani tam počká dalších 18,88µs a zkontroluje třetí a dále tímto způsobem i čtvrtou. Ve chvíli kdy se na konkrétní pozici nachází logická nula, je tato pozice zaznamenána a její hodnota je uložena do pole proměnných. V kapitole 2.3 je popsáno poziční kódování, podle kterého může daná pozice znamenat jednu hodnotu ze čtyř možných (00,01,10 nebo 11). Po uložení hodnoty komparátor čeká na začátek vysoké úrovně, pomocí které je synchronizován s náběžnou hranou a počká určitý čas který zbývá do konce daného bytu. V případě, že se ani na jedné pozici nenachází logická 0, program počká na příchozí EOF a po jeho ukončení vyšle odpověď s daty o nastalé chybě ‘0F‘. Jelikož je očekávána pouze jednoduchá žádost Inventory, která obsahuje bez SOF a EOF pouze 80 bitů, provede se dané zaznamenávání hodnot čtyřicetkrát a poté se kontroluje správnost EOF. Je-li EOF také správně přijata a dešifrována, je ukončen příjem dat, a emulátor začne porovnávat pole přijatých bitů s polem bitů předem definovaných v paměti. Pokud tato dvě pole proměnných jsou totožná, je povoleno vysílání dat a emulátor musí do 300µs začít odpovídat čtečce zprávu o svém UID. V opačném případě, pokud je příchozí žádost vyslaná čtečkou neznámá, emulátor začne odpovídat zprávu o chybě. Daná zpráva UID nebo Error je složena z hexadecimálních čísel, které se mají poslat. Jelikož, je ovšem odpověď kódována kódem Manchester, je při vyslání každého bitů každého bytu volána funkce logické jedničky nebo logické nuly podle

Obr. 2.4. Tato funkce musela být předem nadefinována, ovšem díky ní se celý program zjednoduší a je více přehledný. Stejně tak je volána speciální fuknce i pro SOF a EOF. Po odeslání EOF odpovědi, je opět zakázáno vysílání a povolen příjem.



Obr. 4.1 – Vývojový diagram použitého programu

5 ZÁVĚR

V první části této práce byly popsány základní informace o RFID technologii. O tom, co to je a z čeho se skládá. Jak může být napájena, jak se dělí dle frekvence, jakou může mít podobu a na jakém principu může pracovat. Dále jsou zde popsány používané standardy pro RFID a okruhy, kde je tato technologie nejvíce využívána nebo by se využívat mohla.

V druhé části práce je popsán standard ISO 15693, podle kterého emulátor pracuje. Je zde popsáno jak se vysílané zprávy z čtečky a tagu kódují a jaká data mají všechny zprávy obsahovat. Kromě Start of Frame a End of Frame, které ohraničují zprávu a udávají její začátek a konec patří mezi ně pole Flags, které definuje základní parametry komunikace a CRC16, které slouží jako ochrana proti chybnému přenosu.

Ve třetí části práce je popsán návrh a konstrukce emulátoru tagu využívající pásmo HF pásmo, tedy 13,56 MHz. Je zde vykresleno schéma emulátoru a popsány jeho jednotlivé části, především návrh planární cívky a její výpočet. Dále jsou zde ukázky z měření příjmu signálu ze čtečky a odpovědi z emulátoru. Měření úrovně signálu, a jeho správnosti co se týče kódování a časování. Nakonec je popsán výběr použitého mikroprocesoru a obrázky vyrobeného a osazeného emulátoru.

Poslední část informuje o softwaru, se kterým emulátor pracuje. Nejprve je zde popsáno podle jaké základní myšleny byl program vytvořen. Dále je zde přiložen vývojový diagram a detailní popis jak program přijímá žádost, dekóduje a vysílá zpět kódovanou odpověď.

