BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF RADIO ELECTRONICS
ÚSTAV RADIOELEKTRONIKY

RFID READER FOR 13.56 MHZ BAND

RFID ČTEČKA PRO PÁSMO 13,56 MHZ

MASTER'S THESIS
DIPLOMOVÁ PRÁCE

AUTHOR
AUTOR PRÁCE

Bc. Michal Obšitník

SUPERVISOR
VEDOUCÍ PRÁCE

Ing. Aleš Povalač, Ph.D.

BRNO 2021

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Master's Thesis

Master's study program **Electronics and Communication Technologies**

Department of Radio Electronics

Student:	Bc. Michal Obšitník	***ID:*** 195401
Year of study:	2	***Academic year:*** 2020/21

TITLE OF THESIS:

RFID Reader for 13.56 MHz Band

INSTRUCTION:

Study and describe the communication protocols used in the 13.56 MHz band. Focus especially on ISO / IEC 14443 Type A and Mifare Classic incl. its security. Get acquainted with the CR95HF chip, demonstrate the function of the NFC reader on the development board with the STM32 microcontroller. Describe the basic principles of design and tuning of the reader antenna.

Design a prototype reader based on the CR95HF chip with a set of different antennas. Create firmware with a user interface on the display. Measure the maximum reading distance of the created antennas, verify the distance degradation and tuning options if the antenna is in close proximity to a metal object. Document in detail the adjustment procedures and the measurement results.

RECOMMENDED LITERATURE:

[1] FINKENZELLER, Klaus. RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. 3rd ed. Chichester: Wiley, 2010. ISBN 978-0470695067.

[2] STMicroelectronics. CR95HF: 13.56-MHz multi-protocol contactless transceiver IC with SPI and UART serial access: Datasheet [online]. [cit. 2020-05-15]. Dostupné z: https://www.st.com/resource/en/datasheet/cr95hf.pdf

Date of project specification:	8.2.2021	***Deadline for submission:*** 20.5.2021

Supervisor: Ing. Aleš Povalač, Ph.D.

prof. Ing. Tomáš Kratochvíl, Ph.D.
Chair of study program board

WARNING:

The author of the Master's Thesis claims that by creating this thesis he/she did not infringe the rights of third persons and the personal and/or property rights of third persons were not subjected to derogatory treatment. The author is fully aware of the legal consequences of an infringement of provisions as per Section 11 and following of Act No 121/2000 Coll. on copyright and rights related to copyright and on amendments to some other laws (the Copyright Act) in the wording of subsequent directives including the possible criminal consequences as resulting from provisions of Part 2, Chapter VI, Article 4 of Criminal Code 40/2009 Coll.

Abstract

The aim of this thesis is to design an RFID reader for the 13.56 MHz band and to compile a control program. In the first part, the work is aimed at getting acquainted with the principle of operation of RFID and NFC technologies, together with the related international standard, and at getting familiarized with the various transceivers available to operate these technologies. Because the transceiver for the further evaluation is clearly specified in the assignment, their comparison serves a purely informational purpose. In the practical part, the task is to design and revive a prototype RFID reader. The base of the project is a reader board carrying out RFID communication, audiovisual response, and connection to an OLED display. This board is connected to a microcontroller, which controls the whole device. Another part of the project is set of different antennas that can be connected to the reader board and replaced at any time. The manufactured antennas are subject to a testing of how two different tuning methods affect their operation. The maximum reading distance, success of the performed readings and value of the electrical current that is a result of the calibration process are being tested. The output of the thesis is an RFID reader with a control program.

Keywords

RFID, CR95HF, STMicroelectronics, reader, transponder, control program, antennas.

Abstrakt

Cieľom tejto práce je navrhnúť RFID čítačku pre pásmo 13.56 MHz a zostaviť k nej riadiaci program. V prvej časti je najskôr práca smerovaná k oboznámeniu sa s princípom fungovania technológií RFID a NFC, spolu s tým súvisiacimi medzinárodnými štandardami a k oboznámeniu sa s rôznymi dostupnými čipmi na obsluhu týchto technológií. Keďže čip s ktorým sa bude pokračovať je jasne zadaný v návode, ich porovnanie slúži čisto oboznamovaciemu účelu. V praktickej časti je úloha navrhnúť a oživiť prototyp RFID čítačky. Základom je doska sprostredkúvajúca RFID komunikáciu, audiovizuálnu odozvu a pripojenie k OLED displeju. Táto doska je pripojená na mikrokontrolér na ktorý riadi celé ovládanie zariadenia. Súčasťou projektu je aj set rôznych antén, ktoré je možné na dosku pripojiť a zároveň ich vymieňať. Vyrobené antény sú podrobené testovaniu ako dve rozdielne metódy ladenia ovplyvnia ich chod. Testujú sa maximálna vzdialenosť čítania, úspech prevedených čítaní a hodnota prúdu, ktorá sa vznesie pri kalibračnom procese. Výstupom práce je RFID čítač s riadiacim programom.

Kľúčové slova

RFID, CR95HF, STMicroelectronics, čítačka, transpondér, riadiaci program, antény

Rozšírený abstrakt

Technológia RFID sa v posledných rokoch stala neodlúčiteľnou súčasťou nášho sveta. Vďaka rýchlo sa vyvíjajúceho oblasti technológií sa táto technológia stále zlepšuje, čo má za dôsledok, že stále viac a viac sa využíva nie len na identifikáciu osôb ale aj iných predmetov a ich detekciu. Jej hlavnou výhodou je bezkontaktnosť a v porovnaní s čiarovými kódmi netreba vyvinúť úsilie na vizuálnu identifikáciu prostredníctvom skenovania kódu.

Systémy RFID fungujú na princípe indukčnej väzby. Všetko čo je potrebné na úspešnú identifikáciu je, aby sa transpondér (nosič informácie) dostal do elektromagnetického poľa čítačky, ktoré nielen že prenesie dáta rádiovými vlnami, ale slúži aj ako napájanie transpondéru. Vo veľkom množstve prípadov sú transpondéry bez samostatného napájania – pasívne, a teda potrebujú dodanie energie na ich funkciu. V momente, keď sa transpondér priblíži k čítačke, zoberie si energiu pre napájanie svojho mikročipu z vytvoreného poľa, a informáciu, ktorú mikročip v sebe nosí, vyšle naspať. Čítačka túto informáciu prečíta a postupuje podľa ďalej preddefinovaných krokov. Využívanie prenosu rádiovými vlnami naznačuje, že oba transpondér aj čítačka musia mať v sebe zabudovanú anténu, ktorá je naladená na rovnakú pracovnú frekvenciu.

Kvôli rôznorodému využitiu a fyzikálnym princípom sa RFID systémy delia na kategórie podľa frekvencie na ktorej sú prevádzkované. Rôzne frekvencie majú totiž rôzne vzdialenosti čítania s teoretické rýchlosti prenosu. Vlny s kratšou vlnovou dĺžkou budú prenášať informácie rýchlejšie, a vďaka ich väčšiemu povolenému prenosovému výkonu intenzity poľa, budú ich čítacie vzdialenosti väčšie.

Medzinárodné štandardy boli vymyslené na to aby si zjednotilo a zjednodušilo používanie rovnakých technológií naprieč celým svetom. Preto aj technológia RFID, vďaka svojej rôznorodosti podlieha určitým štandardom. Medzi najviac zaužívane v oblasti identifikácie osôb patrí štandard ISO/IEC 14443. Vo svojich 4 častiach pojednáva hlavne o fyzickej charakteristike, vysokofrekvenčnom výkonovom a signálovom rozhraní, inicializácii a proti kolíznom procese, a o prenosových protokoloch. Z tohto štandardu potom vychádza obchodná značka MIFARE založená firmou NXP, ktorá obsahuje rad integrovaných obvodov pracujúcich podľa niektorých častí štandardu ISO/IEC 14443.

Táto práca sa zaoberá návrhom RFID čítačky pre pásmo 13.56 MHz, ktoré podlieha vyššie spomenutému štandardu. Medzi najpoužívanejšie integrované obvody slúžiace ako vysielač-prijímač v tomto pásme patria: CR95HF, TRF7970A a PN532. Z ich teoretického porovnania vyplýva, že spomenuté obvody sú porovnateľne podobné,

len s malými rozdielmi. Pre použitie základných funkcií v nich prakticky rozdiel nie je a výber je na používateľovi. Avšak, pri použití zložitejších funkcií môže nastať situácia, že iba jeden z menovaných obvodov bude danú funkciu podporovať. V takom prípade je nutné si dôkladne preštudovať ich sprievodné listy a vybrať si na základe aplikácie na ktorú budú použité.

V rámci praktickej časti som sa zabýval návrhom prototypu RFID čítačky pre už spomínané pásmo 13,56 MHz. Ako vysielač-prijímač bolo zadané použitie integrovaného obvodu CR95HF of firmy STMicroelectronics. Schéma zapojenia a doska plošných spojov bola navrhnutá v programe Eagle. Pri návrhu som dodržiaval návrhové postupy zadané školskou dielnou. Vo väčšine prípadov je použitá šírka vodivej cesty 0,4 mm a navŕtanými dierami šírky 1 mm. Doska obsahuje aj dve LED diódy a bzučiak na audiovizuálnu signalizáciu stavu čítania. Súčasťou projektu je set šiestich rôznych antén, ktoré sú vymeniteľné a je možné ich použiť s doskou čítačky. Antény boli navrhnuté v dvoch rozmeroch a každý rozmer obsahuje tri rôzne kombinácie počtu závinov na anténnej cievke, čo má za následok rôzne hodnoty indukčností jednotlivých antén. Antény boli podrobené ladeniu dvoma rôznymi spôsobmi a to ladenie na základe software poskytovaného od STMicroelectronics. V rámci druhej metódy ladenia boli jednotlivé antény pripojené na sieťový analyzátor Agilent a následne boli menené hodnoty kondenzátorov na doladenie.

Pre daný projekt bol následne vytvorený riadiaci program, na sprostredkovanie RFID komunikácie a ovládanie CR95HF. Riadiaci program obsahuje niekoľko dôležitých funkcií, ktoré ovplyvňujú ako komunikácia prebieha. Funkcia uart_process_command čaká na jeden z príkazov od užívateľa, ktorý má tým pádom plnú kontrolu nad ovládaním čipu CR95HF. Bez žiadneho zadaného príkazu čip ostáva v poslednom známom stave okrem stavu „tag detection“ (detekcia transpondéru) je čip nečinný. Ďalšími dôležitými funkciami sú zápis a čítanie správ, ktoré prebiehajú medzi vytvorenou doskou s integrovaným obvodom a transpondérom. CR95HF po prečítaní prijatých dát, následne dáta ďalej posiela prostredníctvom rozhrania UART do nasledujúceho zariadenia a taktiež na OLED displej ktorý je pripojený na vyrobenú dosku. Ako základ na ovládanie zariadenia je použitý mikrokontrolér STM32F030.

Celé zariadenie bolo podrobené dôkladnému testovaniu funkčnosti dosky čítačky a jednotlivých antén. Porovnané boli hlavne výsledky maximálnej čítacej vzdialenosti a úspešnosť čítaní pre oba spôsoby doladenia antén. Z výsledkov je zrejmé, že software-ové ladenie poskytuje dobré výsledky čo sa týka čítacej vzdialenosti ale porovnaní s ladením na sieťovom analyzátore je úspešnosť čítaní slabá, čo robí čítač prakticky nepoužiteľný. Ladenie sieťovým analyzátorom teda výrazne pomohlo úspešnosti čítaní. Výstupom diplomovej práce je literárna rešerš na tému RFID pre 13,56 MHz a RFID čítačka schopná čítať ISO/IEC 14443 – A a ISO/IEC 15693 transpondéry. K čítačke je set vymeniteľných antén a riadiaci program, ktorý čítačku obsluhuje.

Bibliographic citation:

OBŠITNÍK, Michal. *RFID Reader for 13.56 MHz Band* [online]. Brno, 2021 [cit. 2020-05-08]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/133610. Master's Thesis. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Department of Radioengineering. Supervisor Aleš Povalač.

Author’s Declaration

Author:	Michal Obšitník
Author’s ID:	195401
Paper type:	Master’s Thesis
Academic year:	2020/21
Topic:	RFID Reader for 13.56 MHz Band

I declare that I have written this thesis titled “RFID Reader for 13.56 MHz Band” independently, under the guidance of the advisor and using exclusively the technical references and other sources of information cited in the project and listed in the comprehensive bibliography at the end of the project.

As the author I furthermore declare that, with respect to the creation of this thesis, I have not infringed any copyright or violated anyone’s personal and/or ownership rights. In this context, I am fully aware of the consequences of breaking Regulation S 11 of the Copyright Act No. 121/2000 Coll. of the Czech Republic, as amended, and of any breach of rights related to intellectual property or introduced within amendments to relevant Acts such as the Intellectual Property Act or the Criminal Code, Act No. 40/2009 Coll., Section 2, Head VI, Part 4.

Brno: **20th of May 2021**

....
author’s signature

Acknowledgement

I would like to thank my supervisor Ing. Aleš Povalač, Ph.D. for his effective methodological, pedagogical, and professional help and other valuable advice in the elaboration of my master's thesis. Also, I would like to thank my girlfriend Grace for major support with the English language in my master's thesis and her constant support!

Brno: **20th of May 2021**

....
author's signature

CONTENTS

1. Introduction 1

2. RFID Technology 2

2.1 Frequencies and ranges of RFID systems 4

2.2 Physical and operating principles 6

2.2.1 Physical principles 6

2.2.2 Operating principles 7

2.3 Security of RFID systems 9

2.3.1 Protection 11

2.4 Standardization 12

2.4.1 ISO/IEC 14443 Type A and B 12

2.4.1.1 Physical characteristics 12

2.4.1.2 Radio frequency interface 13

2.4.1.3 Initialization and Anti-collision 13

2.4.1.4 Transmission Protocols 14

2.4.2 Mifare classic 14

2.4.3 ISO/IEC 15693 15

2.4.3.1 Physical characteristics 15

2.4.3.2 Air interface and initialization 15

3. Near-Field communications (NFC) 16

3.1 Modes of operation 16

3.2 NFC tag types 17

3.3 Data transfer 19

3.4 Standardization of NFC 20

3.4.1 ISO/IEC 18092 or ECMA-340 (NFCIP-1) 20

3.4.2 ISO/IEC 21481 or ECMA-352 (NFCIP-2) 20

4. Transceivers for 13.56 MHz Band 22

4.1 CR95HF – STMicroelectronics 22

4.2 TRF7970A – Texas Instruments 22

4.3 PN532 – NXP 23

5. Testing of transceiver CR95HF 24

5.1 Microcontroller and expansion board 24

5.2 Conclusion of testing 25

6. Connection Design 26
6.1 Microcontroller 26
6.2 Display 27
6.3 Antennas 27
6.4 Reader board 27
6.5 Printed Circuit Board layout for Reader board 29
6.6 Printed Circuit Board layout for Antenna boards 30

7. Antenna tuning for RFID reader 32
7.1 Low pass filter 33
7.2 Impedance matching 34
7.3 Matching circuit determined by software 34
7.4 Matching circuit determined by measurements with network analyzer 36
7.5 Detuning caused by conductor 40

8. Firmware 42
8.1 Communication interfaces 43
8.2 Display 43
8.3 Reader source file 44
8.3.1 Operating modes 44
8.3.2 Initializations 45
8.3.3 Reading algorithms 46
8.3.3.1 Anti-collision loop of ISO/IEC 14443 Type A standard 46
8.3.3.2 Reading of ISO/IEC 15693 tag 47
8.3.4 Sending commands 47
8.3.5 UART Commands 48
8.4 Tag detection calibration 49
8.5 Modes of reader operation 50
8.6 Source codes 50

9. Testing of the reader 51
9.1 Antennas tuned by software 51
9.1.1 Comparison of reading ranges using different transponders 51
9.1.2 Testing of the Tag detection calibration procedure 53
9.2 Antennas tuned by network analyzer 54
9.2.1 Comparison of reading ranges using different transponders 54
9.2.2 Testing of the Tag detection calibration procedure 55
9.3 Test results 56

10. Conclusion 57

FIGURES

Figure 2.1: RFID System Components – [5] 2

Figure 2.2: The definition of mutual inductance by the coupling of two coils – [4] 7

Figure 2.3: Comparison of Full-duplex and Half-duplex procedure – [4]....................... 8

Figure 2.4: Load Modulation with Subcarrier – [4]... 9

Figure 2.5: Overview of basic attacks on RFID systems - [4]...................................... 10

Figure 2.6: Communication process with data encryption – [4]................................... 12

Figure 3.1: Overview of NFC modes of operation – [4] 17

Figure 3.2: Map of NFC-related standards and specifications [9]................................ 21

Figure 5.1: Hardware setup... 25

Figure 6.1: Hierarchical schematic design.. 26

Figure 6.2: Schematic of antenna board 27

Figure 6.3: Schematic of reader board... 28

Figure 6.4: PCB layout of Reader board.. 29

Figure 6.5: PCB layout of Antenna boards.. 30

Figure 6.6: Reader board + all antenna boards 31

Figure 6.7: Reader board a) without, b) with OLED display 31

Figure 7.1: eDesign suite 32

Figure 7.2: CR95HF tuning circuit with an EMI filter – [19] 33

Figure 7.3: Impedance matching with an EMI filter – [19]... 34

Figure 7.4: Calculator of impedance matching circuit in ST25R95 EMI filter calculation tool 35

Figure 7.5: Smith Chart drawn by ST25R95 EMI filter calculation tool 35

Figure 7.6: Measurement of resistance and inductance... 37

Figure 7.7: Connection points for network analyzer measurements 38

Figure 7.8: Results a) Return loss measurement, b) Smith chart antenna matching of tuned 47x34/6 antenna.. 39

Figure 7.9: Results a) Return loss measurement, b) Smith chart antenna matching of antenna detuned by metal 41

Figure 7.10: Testing of antenna with metal plate in proximity 41

Figure 8.1: Graphical interface of STM32CubeIDE, pinout view 42

Figure 8.2: CR95HF initialization and operating state change – [11] 44

Figure 8.3: Principle of card activation sequence of ISO/IEC 14443A – [14]............... 45

Figure 8.4: Principle of anti-collision loop – [14] 46

Figure 8.5: Communication with the CR95HF provided by serial terminal 48

Figure 9.1: Comparison of maximum reading distances using different transponders .. 53

Figure 9.2: Second comparison of maximum reading distances using different transponders 55

TABLES

Table 1: Categorizations of RFID tags by frequency - [5] 4
Table 2: Data transfer from reader to transponder – [4] 13
Table 3: Data transfer from transponder to reader – [4] 13
Table 4: Overview of NFC tag types – [9] 19
Table 5: Data transfer from reader to transponder – [9] 19
Table 6: Data transfer from transponder to reader – [9] 20
Table 7: Comparison table of different transceivers and their main characteristics 23
Table 8: Antenna variations 30
Table 9: Inductance values for antenna variations 33
Table 10: Values of impedance matching circuitry calculated by software 36
Table 11: Real properties of antennas 37
Table 12: Final capacitor values determined by tunning on the network analyzer 40
Table 13: Comparison of maximum reading distances using different transponders 52
Table 14: Reference values from calibration procedure 54
Table 15: Second comparison of maximum reading distances using different transponders 54
Table 16: Reference values from calibration procedure after the antenna tuning 55
Table 17: Comparison on how tuning by the network analyzer affected the results. Change in success rate and reading range are from testing of ISIC school card 56

1. INTRODUCTION

Throughout history, there have been various instances in which RFID systems contributed to society. During World War II., aircrafts were identified by airmen utilizing radio waves. Subsequently, in 1973, the first passive transponder with memory was created and patented by Mario Cardullo – [1]. This is considered to be the first true ancestor of modern RFID. Although, the abbreviation we use and know today was not mentioned until the year of 1983, associated with the patent granted to Charles Walton – [2]. As the name of the technology hints, RFID is carried over radio waves. These waves carry the information from the reader to the transponder and back, making the technology contactless. Thus, the process of identification became much easier, transforming scanning barcodes to contactless identification of the object / animal / person via invisible radio waves; ensuing a more effortless process. In recent years, automatic identification procedures have become extremely popular in many service industries, distribution logistics, and manufacturing companies, all with the help of RFID systems. With the ability to read the transponder up to 15 meters, this technology can be used virtually anywhere, making the RFID market one of the fastest growing markets in radio technology.