Práce měla za cíl vyrobit fungující emulátor včetně softwaru, který by simuloval bezkontaktní kartu s vazbou na dálku. Emulátor spolehlivě přijímá a dekóduje základní přijatou žádost Inventory, a je schopen na ni odpovědět buď zprávou o svém UID nebo zprávou o případné nastalé chybě. Tato odpověď je sice manuálně nebo přes citlivé počítačové dekodéry čitelná, ovšem na běžné čtečky má příliš nízkou úroveň zátěžové modulace. Tato úroveň zátěžové modulace by šla navýšit hardwarovou úpravou emulátoru, například vložením tranzistoru Q3 před Graetzův můstek jenž nyní usměrňuje i danou odpověď a tím snižuje její úroveň na polovinu.

Případná další práce by se mohla věnovat vylepšování parametrů emulátoru, větší databázi možných žádostí, na které může emulátor odpovídat, lepší synchronizaci případně i možnost antikolize.

Literatura

[1] ŘEZNÍČKOVÁ, Lenka. *RFID*. Pardubice, 2009. Bakalářská práce. Univerzita Pardubice Fakulta ekonomicko-správní. Vedoucí práce Ing. Milan Tomeš.

[2] ČERNÝ, Tomáš. *Technologie RFID: možnosti jejich využití a nasazení v podniku*. V Praze, 2007. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra informačních technologií, Vedoucí práce Doc. Ing. Jan Pour, CSc.

[3] HANAČÍK, Radim. *BEZPEČNOST RFID*. V Brně, 2011. Bakalářská práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací. Vedoucí práce Ing. ZDENĚK MARTINÁSEK.

[4] ULBERT, Martin. *Možnosti využití RFID technologie pro potřeby Dopravního podniku měst Chomutova a Jirkova, a. s.* V Pardubicích, 2014. Bakalářská práce. Univerzita Pardubice Dopravní fakulta Jana Pernera.

[5] SOMMEROVÁ, Martina. Základy RFID technologií. In: RFID vsb Ostrava [online]. 2013 [cit.2014-12-15]. Dostupné z: http://rfid.vsb.cz/miranda2/export/sites-root/rfid/cs/okruhy/informace/RFID_pro_Logistickou_akademii.pdf.

[6] ŠVANDA, Milan; POLÍVKA, Milan. *Antény pro RFID a wearable („nositelné“) antény* [online prezentace]. Katedra elektromagnetického pole, [cit. 2014-12-15]. Dostupný z: <http://old.elmag.org/lib/exe/fetch.php/k317:nka:02pr_a0m17nka_rfid_anteny_svanda-polivka.pdf>

[7] ITLib: Standardy a pravidla pro technologii RFID. *ITLib: Standardy a pravidla pro technologii RFID* [online]. 2013 [cit. 2014-12-16]. Dostupné z: http://itlib.cvtisr.sk/archiv/2013/2/standardy-a-pravidla-pro-technologii-rfid.html?page_id=2461

[8] PEŠEK, David. *RFID - radiofrekvenční identifikace: důvod k obavám?* [online]. 1. vyd. Praha: Sdružení českých spotřebitelů, c2010, 12 s. [cit. 2014-12-16]. Publikace České technologické platformy pro potraviny. ISBN 978-80-903930-9-7..

[9] Kevin Warwick. *Kevin Warwick: What happens when a man is merged with a computer?* [online]. 2011 [cit. 2014-12-16]. Dostupné z: http://www.kevinwarwick.com/Cyborg1.htm

[10] Access server: Klonování RFID čipů na přístupových kartách. HOLENDA, Martin, VAŇEK a ROHLÍK. *Access server: Klonování RFID čipů na přístupových kartách* [online]. 2012 [cit. 2014-12-16]. Dostupné z: http://access.fel.cvut.cz/view.php?nazevclanku=klonovani-rfid-cipu-na-pristupovych-kartach&cisloclanku=2012070003

[11] Koumes.misto.cz. *Návrh plošných cívek* [online]. 2004 [cit. 2014-12-16]. Dostupné z: http://koumes.misto.cz/_MAIL_/navody/civka/civka.htm

[12] Základy elektroniky, diody. *Www.spsemoh.cz* [online]. 2014 [cit. 2014-12-16]. Dostupné z: http://www.spsemoh.cz/vyuka/zel/diody.htm

[13] LANG, Radek. *MĚŘENÍ DYNAMICKÝCH VLASTNOSTÍ BIPOLÁRNÍCH A UNIPOLÁRNÍCH TRANZISTORŮ*. Brno, 2013. Bakalářská práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Ing. Jiří Dřínovský, Ph.D.

[14] VISHAY SILICONIX. *IRFD110, SiHFD110: Datasheet*. 2010 [cit. 2014-12-16]. Dostupné z: http://www.vishay.com/docs/91127/sihfd110.pdf

[15] www.czechduino.cz: co je to Arduino. *www.czechduino.cz* [online]. 2012 [cit. 2014-12-16]. Dostupné z: http://www.czechduino.cz/?co-je-to-arduino,29

[16] ATMEL. *ATMEL 8-BIT MICROCONTROLLE R WITH 4/8/16/32KBYTES IN-SYSTEM PROGRAMMABLE FLASH: Datasheet*. 2014. Dostupné z: http://www.atmel.com/images/Atmel-8271-8-bit-AVR-Microcontroller-ATmega48A-48PA-88A-88PA-168A-168PA-328-328P_datasheet_Complete.pdf

[17] ČERNÝ, Jakub. *EVIDENCE MAJETKU PROSTŘEDNICTVÍM RFID*. Brno, 2007. Bakalářská práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, FAKULTA PODNIKATELSKÁ ÚSTAV INFORMATIKY (UI). Vedoucí práce ING. JIŘÍ KŘÍŽ, PH.D.

[18] BAŤA, Tomáš. *Zabezpečení zboží RFID technologiemi*. Zlín, 2011. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce JUDr. Vladimír Laucký.

[19] VISHAY SEMICONDUCTORS. *BAT42, BAT43: Datasheet*. 2013. Dostupné z: http://www.vishay.com/docs/85660/bat42.pdf

[20] http://www.circuits.dk: Single layer Planar spiral coil inductor calculator. [online]. 2010 [cit. 2015-5-8]. Dostupné z: http://www.circuits.dk/calculator_planar_coil_inductor.htm

[21] MELEXIS, Microelectronic integrated systems. *13.56 MHz RFID systems and antennas design guide.* 2004. Dostupné z: http://webcache.googleusercontent.com/search?q=cache:kIPB_sVTLD0J:www.melexis.com/Asset/1356-MHz-RFID-systems-and-antenna-design-guide-DownloadLink-6098.aspx+&cd=1&hl=cs&ct=clnk&gl=cz

[22] *Identification cards — Contactless integrated circuit(s) cards: Vicinity cards*. Geneva, Switzerland: ISO Central Secretariat, 2000.

[23] *www.Alza.cz: Arduino Nano V3.0* [online]. [cit. 2015-05-27]. Dostupné z: https://www.alza.cz/arduino-nano-v3-0-d569054.htm#prislusenstvi

[24] Hitoshi Kitayoshi and Kunio Sawaya: *Long range Passive RFID-tag for sensor network.* Japan. Tohoku University, 2005. Dostupné z: www.geocities.jp/ayashii_jp/VTC05f6k1.pdf