The topic I chose as my master's thesis is titled: RFID Reader for 13.56 MHz Band. The main goals given to me by my supervisor are as follows: "Study and describe the communication protocols used in the 13.56 MHz band. Design a prototype reader based on the CR95HF with a set of different antennas. Create firmware with a user interface on the display. Measure max. reading distance of the created antennas, check the distance degradation and tuning options if the antenna is in close proximity to a metal object. Document the adjustment procedures used and the measurement results in detail."

To begin, my plan is to research and collect copious amounts of information pertaining to the topic, and summarize it within my thesis. With this information obtained, I will begin to create the control program for the CR95HF transceiver. Within that program, my main goal is to read the unique identifier of transponders based on the ISO/IEC 14443 A and Mifare Classic as well as ISO/IEC 15693. The information from the transponder will be transferred to the computer over UART and also displayed on the OLED display. For the hardware components, I plan to work with the basic STM32 microcontroller - STM32F030 and design my own board, which contains the earlier mentioned transceiver. The aim of my master's thesis is to build a working prototype of a RFID reader and test out multiple antennas matched to 13.56 MHz frequency, ultimately, being able to compare their different reading ranges and influence of interference. After prototype is built, I plan on tuning the antennas with network analyzer and test the reading ranges of each antenna.

2. RFID TECHNOLOGY

The abbreviation RFID stands for radio frequency identification, which can be described as carrying identification information about a person, object etc. over radio waves. According to Lehpamer, “This technology is fundamentally based on wireless communication, which makes use of radio waves, which is ultimately part of an electromagnetic spectrum. A basic RFID system is made up two components: the transponder (tag) and reader. The transponder is always located on the person or object which is being identified while the reader’s location depends on the design of the system is located in the area where the identification is made. The essential requirement of the RFID system is to transfer data stored in a transponder to a reader across a wireless air interface. A two-way communication process is required to do this, and it requires a radio carrier signal suitably modified (modulated) to carry the data” [3]. An excellent example of this system is an ID card which is used to get into a building. The ID card is a transponder, while the reader is the device on the wall that you need to bring your card closer to.

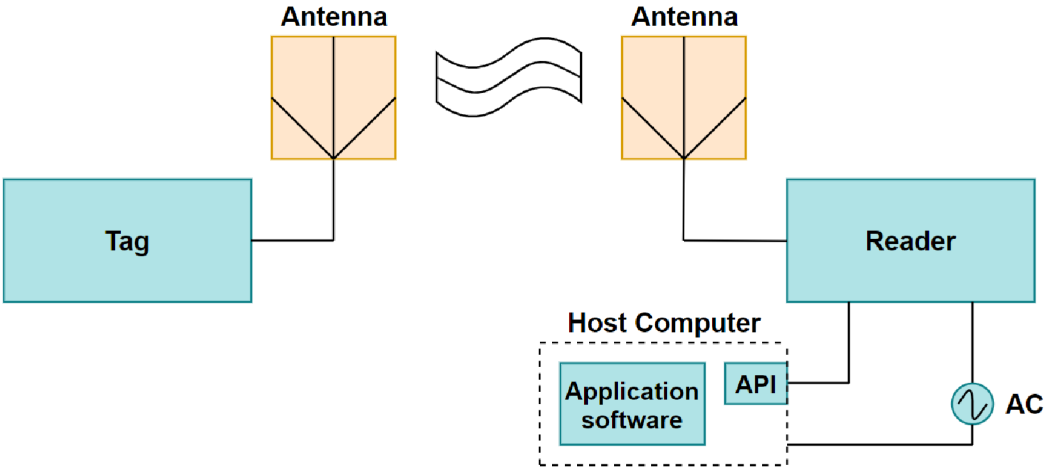


Figure 2.1: RFID System Components – [5]

As [4] says, the transponder is the actual data-carrying device of an RFID system. Typically, it consists of a coupling element and an electronic microchip. When the transponder is not within the interrogation zone of a reader, it is completely passive, because it does not usually have its own battery to provide needed power. The transponder is only activated when the activation power is supplied while it is within the interrogation zone of a reader. Power is supplied through the coupling unit, as well as the timing pulse and data. Finkenzeller states, “Reader typically contains a radio frequency module (transmitter and receiver), a control unit, and a coupling element to the transponder. In addition, many readers are fitted with an additional communication interface (RS 232/485, etc.) to enable them to forward the data received from the transponder to another system (PC, microcontroller)” [4]. The architecture of the RFID system can be seen on Figure 2.1.

As [4] expresses, capacity of data RFID transponders can normally carry ranges from a few bytes to several kilobytes. Although, so-called 1-bit transponders are an special exception. In this case, stored data is exactly 1 bit, which is plenty to signal two states to the reader. One is considered to be a "transponder in the detection range" and the other is considered to be a "transponder outside the detection range". This kind of system is perfectly suitable for simple monitoring or signaling functions. 1-bit systems are commonly used in shops and businesses to protect goods from being stolen. They will signal the transponder in the detection range to the readers at the exit if someone is trying to steal the goods. Therefore, the transponder must be removed or deactivated after the goods are paid for. Lehpamer says, "There are many other potential applications for more advanced RFID technologies. The most obvious one is a more robust replacement of barcodes as mentioned before, however innovative companies are regularly finding new applications for the enhanced range, capacity, and read/write capability" [3]. Readers can be different sizes which is a big advantage for this technology.

Described by [4], one of the most innovative functions of RFID systems is the possibility of reading/writing data to the transponder. In a simpler system, such as the transponder's data record, a number is typically incorporated when the chip is manufactured, and cannot be changed afterwards. In writeable transponders, one gains a possibility to write data directly to the transponder at any given moment. This process is done by a reader, and can be done multiple times. There are three main procedures to store the data. First procedure, the most dominant, is where data is stored in the inductively coupled RFID systems EEPROM (electrically erasable programmable read-only memory). However, EEPROM have a disadvantage of limited number of write cycles and high-power consumption during the writing operation. The second system is named FRAM (ferromagnetic random-access memory) has power consumption lower than EEPROMs by a factor of 100 and writing time typically 1000 times lower. The third and final storage system, which is particularly common in microwave applications, is SRAM (static random-access memory). SRAMs have incredibly fast write cycles; however, an uninterruptible power supply from battery is required for data retention. According to Lehpamer, "RFID systems themselves can achieve high levels of complexity, from 1-bit systems to having incorporated memory, which allows for data processing capabilities that include communication encryption, and protocols." [3]

As previously mentioned, another important feature of RFID system is the power supply in transponders. According to the [4], this feature splits transponders into two categories: passive and active. The more commonly used, passive transponders do not have their own power supply. Therefore, the lack of power required for the operation of this particular transponder is drawn from the electromagnetic field of reader. On the other hand, active transponders have a battery inside of them, which provides all, or part of the power required for the operation. Consequently, that electromagnetic field on the reader must be much weaker. This condition can substantially increase the communication range if the transponder is capable of detecting the weaker reader signal. Yet even an active RFID transponder is not able to generate high frequency signal on its own but can only modulate the reader's field in order to transmit data to the reader.

2.1 Frequencies and ranges of RFID systems

The most important differentiation criteria for RFID systems are the operating frequency of the reader, the physical coupling method, and the range of the system. Spectrum of frequencies, where RFID systems could operate is quite wide, ranging from 125 kHz longwave to 5,8 GHz in the microwave range. This spectrum is an unlicensed spectrum space, referred to as ISM, but the exact frequencies that constitute ISM may vary, depending on the regulations in different countries. The frequency bands must be selected carefully for applications because each one has its own advantages and disadvantages. The achievable range of the communication could vary from millimeters up to 100 meters, as is possible due to newest systems in microwave frequency range. As seen on the Table 1, the lower the frequency of the system is means shorter the communication range is.

Band	Commonly used frequency	Type of tag	Communication range		Allowed field strength transmission power
			Typical	Max.	
LF	125-134,2 kHz	Passive	20cm	100cm	72 dB μA/m max.
HF	13.56 MHz	Passive Semi-passive	10cm	1.5m	60 dB μA/m max.
UHF	433 MHz	Active	3m	10m	10-100 mW
	860 and 915 MHz	Active Passive	3m	15m	0,1-4 W
Microwave	2.4 and 5.8 GHz	Active Passive	3m	30m	0,5-4 W

Table 1: Categorizations of RFID tags by frequency - [5]

According to [6], which talks more about the frequency bands and will be used as a reference in this whole chapter, the low frequency range (LF) systems have low energy, which means they transmit data more slowly and their range is limited to a couple centimeters. The theoretical maximum of LF range is up to 100 centimeters but in real-life applications it is hardly possible. However, even though LF have a smaller range than higher frequencies they are more tolerant of obstacles, even moderately tolerant of small amounts of ferrous metal in the way. This means that LF tags can be easily read while attached to objects containing water, animal tissue, metal, wood, and liquids. By using near-field inductive coupling to obtain power and communicate, LF have the lowest data transfer rate among all the RFID frequencies and usually store a small amount of data. LF tags are used in access control, asset tracking, animal identification, automotive control (vehicle immobilizers) and healthcare. As website RFID4u states “The automotive industry is the largest user of them. For example, in an automobile vehicle immobilizer system, an LF tag is embedded inside the ignition key. When that key is used to start the car, an RFID interrogator placed around the key slot reads the tag ID. If the tag ID is correct, the car can be started. If the ID is incorrect or no tag is found, the car cannot start.” [6]

In theory, the high frequency range (HF) is considered to be all frequencies from 3 to 30 MHz but only the frequency of 13.56 MHz is used in the RFID applications. This frequency is now used worldwide for various RFID systems with the same power level. Like the LF tags, they also use near-field inductive coupling to obtain power and to communicate. The range of communication is again very similar to LF tags, but the theoretical maximum is a bit higher, ranging about 150 centimeters. Because of a shorter wavelength and having more energy, the read speed is much faster as well as having higher data rate compared to LF tags and could also store up to 4 Kb of data. HF RFID systems are used in a wide variety of applications including ticketing, contactless payments, tracking library books, patient flow tracking and general data transfer applications. Due to simple antenna design, HF tags are the cheaper option on the market. Price and absence of restrictions on the use of the HF frequency makes the HF tags the most widely used tags around the world.

In the ultra-high frequency spectrum (UHF), which ranges from 300 to 1000 MHz, only two frequency ranges are used for RFID applications and those are 433 MHz and 860–960 MHz. Up until this point, all of tags previously mentioned were passive tags but with the 433 MHz frequency, active tags are finally making the appearance. The 860–960 MHz range is used mostly for passive and semi-passive tags which use far-field radiative coupling, or backscatter coupling. With an even shorter wavelength comes even faster read speed and bigger communication range. With UHF tags, it is possible to communicate with the reader in ranges up to 15 meters with the typical range being around 2-3 meters. While this might look like a big advantage over smaller frequency systems, it also has a lot of disadvantages. The UHF tags cannot be easily read while attached to objects containing water and animal tissues because water absorbs very short UHF waves. Another disadvantage happens when attached to metal objects, because they easily get detuned and will not read properly. To improve their performance, UHF tags must be separated from the metal objects or objects with liquid.

There is a technology that allows RFID applications to work at the microwave frequency spectrum especially at 2,4 GHz and 5,8 GHz. Essentially, these systems work very similarly to the UHF systems with a range that could get up 30 meters, with typical ranges reaching around 3-5 meters. The highest range is possible to achieve with active transponders, because unlike the passive transponders, they use their own transmitter to communicate.

2.2 Physical and operating principles

The vast majority of RFID systems operate according to the principle of inductive coupling. Therefore, understanding the physical principles of magnetic phenomena is required. This chapter will analyze the magnetic field from the point of view of RFID.

2.2.1 Physical principles

As stated in [4], the read/write devices of inductively coupled RFID systems use short cylindrical coils or conductor loops as antennas to generate the magnetic alternating field. The magnitude of the magnetic field is described by the magnetic field strength – H. If one compares measurements in the center of the coil with measurement moved away along the coil axis (x-axis), one can observe that when moved away from the center, strength of field H will decrease, as the distance of x increases.

Also described by [4], a magnetic field and thus a magnetic flux Φ (the surface integral of the normal component of the magnetic field flux density B passing through that surface) will be generated around every conductor. This will be particularly intense if the conductor is in the form of loop (coil). Normally there are multiple N conduction loops in the same area with the same current flowing through them. Each of the loops contribute the same proportion of Φ to the total flux Ψ:

$$\Psi = \sum_N \Phi_N = N \cdot \Phi = \mathrm{N} \cdot \mu \cdot \mathrm{H} \cdot \mathrm{A} \tag{2.1}$$

Described by Finkenzeller, as visible on Figure 2.2, “if a second conductor loop 2 (area A2) is located in the vicinity of conductor loop 1 (area A1), through which a current is flowing. then this will be subject to a proportion of the total magnetic flux Φ flowing through A1. The two circuits are connected by this partial flux or coupling flux. The mutual inductance M_{21} of the conductor loop 2 in relation to conductor loop 1 is defined as the ratio of the partial flux ψ_{21} enclosed by conductor loop 2, to the current I1 in conductor loop 1.” [4]

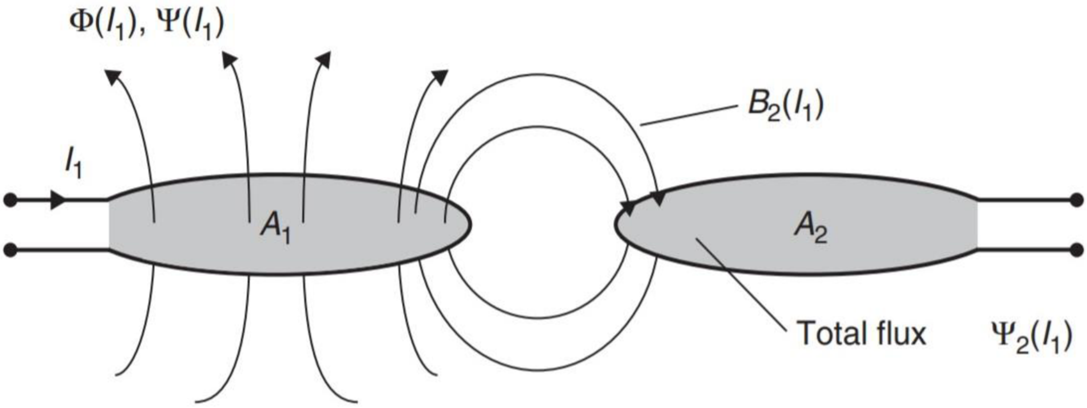


Figure 2.2: The definition of mutual inductance by the coupling of two coils – [4]

According to [4], described by Faraday's Law, any change to the magnetic flux generates an electric field. A Voltage is induced in the conductor loop of the transponder by time varying flux in the conductor loop of the RFID reader due to mutual inductance. This voltage is used to provide the power to the microchip of the passive tag. To significantly improve the efficiency of the circuit, a capacitor C is connected in parallel with the coil L to form parallel resonant circuit with resonant frequency:

$$\mathrm{f} = \frac{1}{2\pi\,\sqrt{L\cdot C}} \tag{2.2}$$

For LF transponders, chip capacitor is connected in parallel with the coil L to achieve the required resonant frequency. For HF transponders, typically the required capacitance is so low that it is provided be the input capacitance of the data carrier together with the parasitic capacitance of the coil.

While passive tags obtain their power supply from the voltage u_2, which is converted into direct current using a low loss bridge rectifier and then smoothed, active tags incorporate their own battery to provide the power supply to the data carrier. In these transponders, the voltage u_2 is generally only required as a 'wake up' signal. As soon as the certain limit of voltage u_2 is exceeds, tag switches into operating mode. After the transaction of the data with the reader, the transponder returns to its power saving mode – described in [4].

2.2.2 Operating principles

As the reference [4], this chapter is inspired from states, in contrast to 1-bit transponders, more advanced transponders have data storage capacity between a few bytes and 100 kilobytes. All this stored data needs to be transferred and it takes place according to one of two main procedures: full-duplex and half-duplex (Figure 2.3). "At frequencies below 30 MHz, half-duplex (HDX) is most often used with the load modulation procedure, either with or without a subcarrier, which involves very simple circuitry. The full-duplex (FDX) includes procedures in which data is transmitted from the transponder at a fraction of the frequency of the reader (subharmonic), or at a completely independent (enharmonic) frequency.” [4]

Load modulation that was previously mentioned in HDX procedure works on the principle of transformer-type coupling (the distance between the coils cannot exceed $\lambda/2\pi = 0{,}16\lambda$). When a resonant transponder is brought within the magnetic alternating field of the reader, it draws the energy from that magnetic field. The resulting feedback of the transponder on the reader’s antenna can be interpreted as transformed impedance Z_T. Change of voltage at the reader’s antenna is caused by switching a load resistor on and off at the transponder’s antenna, thus the change of the impedance Z_T. This has the effect of an amplitude modulation of the voltage U_L at the reader’s antenna coil. When data is transferred from the transponder to the reader, the timing with which the load resistor is switched on and off is controlled by that data. To reconstruct the data after the transfer, the voltage at the reader’s antenna must be rectified. This represents the demodulation of an amplitude modulated signal.

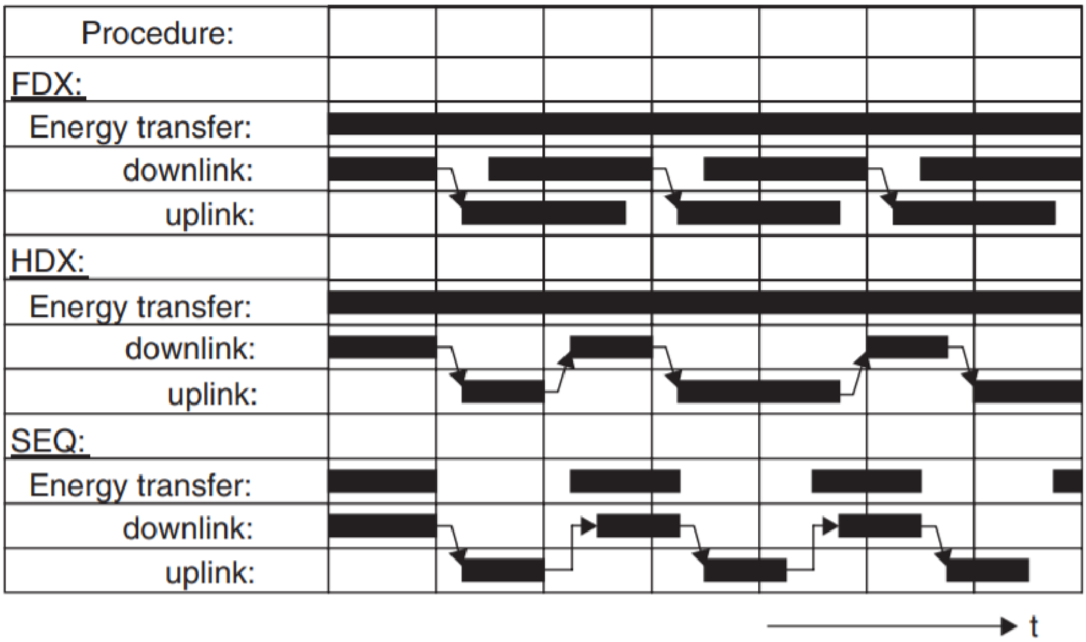


Figure 2.3: Comparison of Full-duplex and Half-duplex procedure – [4]

Caused by the weak coupling between the reader antenna and the transponder antenna, the voltage changes at the antenna of the reader that carry the useful signal are smaller by orders of magnitude than the output voltage of the reader. As Finkenzeller states, “If the load resistor in the transponder is switched on and off at a very high elementary frequency f_S, then two spectral lines are created at a distance of ± f_S around the transmission frequency of the reader f_{READER}, which can be easily detected. In the terminology of radio technology, the new elementary frequency is called a subcarrier.

Data transfer is by ASK, FSK or PSK modulation of the subcarrier in time with the data flow. This represents an amplitude modulation of the subcarrier.” [4]

As visible on the Figure 2.4, load modulation with a subcarrier creates two subcarrier modulation sidebands around the main operating frequency. These sidebands can be separated from the significantly stronger signal of the reader by bandpass filtering on one of the two frequencies $f_{READER} \pm f_S$. Once the subcarrier has been amplified, the signal is then simple to demodulate. The actual information is carried in the sidebands of the two subcarrier sidebands. Load modulation with subcarriers is mainly used in the frequency range 13.56 MHz. Typical subcarrier frequencies are 212 kHz, 424 kHz (e.g. ISO/IEC 15 693) and 848 kHz (e.g. ISO/IEC 14443), see [4].

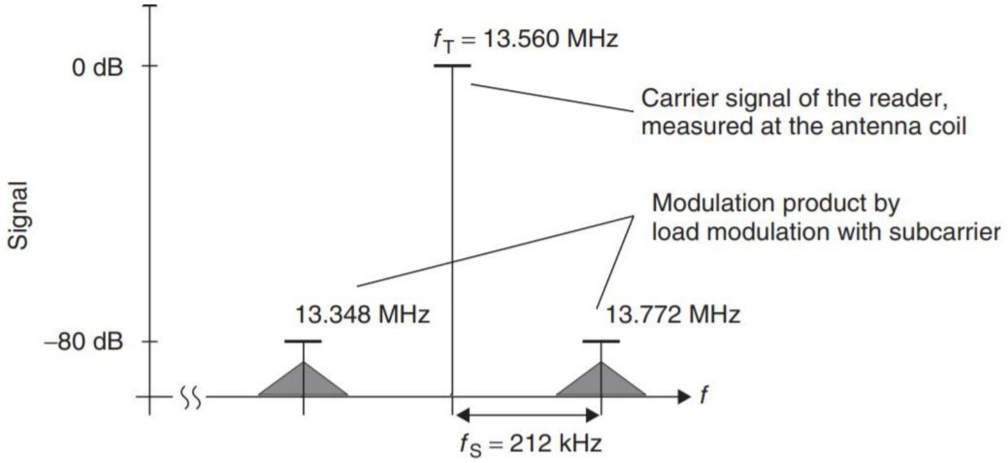


Figure 2.4: Load Modulation with Subcarrier – [4]

2.3 Security of RFID systems

Finkenzeller in [4] states that as well as any other telecommunication and information technology system, RFID systems are also vulnerable, with the biggest threat being the potential risk of being spied on or manipulated. In general, attacks may be directed at the transponder, reader, or RF interface between the transponder and the reader. They can be grouped into four attack types – according to the [4]:

- *Spying out*: The attacker tries to obtain unauthorized access to information and data of the active and passive file.
- *Deception*: The attacker tries to feed incorrect information into the RFID system in order to deceive the active party, i.e. the RFID system operator, or the passive party, i.e. the user of the RFID system.
- *Denial of service*: This kind of attack affects the availability of functions of the RFID system.
- *Protection of privacy*: The attacker considers the RFID system to be a threat to the privacy and tries to protect themselves with attacks on the RFID system.

When it comes to RFID systems, attacks on transponders are generally the easiest to perform. The most frequent attacks are a permanent destruction where the attacker destroys the antenna or microchip, so the transponder does not work anymore, or shielding where the attacker uses metal surfaces in order to shield a transponder from a reader's electromagnetic radiation. Both attacks could be done in a very effective way in just a matter of seconds. More advanced attacks on transponders are called spoofing and cloning, where the attacker has their own active reader, which activates the transit of the serial number of the transponder. With the knowledge of the serial number, the attacker can now build a transponder and clone the same serial number on it.

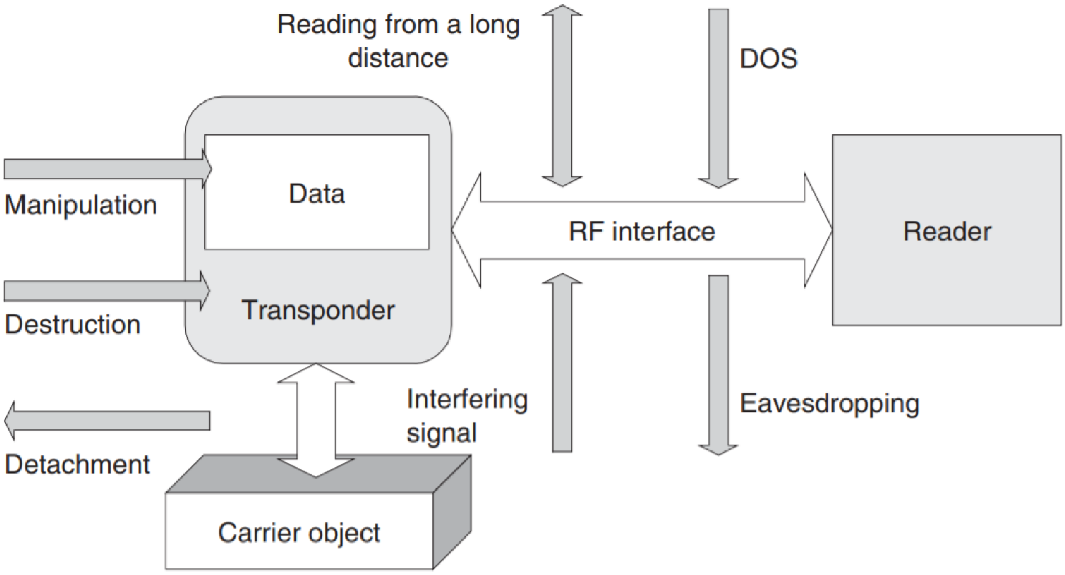


Figure 2.5: Overview of basic attacks on RFID systems - [4]

An attacker could also take an different approach and attack the RF interface. As all the communication is carried out via electromagnetic waves and the attacker does not require any physical access to the reader or transponder, this attack approach becomes very attractive. Another example is eavesdropping, in which the attacker intercepts a signal between a reader and transponder. In order to receive useful signals, radio receivers only need an antenna output voltage that is an order of magnitude lower. This generates probable cause that some communication may become compromised from a much greater distance.

Another simple method of attack is jamming, where data transfer becomes interrupted by an interfering signal. In order to be able to superimpose a reader's strong carrier signal distance, transmission power and antenna gain, or antenna diameter, have to correspond to at least the reader that is used. Ultimately, it is much easier for an attacker to focus on weak modulation sidebands that are generated by the transponder's load modulation, which transmits data from transponder to reader. An additional attack is called a relay attack, where the attacker can intentionally extend the range between the reader and transponder by insinuating a transmission device (relay). Two different components that are linked via radio communication are required to successfully carry out a relay attack. One component receives the reader's signals and generates a load modulation in order to communicate to the reader (simulating a transponder) which is located close to the reader. The second component consists of a transmitter which supplies a transponder with the power required for its normal operation as well as demodulates a load modulation of the transponder (simulating a reader) which is located close to the transponder. For details, see [4].

2.3.1 Protection

With so many possible threats and attacks on RFID systems, such as ticketing and payment systems, they require a certain level of protection. It is necessary to protect and defend themselves by cryptographic measures. For example, mutual authentication between the reader and transponder is based upon the principle of a three-pass mutual authentication. In this procedure, described by Finkenzeller in [4], all transponders and receivers which are included in the system are in possession of the same secret cryptological key K. Random numbers R_A and R_B are generated and sent out. Using a secret key, key algorithm, and random numbers, tokens 1 and 2 are made and sent from the transponder to the reader and vice versa. Tokens are than decrypted and numbers R'_A and R'_B are compared with previously transmitted R_A and R_B. If both correspond, then the reader is satisfied that the common key has been proven. The transponder and reader have thus ascertained that they belong to the same system and communication is legitimized. A significant improvement on the authentication procedure described can be achieved by securing each transponder with a different cryptological key. A key K_x is calculated using a cryptological algorithm and master key. Each transponder thus receives a key linked to its own ID number and the master key.

Finkenzeller states, “cryptological procedures are used to protect against both passive and active attacks. To achieve this, the transmitted data may be encrypted prior to transmission so that a potential attacker can no longer draw conclusions about the actual content of the message. The transmission data is transformed into cipher data using a secret key K and a cryptographical algorithm. Without knowing the encryption algorithm and the secret key K a potential attacker is unable to interpret the recorded data. If each character is individually encrypted prior to transmission, the procedure is known as sequential ciphering (or stream ciphering).“ [4]

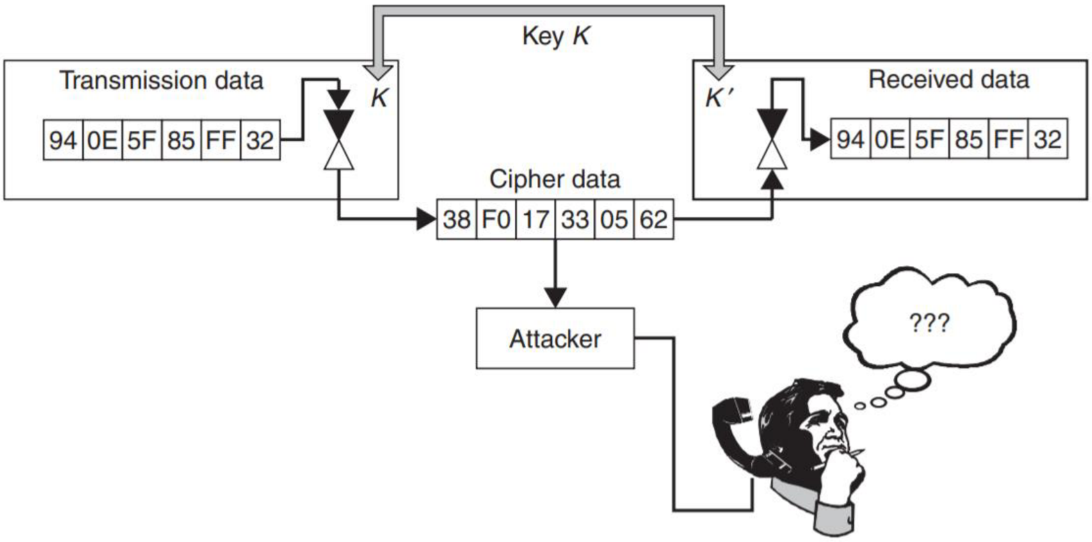


Figure 2.6: Communication process with data encryption – [4]

2.4 Standardization

Standardization is the process of implementing and developing technical standards based on the consensus of different parties that include firms, users, interest groups, standards organizations, and governments. The development of standards is the responsibility of the technical committee of standardization institutes (ANSI – USA, DIN – Germany). ISO – International organization for standardization, is a union, which consist of numerous committees, working groups, and regularly contributes to the development of RFID. There are various groups of standards which discuss RFID systems, but the most important group of ISO standards for this research is contactless smart cards. Information about both standards in this chapter are mainly based on [4].

2.4.1 ISO/IEC 14443 Type A and B

Standard ISO/IEC 14443, also called 'Identification cards – Proximity integrated circuit cards' mainly talks about the operating method and parameters of contactless smart cards. Those are contactless proximity-coupling smart cards with an estimated range of 7 to 15 cm, such as those used in the field of ticketing and access cards. According to [4], the standard comprises the following parts:

- Part 1: Physical characteristics.
- Part 2: Radio frequency power and signal interface.
- Part 3: Initialization and anti-collision
- Part 4: Transmission protocols

2.4.1.1 Physical characteristics

"First part of the standard defines the mechanical properties of the smart cards. The dimensions correspond with the values specified in ISO/IEC 7810, i.e. 85.72 × 54.03

× 0.76 mm ± tolerances. Furthermore, this part of the standard also includes notes on the testing of the dynamic bending stress and dynamic torsion stress, plus irradiation with UV, X-ray and electromagnetic radiation.” [4]

2.4.1.2 Radio frequency interface

At a frequency of 13.56 MHz, magnetic alternating field of a reader providing the power required for operation of inductively coupled proximity cards. The range in which the magnetic field generated by the reader must be is 1.5 A/m ≤ H ≤ 7.5 A/m. Described by Finkenzeller, „Unfortunately, it was not possible to come to agreement for the common communication interface in the development of this standard. For this reason, two completely different procedures for the data transfer between reader and proximity-coupling smart card have found a place in ISO/IEC 14443 – Type A and Type B“ [4]. Comparison of both types is described as follows:

PCD → PICC	TYPE A	TYPE B
Modulation	ASK 100%	ASK 10%
Bit coding	Modified Miller code	NRZ code
Synchronization	At bit level (start-of-frame, end-of-frame marks)	1 start and 1 stop bit per byte
Baud rate	106 kBd	106 kBd

Table 2: Data transfer from reader to transponder – [4]

PICC → PCD	TYPE A	TYPE B
Modulation	Load modulation with subcarrier 847 kHz, ASK modulated	Load modulation with subcarrier 847 kHz, BPSK modulated
Bit coding	Manchester code	NRZ code
Synchronization	1 bit frame synchronization (start-of-frame, end-of-frame marks)	1 start and 1 stop bit per byte
Baud rate	106 kBd	106 kBd

Table 3: Data transfer from transponder to reader – [4]

2.4.1.3 Initialization and Anti-collision

When a desired proximity-coupling smart card enters the interrogation field of a reader, then a communication must be established between the reader and smart card. Although, the fact that the reader may already be in communication with another card because there may be more than one smart card within the same area must be considered.

Therefore, part three of the standard describes the structure of the protocol frames from the basic elements (data bit, start-of-frame and end-of-frame marks) to the anti-collision procedure used for the selection of an individual card. Since different modulation procedure for Type A and Type B also requires a different frame structure and anti-collision procedure there is a difference, which is described at [4].