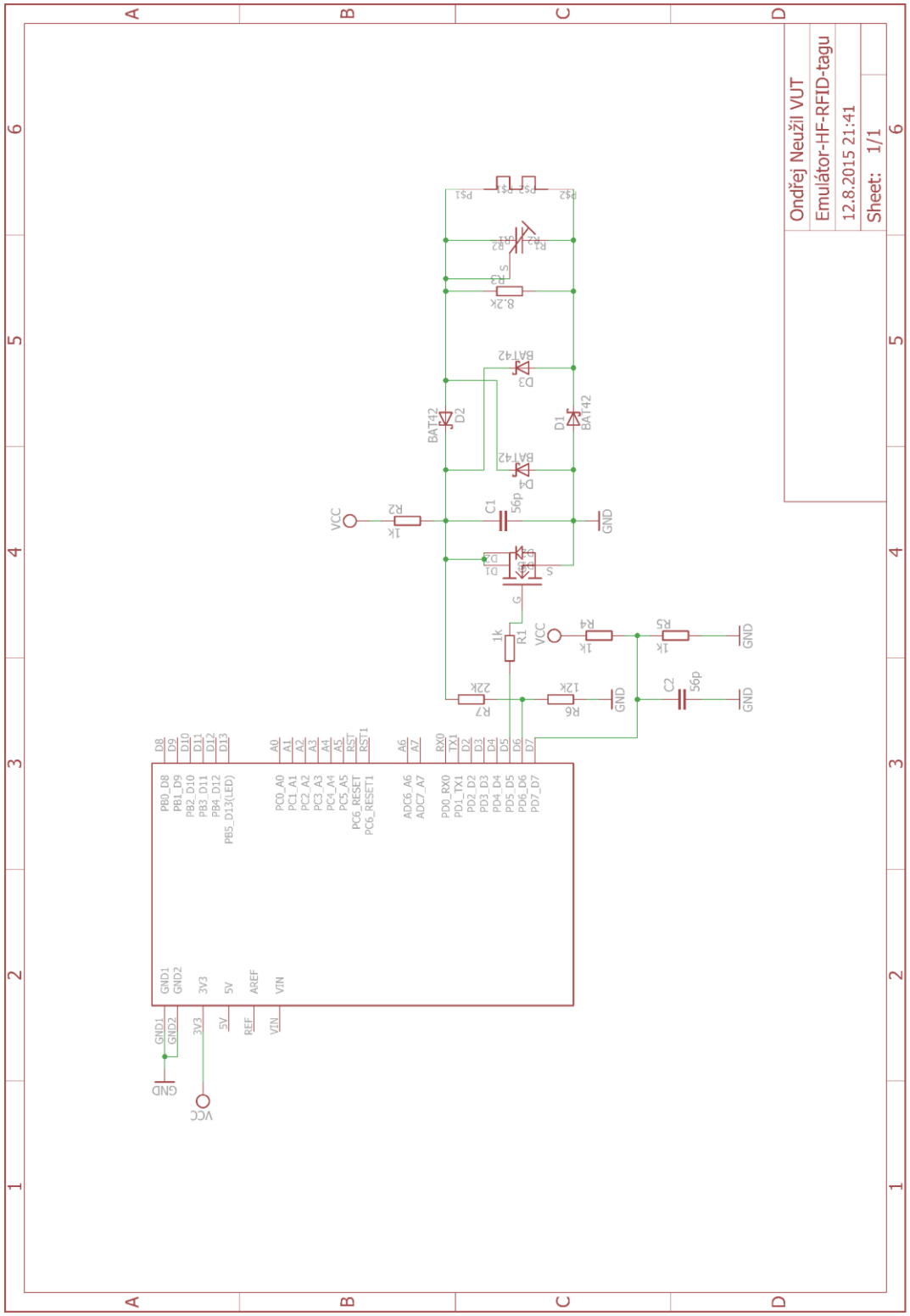
[25] *www.barcodesinc.cz: FEIG ID CPR30 RFID Reader* [online]. [cit. 2015-08-12]. Dostupné z: https:// http://www.barcodesinc.com/feig/id-cpr30.htm