2.4.1.4 Transmission Protocols

Fourth part of the standard describes the situation after the relationship between the reader and a smart card has been established, thus commands for reading, writing and the processing of data can be sent to the card. Mainly, it goes over the structure of the data protocol and the processing of transmission errors, so that data can be transferred seamlessly. In the Type A card, additional information must be transferred that serve for the configuration of the protocol because card and reader may have different properties. In Type B card, this information is transferred during the anti-collision process (ATQB) so in this case, the protocol can be immediately started.

2.4.2 Mifare classic

As official website [7] describes, MIFARE® is NXP's well-known brand for a wide range of contactless IC products with a typical read/write distance of 10 cm used in more than 40 different applications worldwide. MIFARE products comply with the international standard ISO/IEC 14443, which is used in more than 80% of all contactless smart cards today. Within the MIFARE product families, backward compatibility ensures that the existing infrastructure can be smoothly upgraded to high security and feature levels. MIFARE Classic® is s series of contactless smart card IC chips operating in the 13.56 MHZ frequency range with read/write capability. It makes use of a proprietary protocol compliant to parts 1–3 of ISO/IEC 14443 Type A, and NXP proprietary security protocol for authentication and ciphering.

The MIFARE Classic can be made in two variants: 1K or 4K. According to [8], the 1K variant offers 1,024 bytes of data storage, which is split into 16 sectors. Each sector is protected by two different programmable keys, called A and B, to allow operations such as reading, writing, increasing value blocks. The 4K variant offers 4,096 bytes split into 40 sectors, of which 32 are same size as in the 1K variant and 8 that are quadruple size sectors. The very first 16 bytes are typically read only and contain the serial number of the card and certain other manufacturer data. Also, in both IC variants, different 16 bytes per sector are reserved for the keys A and B and access conditions. These 16 bytes than cannot normally be used for user data. That brings the net storage capacity of these cards down to 752 bytes for MIFARE Classic with 1K memory and 3,440 bytes for MIFARE Classic with 4K memory. -+90.

2.4.3 ISO/IEC 15693

The standard ISO/IEC 15693 also called 'Identification cards – contactless integrated circuit cards – Vicinity Cards' mainly talks about the functioning and operating parameters of contactless vicinity-coupling smart cards. These are smart cards with estimated range of up to 1 m. Cheap memory modules with simple state machines are typically used in the data carriers used in these smart cards. The standard, according to the [4] is made up of the following parts:

- Part 1: Physical characteristics
- Part 2: Air interface and initialization
- Part 3: Anti-collision and transmission protocol

2.4.3.1 Physical characteristics

"Part 1 of the standard defines the mechanical properties of proximity-coupling smart cards. The dimensions of the smart card correspond with those specified in ISO/IEC 7810, i.e. 85.72 × 54.03 × 0.76 mm ± tolerances. Furthermore, this part of the standard includes additional notes for the testing, which is same as ISO/IEC 14443." [4]

2.4.3.2 Air interface and initialization

Operating frequency generated by reader to transfer power is again 13.56 MHz. This time the range in which the magnetic field generated by the reader must be in 115 mA/m $\leq$ H $\leq$ 7.5 A/m. Thus, it is automatically the case for the interrogation field strength of a proximity-coupling smart card which is Hmin $\leq$ 115 mA/m.

According to [4] vicinity cards use both 10% ASK and 100% ASK modulation for the data transfer from a reader to a smart card. Regardless of the earlier mentioned type of modulation, one of two different coding procedures can be used: a '1 of 256' code or a '1 of 4' code. Vicinity smart cards must support both modulation and coding procedures at the same time. For example, 10% ASK modulation combined with a '1 of 256' coding should be preferred in the use of long-distance mode. Full exploitation of the acceptable magnetic field strength for the power supply of the card is allowed by the lower field strength of the modulation sidebands in comparison to the field strength of the 13.56 MHz carrier signal in this combination. By contrast, 100% ASK modulation combined with a '1 of 4' coding in readers should be preferred in the use with reduced range or even shielded readers.

3. NEAR-FIELD COMMUNICATIONS (NFC)

Near-field communication is a wireless data interface between devices, similar to Infrared or the well-known Bluetooth which has several characteristics that are of interest in relation to RFID systems. NFC describes a technology which can be used for contactless exchange of data over short distances. According to Finkenzeller, "Data transmission between two NFC interfaces utilizes high-frequency magnetic alternating fields in the frequency range of 13.56 MHz. The maximum communication range typical for NFC data transmission is 20 cm because the respective communication counterpart is located in the near-field of the transmitter antenna, therefore, the communication is called near-field communication." [4]

For communication between two NFC devices, each NFC interface is assigned a different function, one being an NFC initiator and other being an NFC target. Communication is always introduced by the NFC initiator who also controls the data exchanges. The target device is the one that responds to the request from the initiator and accepts the communication with the initiator to happen. In addition, NFC communication is divided between two different modes of operation: the active and the passive mode.

3.1 Modes of operation

- **Passive mode:**

Both described by the [9], in the passive mode of operation, only one NFC device generates a RF field. In this sense, it is active and always plays the role of initiator. The other device is passive, and it always plays the role of target. The initiator induces a magnetic alternating field for transmitting data to the target. The field's amplitude is modulated in line with the pulse of the data to be transmitted (ASK modulation). However, after having transmitted a data block, the field is not interrupted, but continues to be emitted in an unmodulated way. The NFC target is now able to transmit data to the NFC initiator by generating a load modulation.

- **Active mode**

In the active mode of operation, both NFC devices generate a RF electromagnetic field. One of the NFC interfaces activates its transmitter and thus works as the initiator. The high-frequency current that flows in the antenna induces an alternating magnetic field H which spreads around the antenna loop. Part of the induced magnetic field moves through the antenna loop of the other NFC interface which is located close by. A voltage U is then induced in the antenna loop and can be detected by the receiver of the other NFC interface. If the NFC interface receives signals and the corresponding commands of an initiator, the NFC interface automatically adopts the roll of a target. Each side transmits data using an ASK (amplitude shift keying) modulation scheme. Compared to passive mode, larger operating distances, up to 1 m and High data transfer rates, up to 6.78 Mbit/s are reached.

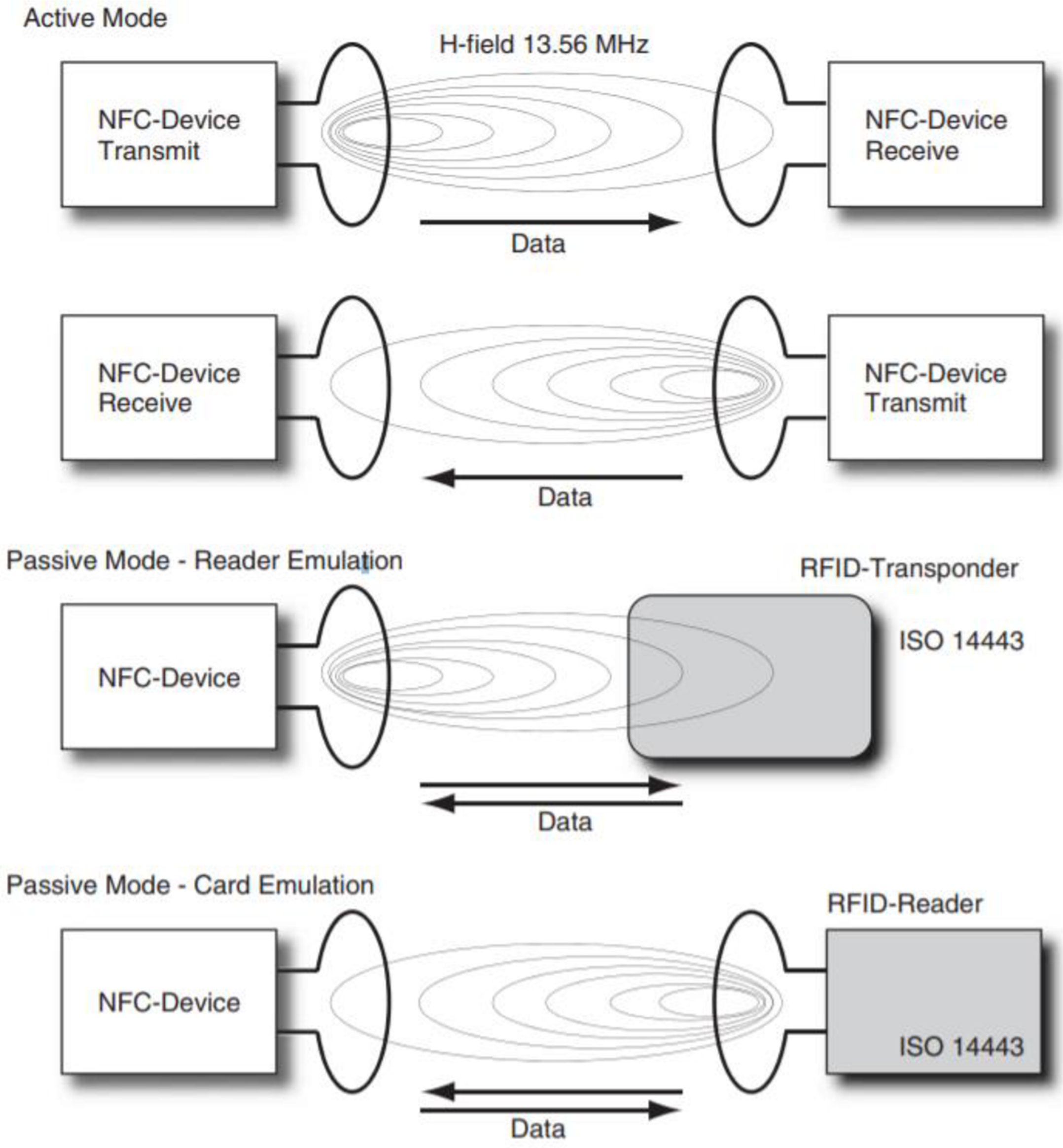


Figure 3.1: Overview of NFC modes of operation – [4]

3.2 NFC tag types

The NFC Forum defines four types of NFC tags. An additional fifth type is related with NFC-V technology and has just recently been included in the Forum specifications. These NFC tag type formats are based on ISO/IEC 14443 Types A and B and Sony FeliCa, which conforms to ISO 18092. There are many design and manufacturing considerations to be taken into account for NFC tags. They are intended to be manufactured for very low cost in very large quantities, while maintaining their performance. From the definitions of the different NFC tag types, as can be seen on Table 4, type 1 and 2 tags are very different to type 3 and 4 tags. It is expected that there is likely to be very little overlap in applications of Tag types 1 / 2 and types 3 / 4. According to the [9]:

- **Tag Type 1**

  The type-1 tag is compliant with ISO/IEC 14443A specification. It is read-write capable, and it may be user-configurable to read-only mode. The memory size ranges from 93 bytes to 2 Kbytes and the communication speed or data rate is of 106 kbit/s. Type-1 tag does not support anti-collision mechanism.

- **Tag Type 2**

  The type-2 tag is compliant with ISO/IEC 14443A specification. It is read-write-capable, and it may be user-configurable to read-only mode. The memory size ranges from 48 bytes to 2 Kbytes and the communication speed or data rate is of 106 kbit/s. Type-2 tag supports anti-collision mechanism.

- **Tag Type 3**

  The type-3 tag is compliant with ISO/IEC 18092 and JIS X 6319-4 standards, except for encryption and authentication which are not supported. Even if featuring a read / write capability, a tag of type 3 can be set to read-only mode. Specific service equipment may be used to enable re-writing of type-3 tag data in the field. Type-3 tag contains two Kbytes of memory. The data rate is 212 kbit/s or 424 kbit/s. Type-3 tag supports anti-collision mechanism.

- **Tag Type 4**

  Type-4 tag complies with both A and B versions of ISO/IEC 14443 standard. The type-4 tag is factory-set to read-only mode and specific service equipment is required for updating its data. Type-4 tag contains up to 32 Kbytes of memory, supports 106 kbit/s, 212 kbit/s and 424 kbit/s data rates, as well as the anti-collision mechanism.

- **Tag Type 5**

  Type-5 tag (NFC-V) has recently been adopted by NFC Forum specification. It relies on ISO/IEC 15693 standard, contains more than 64 Kbytes of memory, supports 26.48 kbit/s data rate, and has anti-collision mechanism.

Property	Type 1	Type 2	Type 3	Type 4	Type 5
Standard	ISO/IEC 14443A	ISO/IEC 14443A	ISO/IEC 18092 JIS X 6319-4 FELICIA	ISO/IEC 14443A ISO/IEC 14443B	ISO/IEC 15693
Memory	96 to 2 Kbytes	48 to 2 Kbytes	2 Kbytes	32 Kbytes	64 Kbytes
Data rate	106 kbit/s	106 kbit/s	212 kbit/s 424 kbit/s	106 kbit/s 212 kbit/s 424 kbit/s	26.48 kbit/s
Capability	Read, Re-write Read-only	Read, Re-write Read-only	Read, Re-write Read-only	Read, Re-write Read-only	Read, Re-write Read-only
Anti-collision	No	Yes	Yes	Yes	Yes
Notes	Simple, cost effective	-	Higher cost, complex	-	Vicinity area

Table 4: Overview of NFC tag types – [9]

3.3 Data transfer

Similarly, to the NFC Tag types, [9] also talks about data transfer. To ensure data transfer between the NFC initiator and target, data signaling, and data coding are used. Different types of NFC (NFC-A,NFC-B, NFC-V) may use different techniques or values. Tables 5 and 6 below give a summary of different data transfer diagrams.

PCD → PICC	NFC-A	NFC-B	NFC-V
Frequency	13.56 MHz	13.56 MHz	13.56 MHz
Data signaling	100% ASK Modulation	10% ASK Modulation	10% or 100% ASK Modulation
Bit coding	Modified Miller	NRZ	1/4 PPM or 1/256 PPM
Data rate	106 kbit/s typ. up to 424 kbit/s	106 kbit/s typ. up to 424 kbit/s	26.48 kbit/s or 1.65 kbit/s

Table 5: Data transfer from reader to transponder – [9]

STMicroelectronics describes, “The goal of the data signaling is to reliably distinguish binary states. The goal of data coding is to organize binary states in a way to form a binary data stream of logical ones and zeros that can be reliably interpreted by the data receiving side. For data signaling, techniques like direct and indirect RF field modulation are used. For binary data stream, bit-coding into ones and zeros is done using know data coding methods.” [9]

PICC → PCD	NFC-A	NFC-B	NFC-V
Data signaling	ASK load modulation, OOK of sub-carrier	ASK load modulation, BPSK of sub-carrier	ASK load modulation, OOK/FSK of sub-carrier
Sub-carrier	848 kHz	848 kHz	424/848 kHz
Bit coding	Manchester	NRZ	Manchester
Data rate	106 kbit/s typ. up to 424 kbit/s	106 kbit/s typ. up to 424 kbit/s	OOK: 6.62 / 26.48 kbit/s FSK: 6.67 / 26.69 kbit/s

Table 6: Data transfer from transponder to reader – [9]

3.4 Standardization of NFC

As well as RFID technology, NFC follows worldwide accepted standards issued by International organization for standardization (ISO), which should every designer follow.

3.4.1 ISO/IEC 18092 or ECMA-340 (NFCIP-1)

According to the [9], this standard defines communication modes for NFC interface and protocol (NFCIP-1), using inductive-coupled devices operating at the center frequency of 13.56 MHz, for interconnection of computer peripherals. ISO/IEC 18092 also defines the active and passive operating modes of NFCIP-1 to set up a communication network using NFC devices for networked products and for consumer equipment.

In particular, it specifies modulation schemes, coding, transfer speeds and frame format of the RF interface. It also describes initialization schemes and conditions required for data anti-collision control during the initialization, as well as transport protocol including protocol activation and data exchange methods. ISO/IEC 18092 is aligned with ISO/IEC 13157-1:2010 (NFCIP-1 security services and protocol) and conforms with ISO/IEC 14443-2, ISO/IEC 14443-3, and ISO/IEC 14443-4, as well as with ISO/IEC 15693-1, ISO/IEC 15693-2, and ISO/IEC 15693-3.

3.4.2 ISO/IEC 21481 or ECMA-352 (NFCIP-2)

Described in the [10], this Standard specifies the communication mode selection mechanism, designed not to disturb any ongoing communication at 13.56 MHz, for devices implementing ECMA-340, ISO/IEC 14443 or ISO/IEC 15693. This Standard requires implementations to enter the selected communication mode as specified in the respective standard. The communication mode specifications, however, are outside the scope of this Standard.

The NFCIP-2 Standard specifies the mechanism to detect and select one communication mode out of those three possible communication modes. Furthermore, NFCIP-2 requires that subsequent behavior be as specified in the standard specifying the selected communication mode.

In the following Figure 3.2, it is possible to see the map of all NFC related standards, tag types, data transfer modes etc. NFC forum defined tags make individual columns, where it is possible to see which international standards it uses in different layers like physical characteristics, anti-collision protocols etc. It is a nice summary made by ST that shows, all the connections in the NFC technology and discrediting possible questions about what type of standard is certain tag type uses.

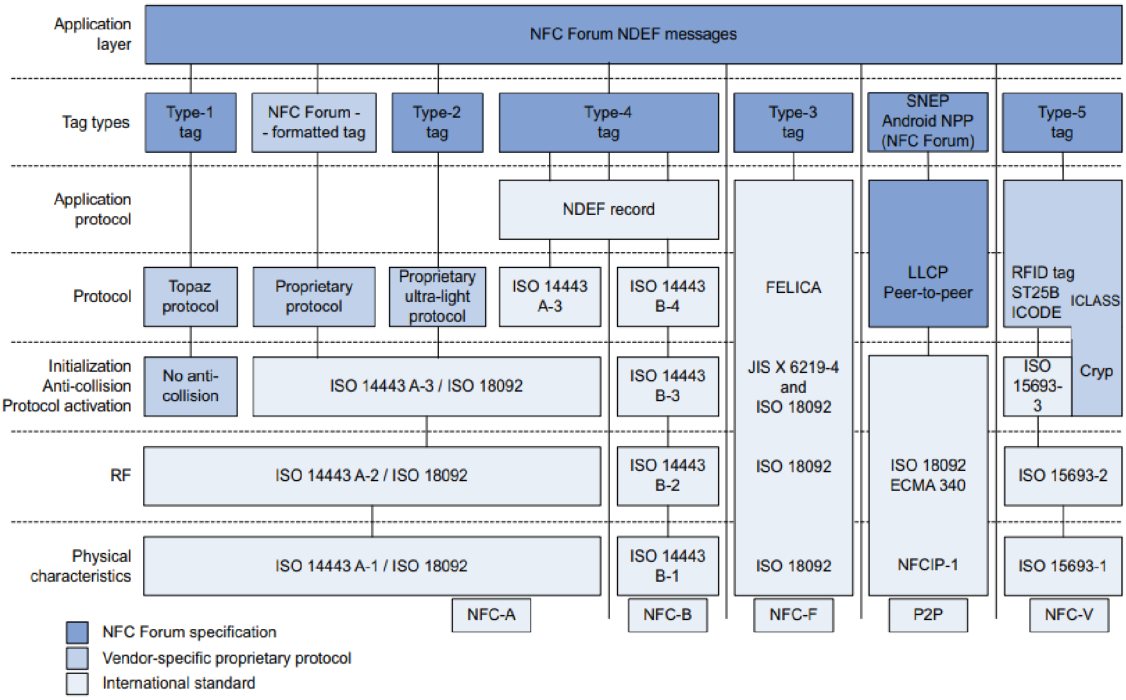


Figure 3.2: Map of NFC-related standards and specifications [9]

4. TRANSCEIVERS FOR 13.56 MHZ BAND

A transceiver is a device that is able to both transmit and receive information through a transmission medium. It is a combination of a transmitter and a receiver, hence the name transceiver. In this chapter, we will go over the three most common transceivers used in the 13.56 MHz frequency band for RFID/NFC applications. They are all made by different brands, so we are able to compare their main characteristics.

4.1 CR95HF – STMicroelectronics

According to the datasheet [11], the CR95HF is an integrated transceiver IC for contactless applications from ST. It embeds the Analog Front End for 13.56 MHz Air Interface. The CR95HF manages the frame coding and decoding in Reader mode for standard applications such as NFC, proximity and vicinity standards. This transceiver supports ISO/IEC 14443 A and B, ISO/IEC 15693 (single or double subcarrier) and ISO/IEC 18092 protocols. It supports reader and writer mode for ISO/IEC 14443-3 Type A and B cards and tags, ISO/IEC 15693, and ISO/IEC 18000-3M1 tags and NFC Forum tag types 1, 2, 3 and 4. It features Optimized power management and Tag Detection mode as its key hardware features. It is housed in 32-pin VFQFPN (5 x 5 mm) ECOPACK package. Communication interfaces with a Host Controller supported by this transceiver are SPI and UART.

4.2 TRF7970A – Texas Instruments

Described in the datasheet [12], the TRF7970A device is an integrated analog front end and multiprotocol data-framing device by Texas Instruments made for a 13.56-MHz NFC/RFID system supporting all three NFC operation modes – reader/writer, peer-to-peer, and card emulation according to ISO/IEC 14443 A and B, Sony FeliCa, ISO/IEC 15693, NFCIP-1 (ISO/IEC 18092), and NFCIP-2 (ISO/IEC 21481). Built-in programming options make the device suitable for a wide range of applications for NFC, proximity, and vicinity identification systems. The TRF7970A device supports data rates up to 848 kbps with all framing and synchronization tasks for the ISO protocols onboard. It also supports reader and writer mode for NFC Forum tag types 1, 2, 3, 4, and 5. Other standards and even custom protocols can be implemented by using one of the direct modes the device offers. These direct modes let the user fully control and gain access to the raw subcarrier data or the unframed, but already ISO-formatted, data and the associated clock signal. It is housed in 32-pin QFN (5 x 5 mm) package. Communication interfaces with a Host Controller supported by this transceiver is only SPI.

4.3 PN532 – NXP

According to [13], the PN532 is a highly integrated transceiver module for contactless communication at 13.56 MHz based on the 80C51 microcontroller core by NXP. It supports 6 different operating modes: ISO/IEC 14443A/MIFARE Reader/Writer, FeliCa Reader/Writer, ISO/IEC 14443B Reader/Writer, ISO/IEC 14443A/MIFARE Card MIFARE Classic 1K or MIFARE Classic 4K card emulation mode, FeliCa Card emulation and ISO/IEC 18092, ECMA 340 Peer-to-Peer. The PN532 implements a demodulator and decoder for signals from ISO/IEC 14443A/MIFARE compatible cards and transponders, FeliCa coded signals and MIFARE Classic 1K or MIFARE Classic 4K cards. It also handles the complete ISO/IEC 14443A framing and error detection. The PN532 transceiver can be connected to an external antenna for Reader/Writer or Card/PICC modes, without any additional active component. It is housed in 40-pin HVQFN (6x6 mm) package. Communication interfaces with a Host Controller supported by this transceiver are I2C, SPI and UART.

	CR95HF	TRF7970A	PN532
Supported standards	ISO/IEC 14443 A/B ISO/IEC 15693, ISO/IEC 18092	ISO/IEC 14443 A/B ISO/IEC 15693, ISO/IEC 18092	ISO/IEC 14443 A/B ISO/IEC 18092
Supported NFC forum types	1, 2, 3, 4	1, 2, 3, 4, 5	1, 2, 3, 4
Package	32-pin VFQFPN	32-pin QFN	40-pin HVQFN
Communication interfaces	UART, SPI	SPI	UART, SPI, I2C
Unique features	Tag detection mode	Custom protocol implementation	I2C communication

Table 7: Comparison table of different transceivers and their main characteristics

In conclusion, as also indicated on Table 7, it is plausible that transceivers from different companies do not showcase major differences. Each of the transceivers have something extra which makes it unique in comparison to the other two. Thus, it ultimately comes down to the application, in which the transceiver will be used. For example, if the need for the communication is I2C, only the PN532 integrated circuit is capable of doing so. But, if custom protocols need to be implemented, then the TRF7970A integrated circuit is the best candidate out of these three. In the case of CR95HF, this model has a tag detection mode which is unique among these three transceivers. This concept of varying utilities for each transceiver can become continuous, as stated above each possesses the ability to hold individualistic tendencies.

5. TESTING OF TRANSCEIVER CR95HF

Out of the three transceivers mentioned earlier, the aim of this thesis is to focus on integrated circuit CR95HF made by STMicroelectronics. This particular company is known for making microcontrollers, discovery kits, and various separately sold integrated circuits. The CR95HF integrated circuit is part of their ST25-NFC family, which contains many other kits and parts that are made for the NFC technology. During semestral project, microcontroller STM32F030, with expansion board X-NUCLEO-NFC03 was chosen to test out the functions of the integrated circuit. Most importantly, testing programing capabilities of the transceiver and its functionality. Because of this decision, a code that will read an UID of the transponder and send it over the communication interface to the host computer must be made. Same program will be used later, and built upon in master's thesis section.

5.1 Microcontroller and expansion board

The center of the setup used for testing is made by microcontroller STM32F030. This particular microcontroller is made with 64 pin Arduino style connectors. It is a base line MCU with Arm Cortex-M0 core clocked at 48 MHz, high-speed embedded 64 Kb of flash memory, 8 Kb of SRAM and an extensive range of enhanced peripherals and inputs/outputs. The main purpose of the MCU in this setup is to redirect the communication between the host computer and transceiver and back. Since the MCU is connected to the host computer, it will receive the input commands and send them to the CR95HF integrated circuit which is processed; then, a response is sent back to the MCU which then sends it to the host computer. It also provides power to the expansion board, controls the output commands of when the LEDs should light up, and stores the code that is executed when the command from user comes.

Expansion board X-NUCLEO-NFC03 is the board that contains the CR95HF integrated circuit and an antenna. It is in charge of the NFC part in this setup and could read and write tags, decode the messages contained in the tags, and send the information further. It contains output pins for UART and SPI communications and four LEDs that could be programmed to light up when there is a new reading of the transponder. Size of the antenna is 47 mm x 34 mm, designed with inductance of roughly 1.15 µH. Parameters of this antenna make it a good compromise between reading distance and communication with various ISO standards.

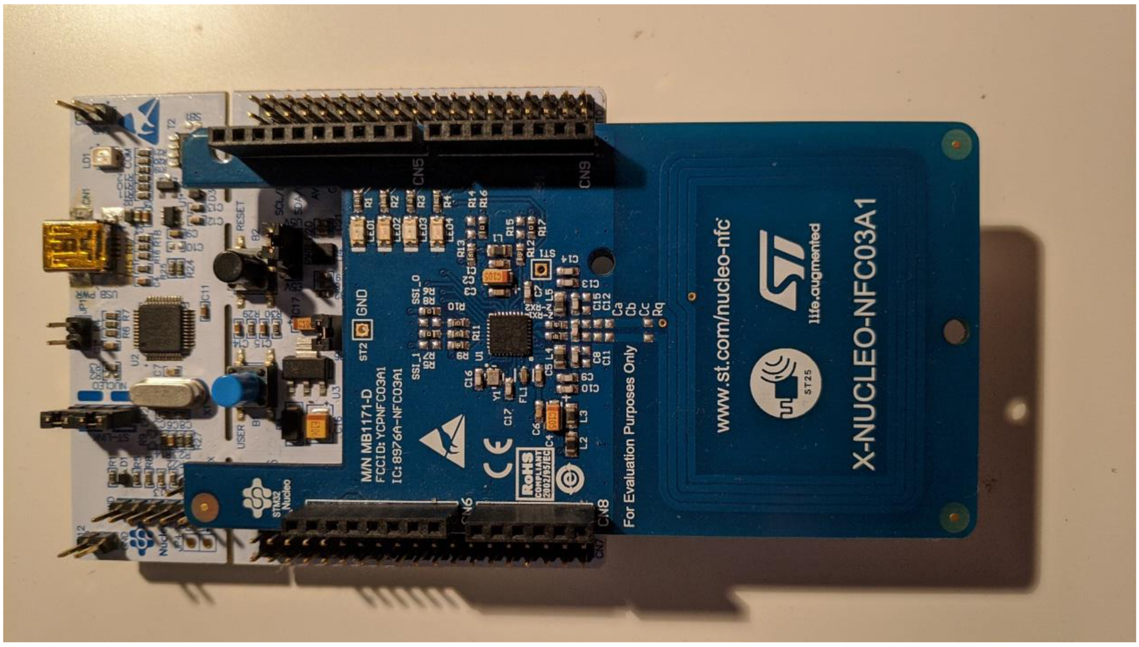


Figure 5.1: Hardware setup

5.2 Conclusion of testing

In the Figure 5.1, it is possible the see the setup used for testing the functions of CR95HF transceiver. The possible reading distance of the Expansion board X-NUCLEO-NFC03 and its antenna, maximum reading distance achieved was approximately 20.7 millimeters when using school ISIC card based on Mifare Classic and ISO/IEC 14443A standards. As for programming capabilities, programming interface called STM32CubeIDE made by STMicroelectronics was used. This interface makes working with their products more straightforward. In this interface, one can specifically pick on a microcontroller board in which the project will be made, thus it will automatically set up the program to work with the picked board. Sample firmware for demonstration and operation of reading RFID tags based on ISO/IEC 14443 standard was successfully made. This program will be built upon and described in its own chapter later.

6. CONNECTION DESIGN

The following topic describes the connection design for the wiring diagram and printed circuit board made in this project. It will go over the design and describe the creative process of designing it. For the construction of the wiring diagram, and later on designing the printed circuit board layout, primarily a program Eagle made by Autodesk was used.

The general idea behind creating the reader was to create a Arduino Shield like board equipped with a Arduino style connectors and designed with multiple different antennas, which could be easily exchanged. The information that the reader receives from the RFID tag would then be visible on a small display and as well as sent over UART to the user’s computer to be displayed in serial terminal. Along with this, multiple LEDs and buzzer are implemented to create a visible and audible response of tag detection.

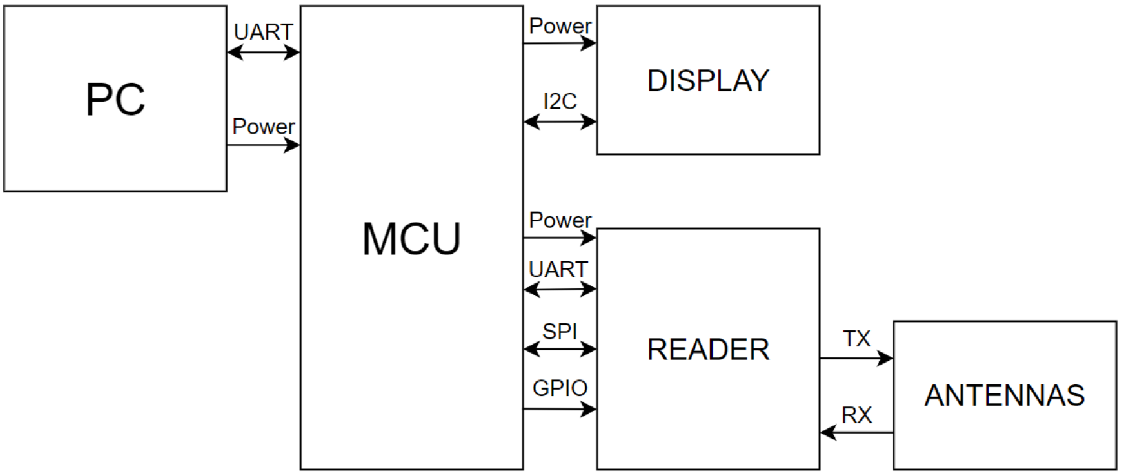


Figure 6.1: Hierarchical schematic design

In Figure 6.1, shown above, is it possible to observe a hierarchical schematic design for project. It contains all of the necessary blocks used in the design.

6.1 Microcontroller

The MCU block represents the microcontroller board. Any microcontroller board could be used, but the boards with classic Arduino Uno style connectors have an advantage, as the designed reader board could simply and easily be connected on top of them. For the purpose of this project, development board NUCLEO-F030R8 with the microcontroller STM32F030 made by the STMicroelectronics was chosen (This board was previously used in Chapter 5 for testing purposes).

6.2 Display

To ensure that a user can view the basic information about the RFID tag, without constantly having to use a computer, it was decided to implement a small display. For this purpose, a 1.54" OLED display with the resolution of 128x64 and I2C connectivity was used. This display works on a SSD1309, single-chip CMOS OLED/PLED driver with controller for organic light emitting diode dot-matrix graphic display system. [15]

6.3 Antennas

As mentioned before, all antennas are going to differ and be interchangeable. As a result of different parameters, each antenna will have its own and unique inductance value, therefore, each antenna will have its own impedance matching circuitry. Figure 6.2 shows the basic schematic design of all the antenna boards. It is shown that each board contains six capacitors, which allows for the purpose of impedance matching. Note, that not all six capacitors necessarily have to be used, but this design serves the purpose of matching the calculated values with the real world components.

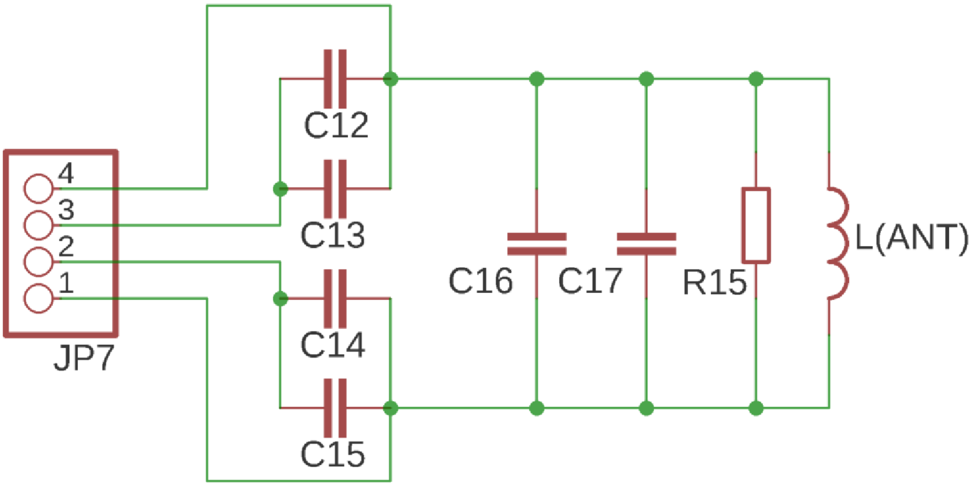


Figure 6.2: Schematic of antenna board

6.4 Reader board

The center and most important part in designing the prototype of the RFID reader is a Arduino shield like board, containing all of the necessary components that will carry out the RFID communication. For this purpose, as stated in the previous chapters, the transceiver CR95HF made by STMicroelectronics is used. The schematic of this board can be seen on the next page (Figure 6.3). It contains Arduino style connectors through which the reader board is powered, provides necessary communication interfaces for both CR95HF and display and also provides connections to GPIO pins (General purpose input output) on the microcontroller. All LEDs as well as buzzer and button are connected to the GPIO pins that can be programmed to toggle their outputs according to application.