Seznam symbolů, veličin a zkratek

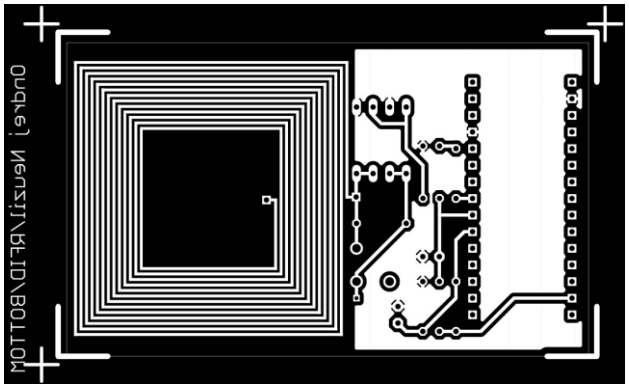
RFID	Radio-frequency identification, radio-frekvenční identifikace
IFF	Identification Friend and Foe, identifikace přítel nebo nepřítel
EPC	Electronic Product Code, elektronický kód produktu
TTF	Tag talks first, tag vysílá první
RTLS	Real Time Location Systém, systém lokalizace v reálném čase
LF	Low Frequency, nízká frekvence
HF	High Frequency, vysoká frekvence
UHF	Ultra-High frequency, ultra-vysoká frekvence
MW	Microwave, mikrovlny
EAS	Electronic Article surveillance, elektronický dozorový článek
ASK	Aplitude shift keying, amplitudové klíčování
RO	Read-Only, pouze čtení
RW	Read/Write, čtení/zapisování
WORM	Write Once/Read Many, zapisování jednou/čtení mockrát
C	Capacitor, kondenzátor
L	Inductor, induktor (cívka)
N	Počet závitů
R	Resistance, odpor
R_{DS}	Resistance(drain-to-source), odpor mezi drain a source
U_{GS}	Gate-Source Voltage, napětí mezi gate a source
PWM	Pulse Width Modulation, pulzně šířková modulace
f_o	frekvence nosné
GND	Ground, uzemění
Vcc	Zdroj
D	Dioda
Q	Tranzistor
SOF	Start of Frame, začátek rámce
EOF	End of Frame, konec rámce
UID	Unique Identifier, unikátní identifikátor
DSFID	Data Storage Format Identifier, strukturování dat v paměti
CRC	Cyclic Redundancy Check, cyklický redundantní součet

A Návrh zařízení

A.1 Obvodové zapojení emulátoru RFID tagu

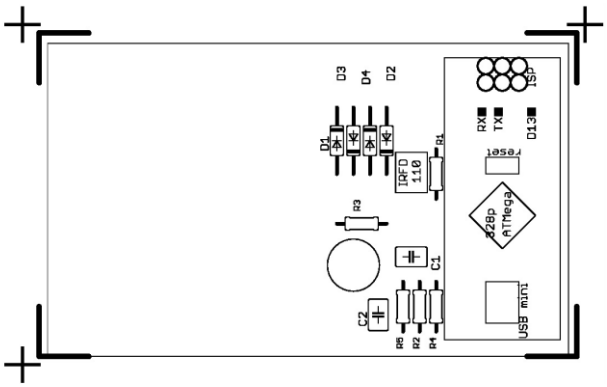


A.2 Deska plošného spoje emulátoru RFID tagu – bottom (strana spojů)



Rozměr desky 82 x 50 [mm], měřítko M1:1

A.3 Osazovací plán



Rozměr desky 82 × 50 [mm], měřítko M1:1

B Seznam součástek

Označení	Hodnota	Pouzdro	Popis
C1	56pF	c2.5-3	Keramický kondenzátor
C2	56pF	c2.5-3	Keramický kondenzátor
C4	3 – 50pF	3008	Kapacitní trimr
IC1		TQFP32	Mikrokontrolér
D1	BAT42	DO35-10	Schottkyho dioda
D2	BAT42	DO35-10	Schottkyho dioda
D3	BAT42	DO35-10	Schottkyho dioda
D4	BAT42	DO35-10	Schottkyho dioda
L1	9,3µH		Planární cívka
Q	IRFD110	TO-92	Unipolární tranzistor
R1	1kΩ	0204/7	Rezistor
R2	1kΩ	0204/7	Rezistor
R3	8,2kΩ	0204/7	Rezistor
R4	1kΩ	0204/7	Rezistor
R5	1kΩ	0204/7	Rezistor
R6	12kΩ	0805	Rezistor
R7	22kΩ	0805	Rezistor