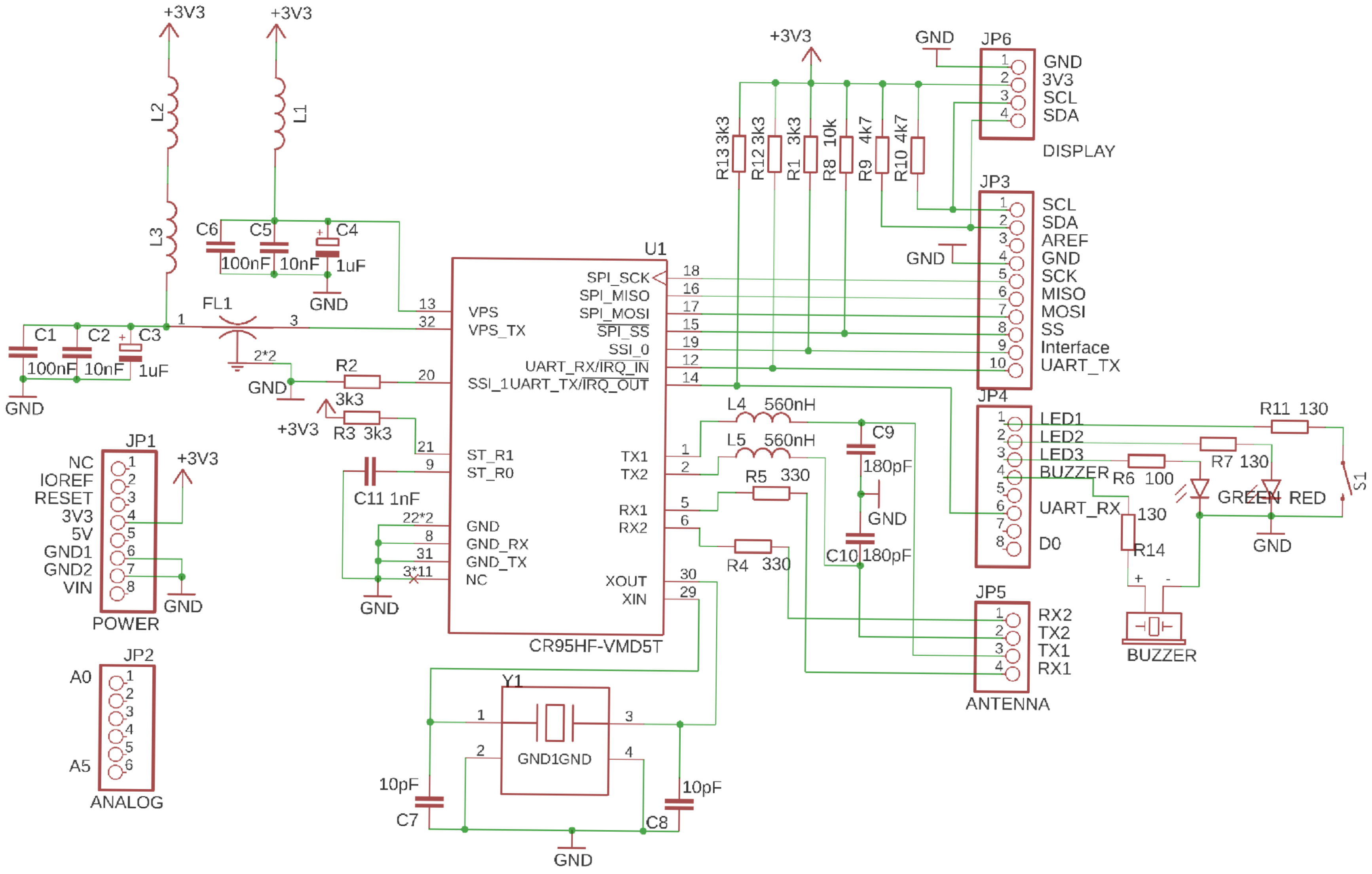


Figure 6.3: Schematic of reader board

6.5 Printed Circuit Board layout for Reader board

Printed circuit board or PCB was also designed in the Eagle, which is made by Autodesk. It is a two layer circuit board designed to use mostly surface-mount technology (SMT) components. Both TOP and BOTTOM layers have spilled copper over them to serve as a ground plate (GND). Trace width used in the majority of the conductive traces was 0.4 mm. Drill holes, used as a via between the layers, have radius of 1 mm. The board follows design rules stated by electromechanics workshop at UREL, The Faculty of Electrical Engineering and Communication at Brno University of Technology. The final layout of Reader board PCB can be seen in Figure 6.4. The size of the reader board is 58 x 54 mm.

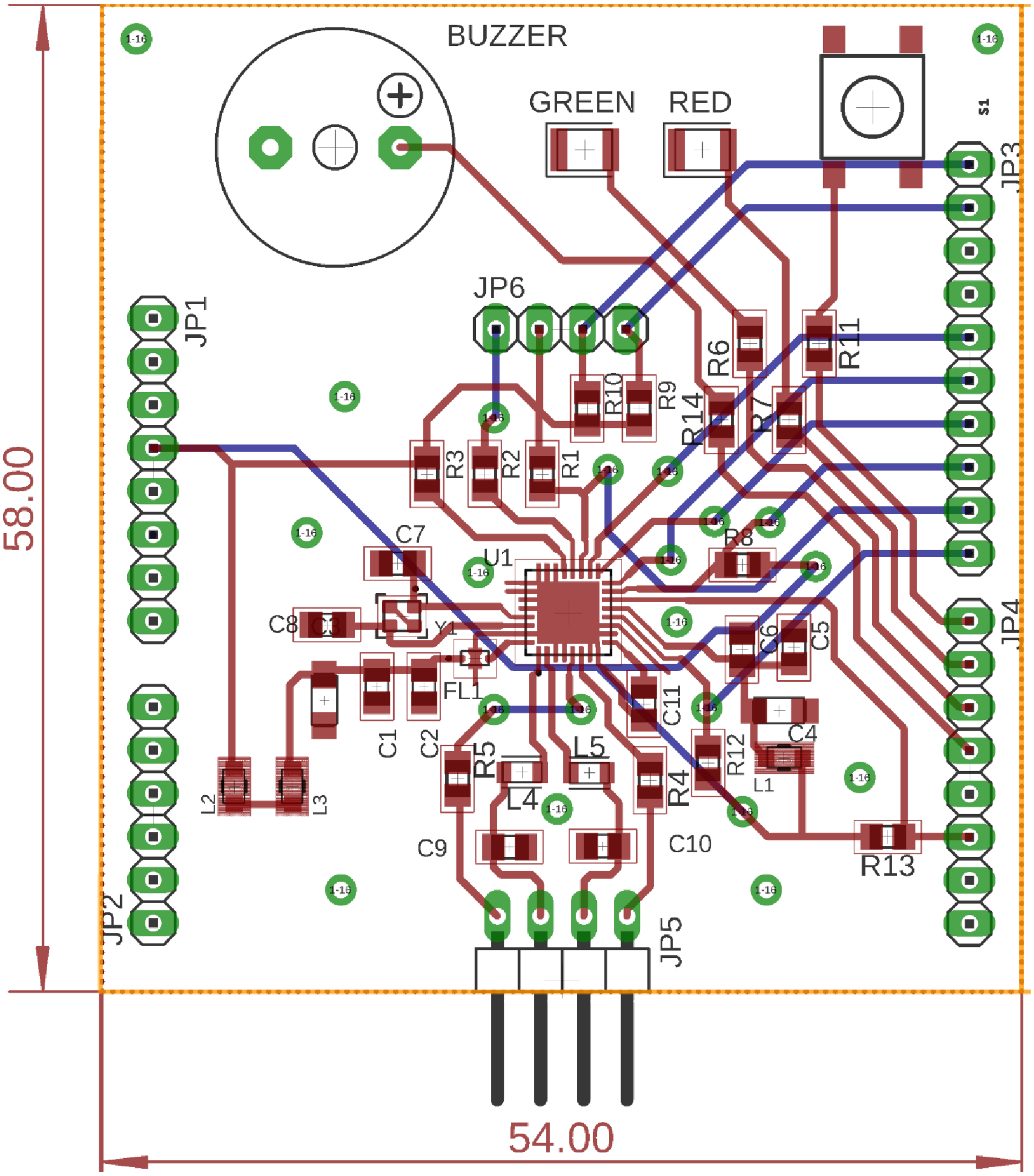


Figure 6.4: PCB layout of Reader board

6.6 Printed Circuit Board layout for Antenna boards

For the purpose of this project, it was decided that six different antennas were going to be made. The ultimate goal was to compare how different sizes and shapes, as well as the inductance of the antenna influence the reading distance. Therefore, two different sizes of antennas, each with three different inductance values were designed. List of variations is as follows:

Size	Turns
47 mm x 34 mm	2
47 mm x 34 mm	4
47 mm x 34 mm	6
60 mm x 18 mm	2
60 mm x 18 mm	4
60 mm x 18 mm	6

Table 8: Antenna variations

In designing the printed circuit board, other properties, which are to be same across all of the boards, have to be established as well. The width of conductive trace was designed to be 1 mm and the spacing between the conductive traces set to 0.4 mm, also following the design rules stated by the electromechanical workshop. Places for passive components are than designed according to the schematic described in a chapter 6.3. The board variation with size 48 mm x 34 mm and 4 turns of conductive trace was designed according to the antenna used in a expansion board X-NUCLEO-NFC03, previously used for the testing of the CR95HF transceiver. Ultimately, it will be possible to compare the antenna design included in a commercially sold device, with its alternatives. Figure 6.5 showcases all of the different PCB layouts for antenna boards.

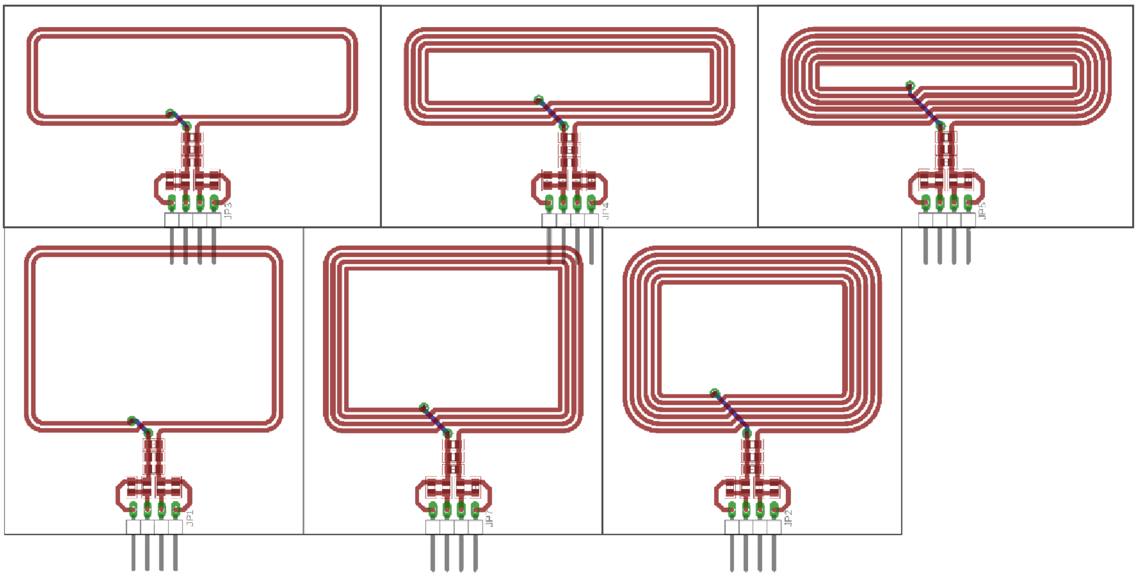


Figure 6.5: PCB layout of Antenna boards

The final assembled boards are shown in the Figures 6.6 and 6.7 below:

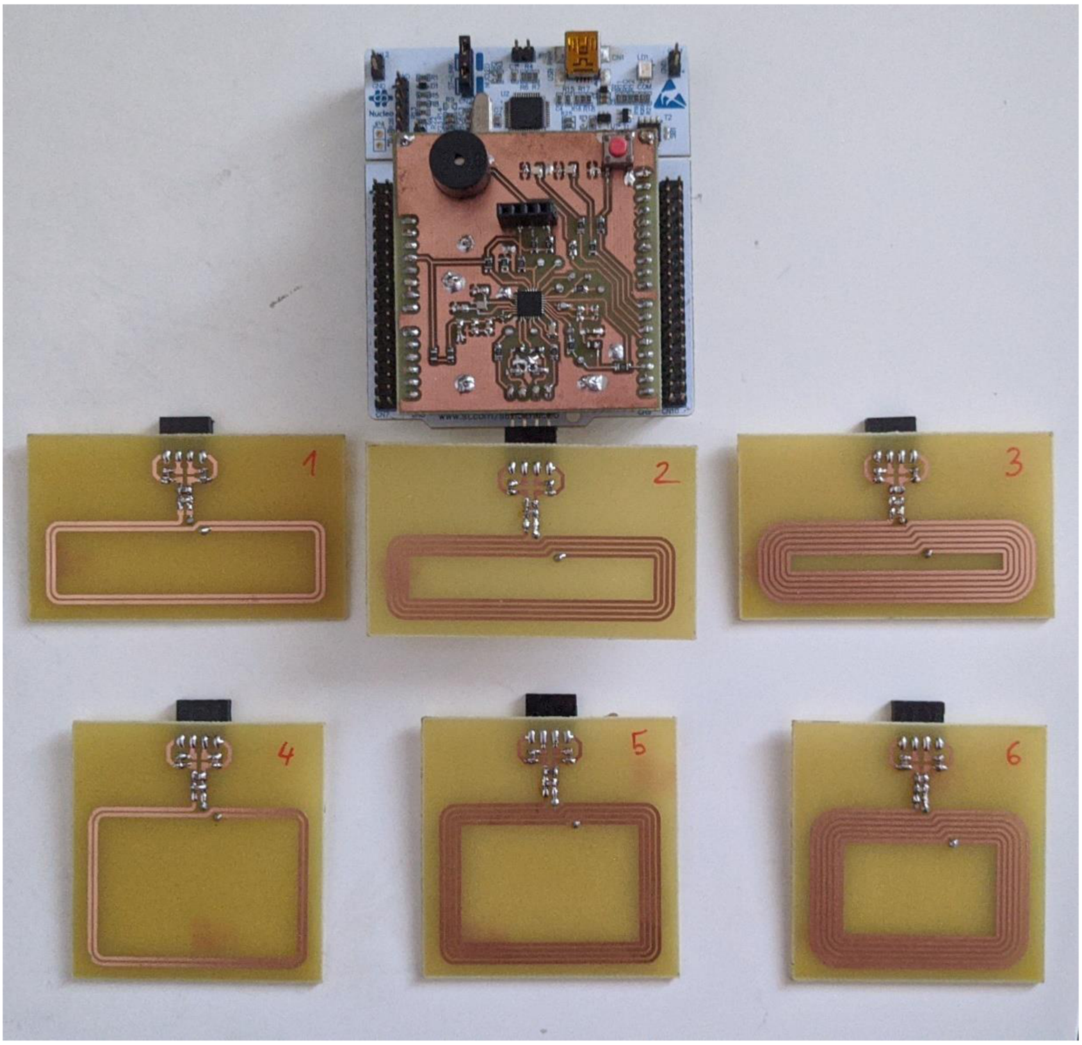


Figure 6.6: Reader board + all antenna boards

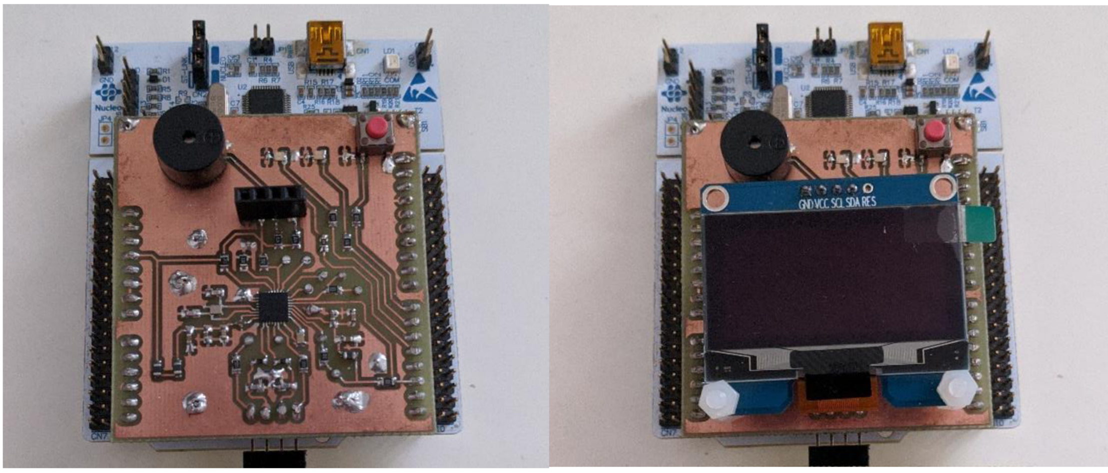


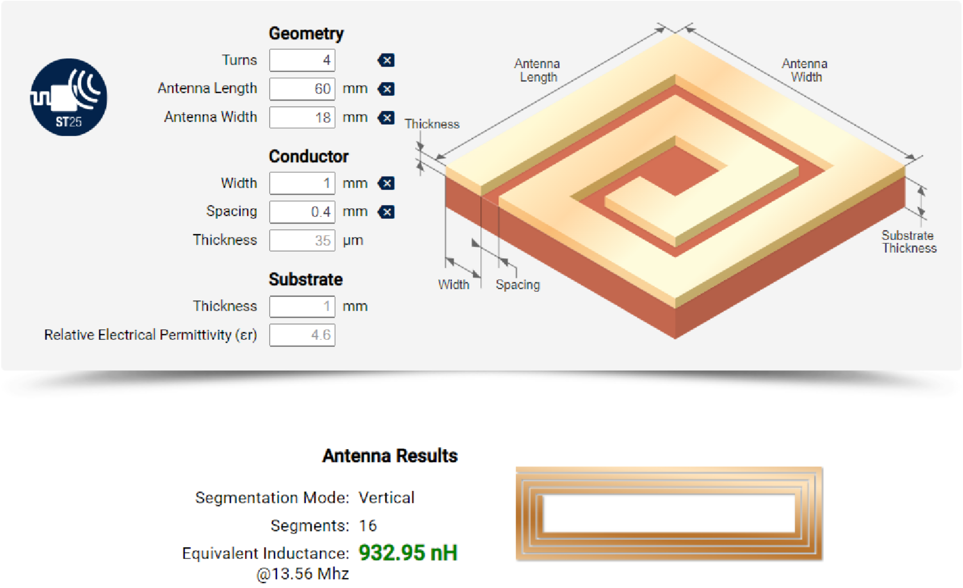
Figure 6.7: Reader board a) without, b) with OLED display

7. ANTENNA TUNING FOR RFID READER

Transceivers are a crucial part of the RFID reader, but they would never work without an antenna sending and receiving the actual information over the electromagnetic fields it creates. Rather than utilizing a random antenna, it must be specifically designed and tuned for the frequency (13.56 MHz) and targeted application. This chapter will go over the designing and tunning of the right antenna for the NFC/RFID application. For tunning, two different methods are going to be used: STMicroelectronics provided software and tunning by network analyzer.

According to [16], when designing an RFID antenna, the engineer must carefully consider the placement of the coil within the final mechanical encasement and ensure that the antenna coil is kept away from all conductors. Any conductor within close proximity to the antenna coil has a dampening effect on the antenna, which changes inductance and affects the tuning of the antenna by causing the center frequency to drift away from 13.56 MHz. Thus, it might reduce the range performance for the antenna and could potentially make the RFID tags unreadable. NXP in [17] mentions that adding a ferrite sheet near the antenna allows to shield the antenna against the influence of the conductor. To reach a proper shielding, the ferrite sheet must, at minimum, fully cover the antenna's surface.

The next step is to determinate the shape of the antenna, length, width, trace width, and number of turns. All of these parameters have influence on the coil inductance. Once all of the parameters determined, it is possible to calculate the theoretical inductance of the antenna. There are various online calculators that could be used to make this calculation, such as [18] made by ST, shown in Figure 7.1.



Geometry

Turns 4

Antenna Length 60 mm

Antenna Width 18 mm

Conductor

Width 1 mm

Spacing 0.4 mm

Thickness 35 µm

Substrate

Thickness 1 mm

Relative Electrical Permittivity (εr) 4.6

Antenna Results

Segmentation Mode: Vertical

Segments: 16

Equivalent Inductance: 932.95 nH
@13.56 Mhz

Figure 7.1: eDesign suite

All of the physical properties of antennas used in this project were established in chapter 6.6. As far as calculated inductances of each antenna, Table 9 establishes the values provided by eDesign suite calculator [18].

Size	Turns	**Inductance**
60 mm x 18 mm	2	357.66 nH
60 mm x 18 mm	4	932.95 nH
60 mm x 18 mm	6	1.38 µH
47 mm x 34 mm	2	426.68 nH
47 mm x 34 mm	4	1.22 µH
47 mm x 34 mm	6	2.1 µH

Table 9: Inductance values for antenna variations

7.1 Low pass filter

It is recommended to use is a low pass filter in the antenna circuitry, as demonstrated as the green part of the Figure 7.2. Described in datasheet [18], this is a second order low-pass filter (EMI filter), and its goal is to attenuate the frequencies above the cut-off frequency of the filter, effectively reducing interferences. Usually, the cut-off frequency of the EMI filter is chosen above 14-15 MHz. In this project, passive components with these values were used, $L_0 = 560nH$ and $C_0 = 180pF$. Therefore, cut-off frequency will be:

$$f_c = \frac{1}{2\pi\cdot\sqrt{L_0\cdot C_0}} = \frac{1}{2\pi\cdot\sqrt{(560\text{n}\cdot 2)\cdot(\frac{180\text{p}}{2})}} = 15.9\ MHz \qquad (7.1)$$

It is worth mentioning that the inductors were replaced by ferrite bead EMI suppressors. Its impedance at 13.56 MHz is 560 nH in series with 3 Ω, and above 200 MHz it behaves as a pure resistor to suppress spurious emissions.

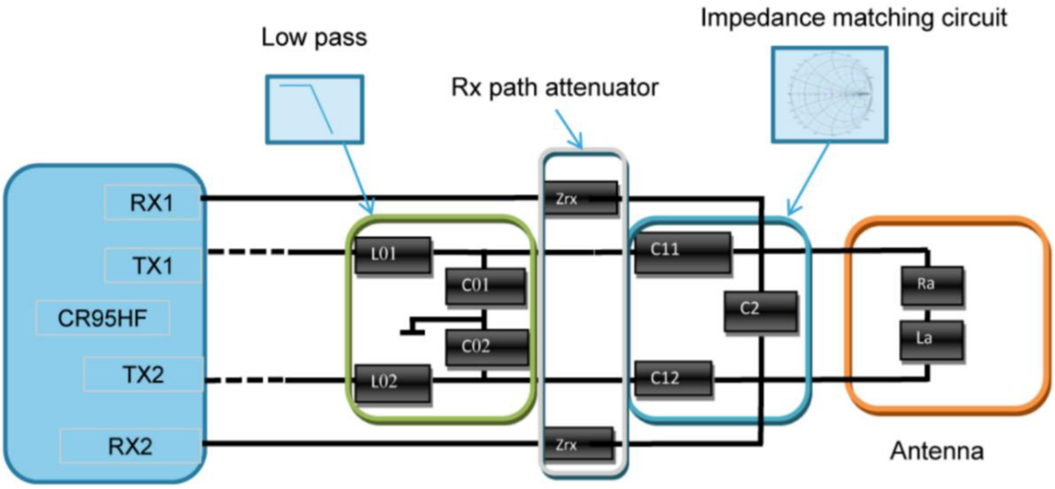


Figure 7.2: CR95HF tuning circuit with an EMI filter – [19]

7.2 Impedance matching

Mentioned in [17], it is required to determine the antenna electrical equivalent (represented by the orange part of the Figure 7.2). To get the serial equivalent circuit of the antenna, two parameters must be established. Inductance (mainly defined by the number of turns of the antenna), and resistance (mainly defined by the diameter and length of the antenna wires). In some cases, it is required to establish capacitance as well (mainly defined by the distance of antenna wires from each other and number of turns).

The Q factor of the antenna depends on its inductance value and series impedance, measuring the selectivity of the antenna. If the Q factor is too high, the antenna may become too selective which can result in the narrowing bandwidth of the resonance. In case the measured antenna quality factor is above the recommended value, R_Q resistors in series can be used to damp it.

The blue part within the Figure 7.2 is called the impedance matching circuit. The capacitors C11, C12 and C2 are calculated so that the tuning circuit input impedance (Zin2) matches the complex conjugate output impedance of the new RF generator, which is made of the transceiver and its EMI filter at the operating frequency of 13.56MHz. As seen in Figure 7.3, matching criteria in this case is Zin2 = Zout_EMI.

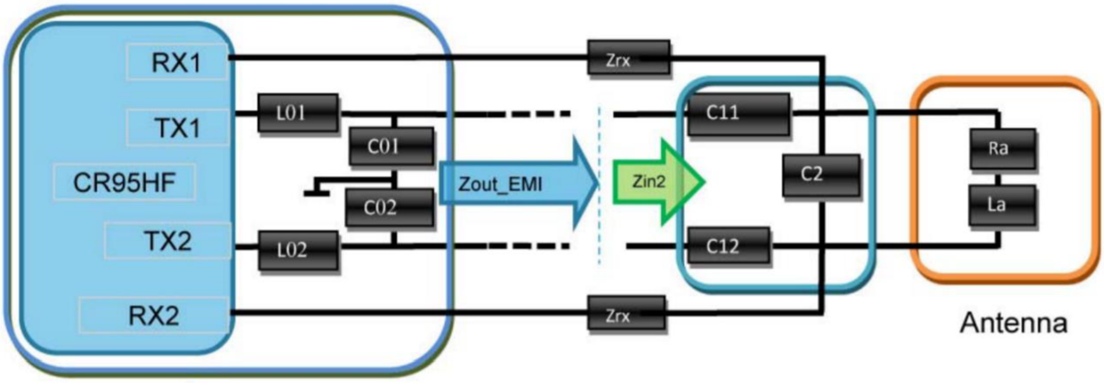
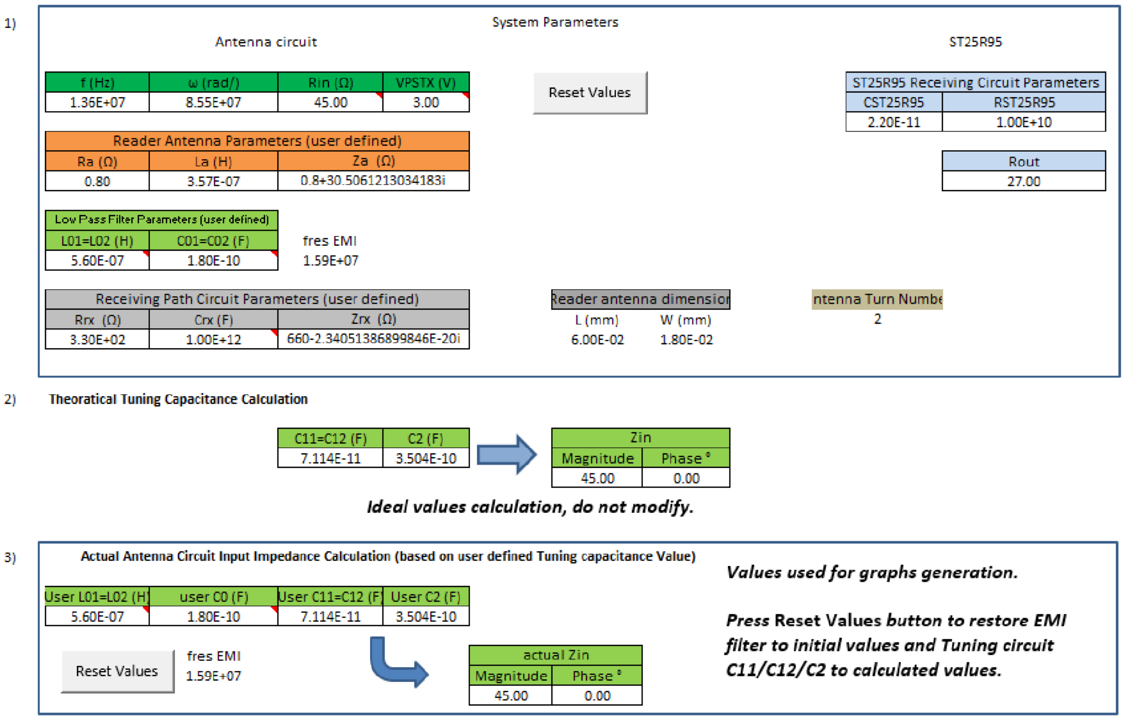


Figure 7.3: Impedance matching with an EMI filter – [19]

7.3 Matching circuit determined by software

The company STMicroelectronics provides a free software called ST25R95 EMI a filter calculation tool on their website [20]. This software calculates the values of impedance matching circuit, specifically the values of capacitors C11 = C12 and C2 according to the input values provided by the designer. In the Figure 7.4, it is possible to observe how does the user interface is seen. Used correctly, this provides information about the Low-pass filter, reader antenna parameters and the program calculate the capacitor values. This software is simple to use and provides the designer with fast and fairly accurate information about the matching circuitry, that is required to be used.



1) System Parameters

Antenna circuit

f (Hz)	ω (rad/)	Rin (Ω)	VPSTX (V)
1.36E+07	8.55E+07	45.00	3.00

Reader Antenna Parameters (user defined)		
Ra (Ω)	La (H)	Za (Ω)
0.80	3.57E-07	0.8+30.5061213034183i

Low Pass Filter Parameters (user defined)	
L01=L02 (H)	C01=C02 (F)
5.60E-07	1.80E-10

fres EMI
1.59E+07

Receiving Path Circuit Parameters (user defined)		
Rrx (Ω)	Crx (F)	Zrx (Ω)
3.30E+02	1.00E+12	660-2.34051386899846E-20i

Reset Values

ST25R95

ST25R95 Receiving Circuit Parameters	
CST25R95	RST25R95
2.20E-11	1.00E+10

Rout
27.00

Reader antenna dimensior	
L (mm)	W (mm)
6.00E-02	1.80E-02

ntenna Turn Numbe
2

2) Theoratical Tuning Capacitance Calculation

C11=C12 (F)	C2 (F)
7.114E-11	3.504E-10

Zin	
Magnitude	Phase °
45.00	0.00

Ideal values calculation, do not modify.

3) Actual Antenna Circuit Input Impedance Calculation (based on user defined Tuning capacitance Value)

User L01=L02 (H)	user C0 (F)	User C11=C12 (F)	User C2 (F)
5.60E-07	1.80E-10	7.114E-11	3.504E-10

Reset Values

fres EMI
1.59E+07

actual Zin	
Magnitude	Phase °
45.00	0.00

Values used for graphs generation.

Press Reset Values button to restore EMI filter to initial values and Tuning circuit C11/C12/C2 to calculated values.

Figure 7.4: Calculator of impedance matching circuit in ST25R95 EMI filter calculation tool

The program also provides the information on antennas reflection coefficient displayed on the Smith Chart. Figure 7.5 shows just that.

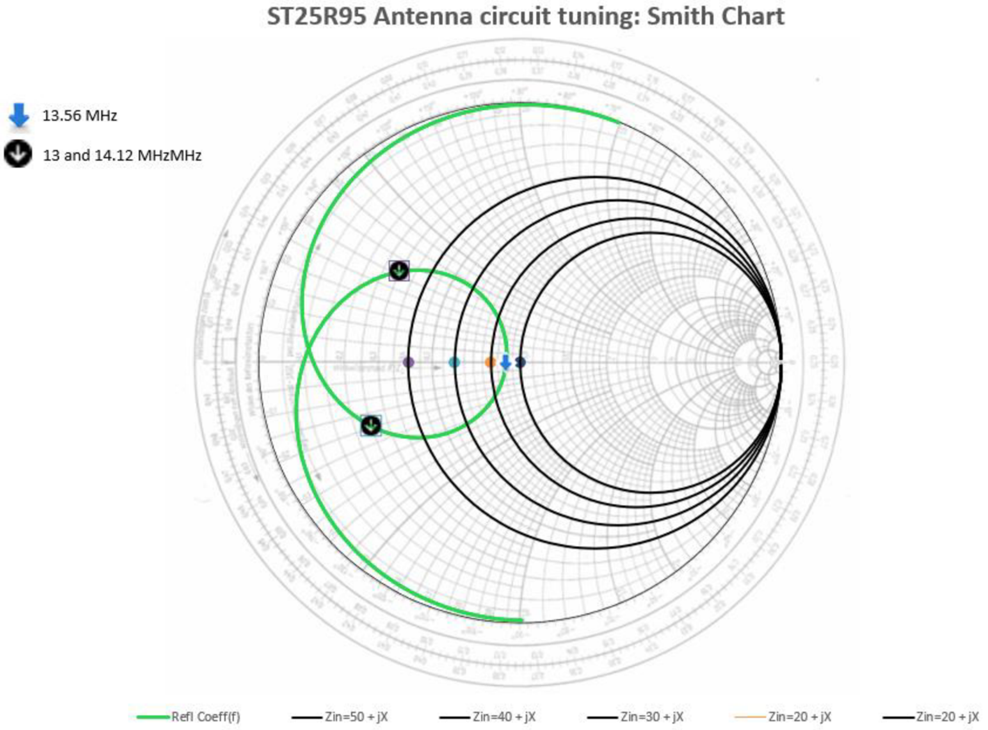


Figure 7.5: Smith Chart drawn by ST25R95 EMI filter calculation tool

After feeding the parameters for all six antennas used in this project, the ST25R95 EMI filter calculation tool determined these results for C11 = C12 and C2 respectively, visible in Table 10. It is important to bear in mind that all of these values are purely theoretically calculated with various software calculators. Real world values could differ and components with the closest values will be used for testing.

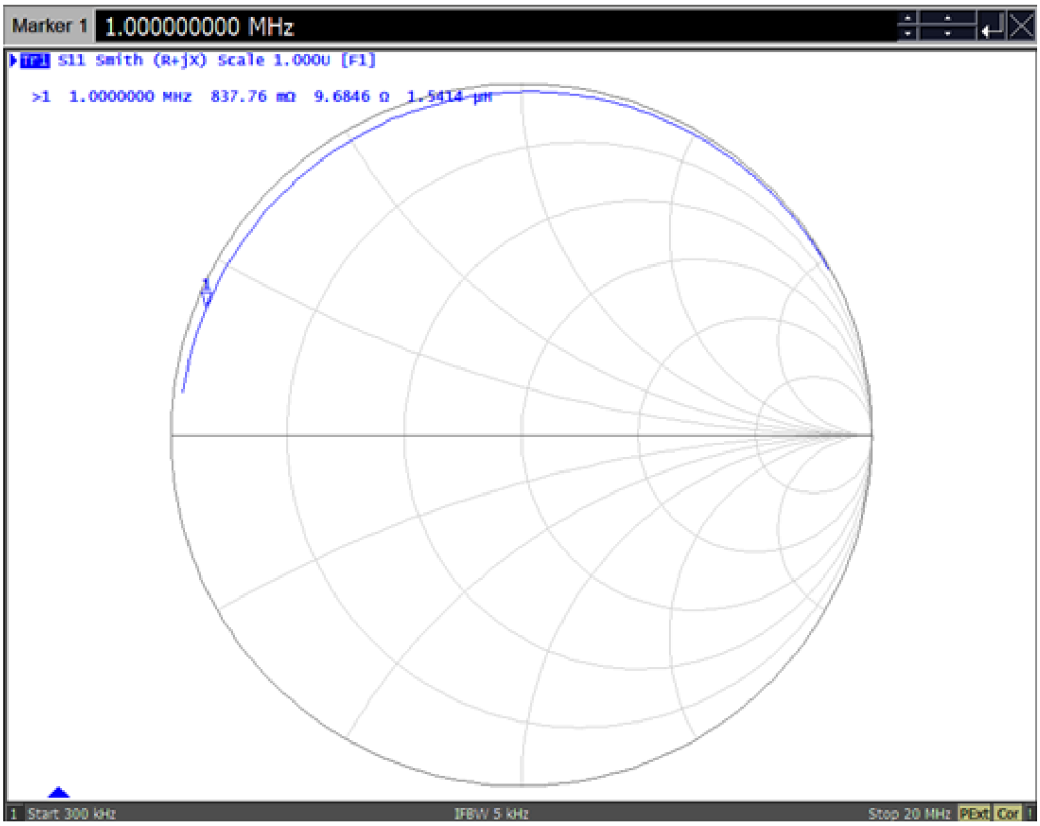
Size	Inductance	**C11 = C12**	**C2**
60 mm x 18 mm / 2	357.66 nH	69.7 pF	339.2 pF
60 mm x 18 mm / 4	932.95 nH	49.9 pF	107.1 pF
60 mm x 18 mm / 6	1.38 µH	48 pF	57.3 pF
47 mm x 34 mm / 2	426.68 nH	63.5 pF	285.2 pF
47 mm x 34 mm / 4	1.22 µH	48.7 pF	79.1 pF
47 mm x 34 mm / 6	2.1 µH	47.4 pF	32 pF

Table 10: Values of impedance matching circuitry calculated by software

7.4 Matching circuit determined by measurements with network analyzer

The second option of how to match the output impedance with the impedance of the antenna is to measure the parameters with the Agilent E5071C Network Analyzer. The network analyzer should provide the information about antennas' inductance, as well as real and imaginary components of the antenna coil and also the reflection coefficient. This way, it is possible to obtain real parameters of each antenna specifically and compare them with calculated values.

In the beginning, the Agilent E5071C Network Analyzer must be calibrated to guarantee the integrity of the results. Calibration is done with Agilent N4433A electronic calibration module, which is connected to the port used for measurements. After connecting the calibration module, the option of ECal and then 1-port calibration is chosen. With now calibrated device, it is time to calibrate the port with an extension cable. For calibration of the port with port extension, it is required to run the calibration process with open and short circuit at the end. With all calibrations completed, the device is ready to be used. The first important measurement is to determinate the resistance and inductance of each antenna (Ra and La in the Figure 7.3). These values were previously calculated with eDesign suite. In the Figure 7.6, the measurement for antenna 60x18/6 is visible. The measurement was carried out on the frequency of 1 MHz with the resulting inductance of 1.54 µH and resulting resistance of 838 mΩ. This process must be repeated for all the antennas. Results of the measurements are displayed in the Table 11.


Marker 1 1.000000000 MHz

Tr1 S11 Smith (R+jX) Scale 1.000U [F1]

>1 1.0000000 MHz 837.76 mΩ 9.6846 Ω 1.5414 µH

Figure 7.6: Measurement of resistance and inductance

Size	Turns	**Resistance**	**Inductance - measured**	**Inductance - calculated**
60 x 18 mm	2	430 mΩ	414 nH	357.66 nH
60 x 18 mm	4	670 mΩ	1.04 µH	932.95 nH
60 x 18 mm	6	830 mΩ	1.54 µH	1.38 µH
47 x 34 mm	2	440 mΩ	474 nH	426.68 nH
47 x 34 mm	4	670 mΩ	1.29 µH	1.22 µH
47 x 34 mm	6	840 mΩ	2.15 µH	2.1 µH

Table 11: Real properties of antennas

After establishing the parameters of the antennas, it is possible to procede to the tunning part. The connection position in which the network analyzer was connected can be seen in the Figure 7.7. When tunning the antenna circuit, it is crucial to consider all the componenets included in the antenna circiut (EMI filter + matching circuitry) and also the true length of the conductive traces. Therefore, the network analyzer device is connected all the way after the inductors from EMI filter. With that being said, it is possible to start preforming the return loss measurement in order to obtain the results of antennas' tunning frequency and impedance magnitude.

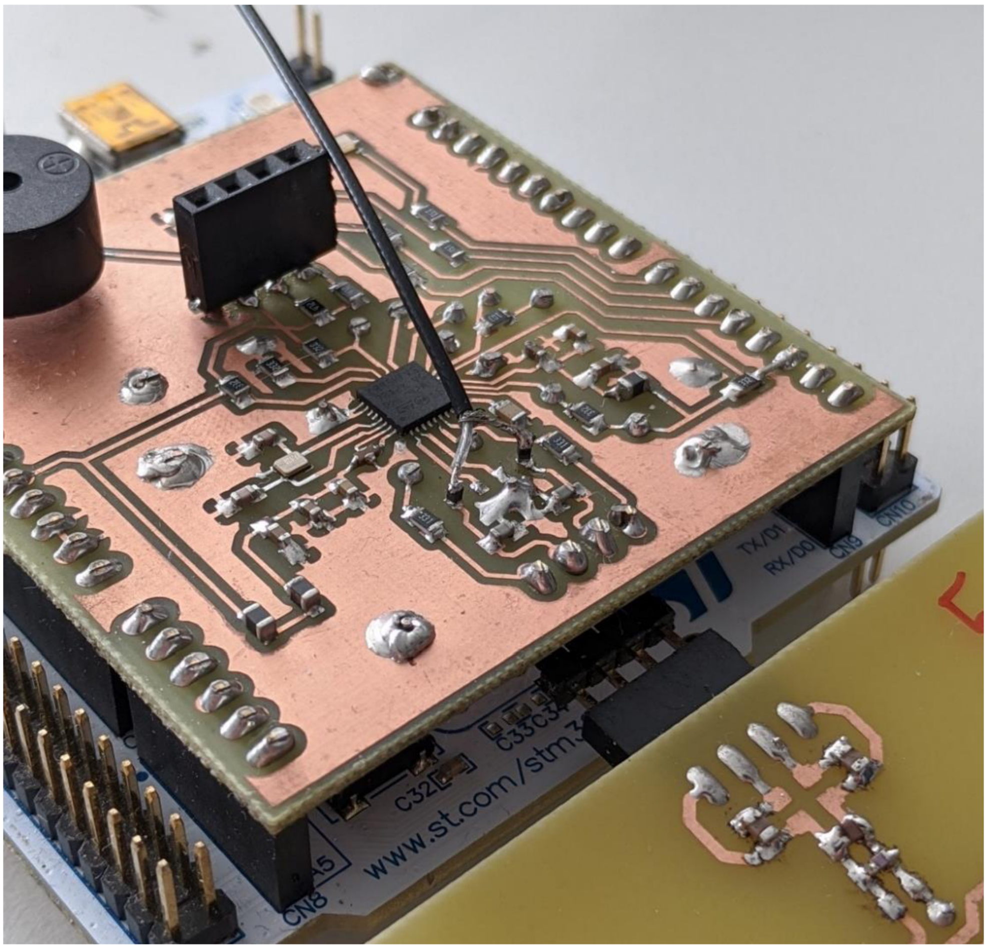


Figure 7.7: Connection points for network analyzer measurements

Generally, when tuning RFID antennas with a similar layout, the designer must consider these changes in order to get a well-tuned antenna:

1. Increasing or decreasing the capacitors in series (C12, C13, C14, C15 in the Figure 6.6) will adjust the impedance magnitude. Decreasing the values will lower the return loss and make the circle in the Smith chart smaller. Increasing the values will cause the scenario to go vice versa.
2. Increasing or decreasing the capacitors in parallel (C16, C17 in the Figure 6.6) will adjust the tunning frequency. Increasing the values will reduce the frequency and vice versa.

Antennas used in this project are assembled with the matching circuitry from calculations made earlier. The assumption and hypothesis that software calculators were not going to be far off from the reality is confirmed after performing the measurement on all of the antennas. It is observed that the common defect on all of the antennas is a slightly higher tunning frequency than desired 13.56 MHz. Therefore, on all of the antennas, capacitors in parallel must be slightly increased to reach the best results. The ideal results should look somewhat similar to ones in the Figure 7.8 representing tuned 47x34 / 6 turns antenna.

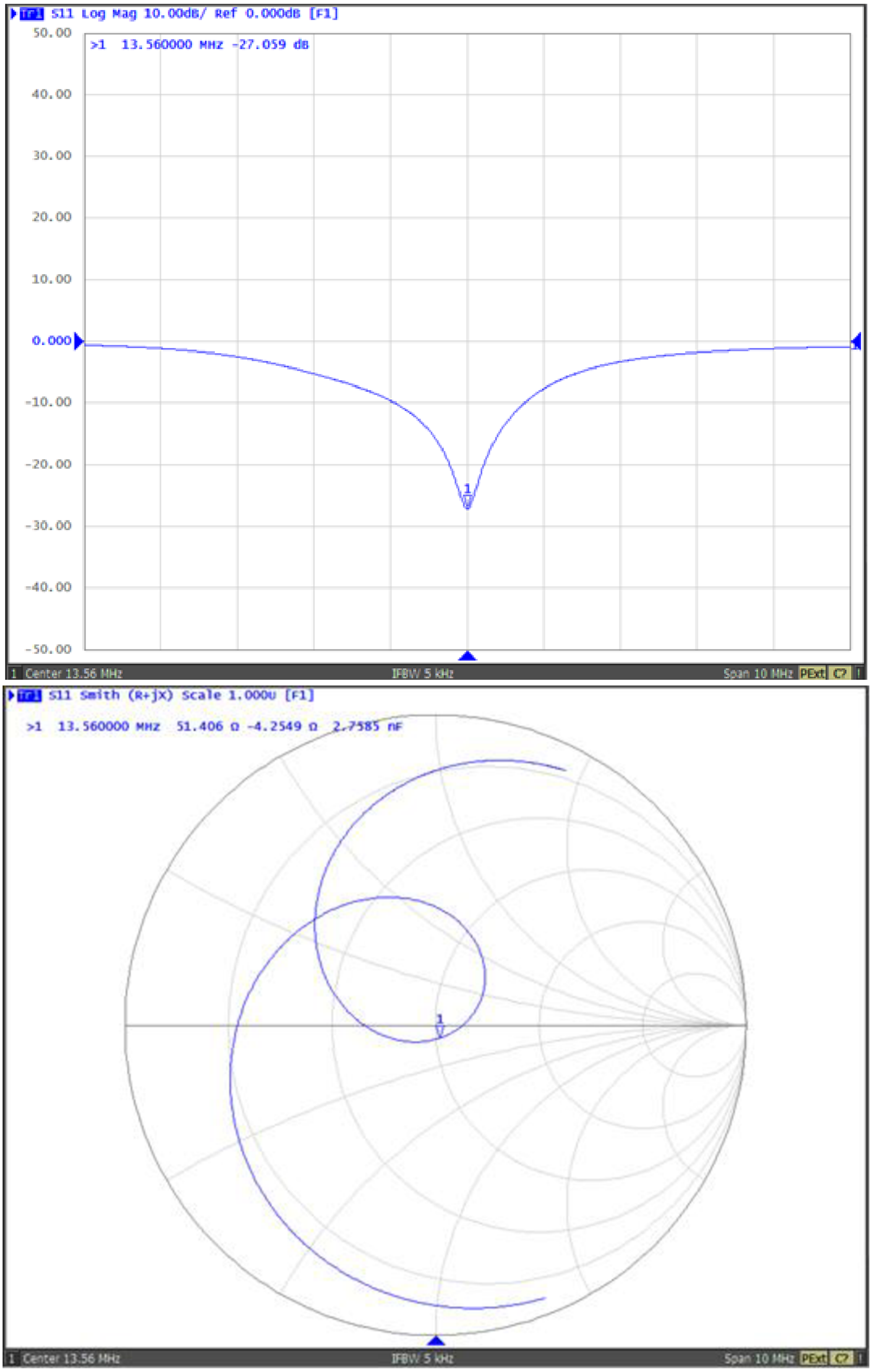


Figure 7.8: Results a) Return loss measurement, b) Smith chart antenna matching of tuned 47x34/6 antenna

The final list of the used matching capacitors values can be seen in the Table 12. The pictures of all return loss measurements and Smith charts can be seen in the Appendix B and C. The results of the measurements on the network analyzer are very similar to the ones determined by the software, even with the influence of parasite capacitance created by conductive traces taken into the consideration. Therefore, it is undeniable that software nowadays provides a safe and fast option to obtaining the reasonable results within antennas matching circuitry. However, it is not always as precise as measurements made on the real product, so if the best results are necessary, tunning must be performed. "Precise tuning is most important when creating an antenna with high Q factor for ISO/IEC 15693 tags, as the sidebands are cut off if the bandwidth is too narrow and the center frequency is off tuned, and that cutoff results in poor performance." [17]

Size	Inductance	**C11 = C12**	**C2**
60 mm x 18 mm / 2	357.66 nH	56 pF	345 pF
60 mm x 18 mm / 4	932.95 nH	47 pF	112 pF
60 mm x 18 mm / 6	1.38 µH	47 pF	66 pF
47 mm x 34 mm / 2	426.68 nH	56 pF	292 pF
47 mm x 34 mm / 4	1.22 µH	47 pF	85.3 pF
47 mm x 34 mm / 6	2.1 µH	47 pF	38.6 pF

Table 12: Final capacitor values determined by tunning on the network analyzer

7.5 Detuning caused by conductor

Well-tuned antennas should have the minimal return loss magnitude on the desired frequency, similar to the Figure 7.8 a), having its lowest point exactly at 13.56 MHz. However, any conductor near to the proximity of well-tuned antenna will detune it. When moving the conductor towards the antenna, it will slowly decrease the inductance of the antenna coil (eddy current on the metal plate) and therefore shift the minimum return loss (resonant frequency) upwards. Figure 7.9 demonstrates the effect of the conductor on the 60x18/2 antenna. The marker shows the position of desired 13.56 MHz on both a) and b). Since the minimum of return loss moved towards 14.56 MHz, the marker on the Smith Diagram moved away from the center point (point of impedance matched). Detuning the antenna with the conductor will lead to an overall worse performance, loss of reading distance and more frequent errors in communication. These problems could be removed by tuning the antenna with the conductor in its field. As it is known that the frequency shifted upwards, increase in parallel capacitors should push it back downwards. Depending on how far the frequency has shifted, an increase of capacitance must be chosen adequately. This way, it is possible to bring back the center frequency back to the chosen value.

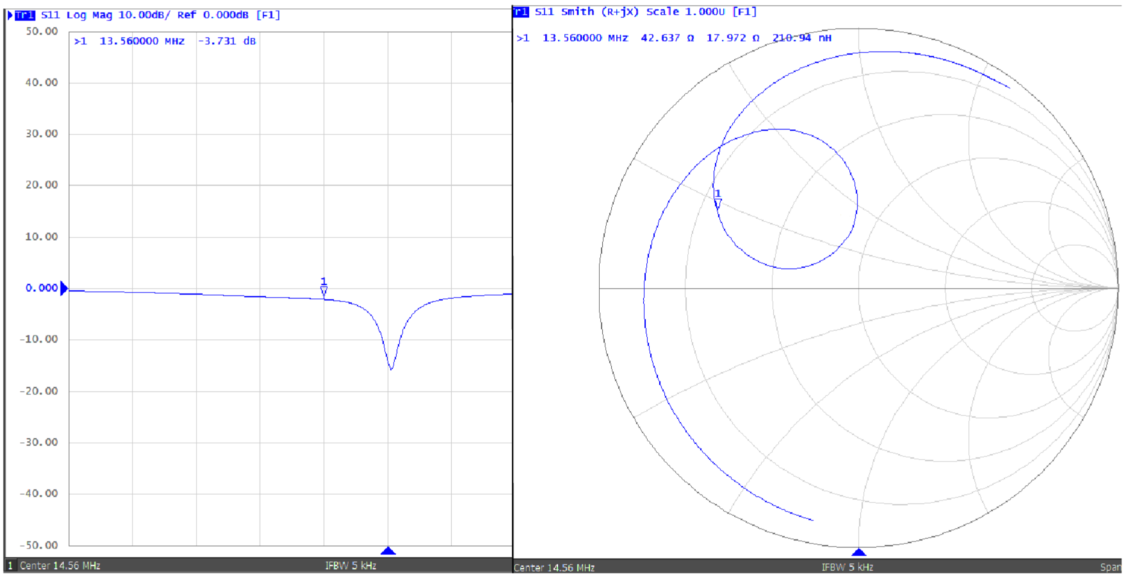


Figure 7.9: Results a) Return loss measurement, b) Smith chart antenna matching of antenna detuned by metal

Conductors within proximity of the antenna also lowers the Q-factor of coil resulting in the loss of reading range. To a small extent, this could be eliminated by decreasing the capacitors in series, yet the antenna will never reach the potential it has without the metal close by. Hence, the designer must always consider the presence of conductors close to the antenna.

As an example of how conductors effect the antennas performance, observe the results of the reading range using the ISO/IEC 15693 transponder (for full comparison, please visit chapter 9 – Testing of the reader). A single reading toggled through the manual operation of the reader was able to read the transponder at the maximum distance: around 69.8 millimeters. However, when a metal plate was placed close to the antenna (Figure 7.10), the reader was only able to detect the transponder at the maximum distance of approximately 30.5 millimeters. This is a loss of 57% from the possible maximum reading range. If the antenna was to be tuned with the metal plate next to the antenna, it is possible to regain some of that maximum reading distance back.

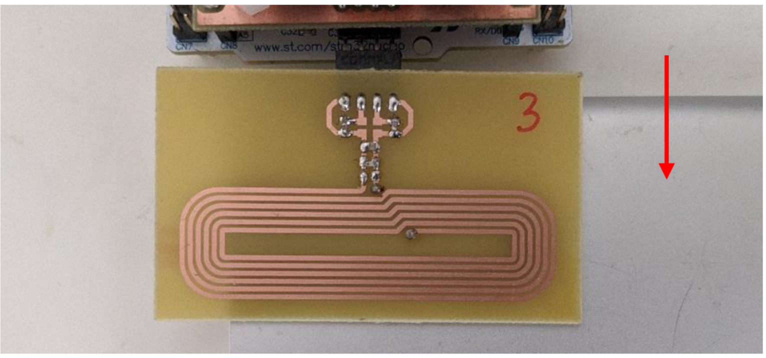


Figure 7.10: Testing of antenna with metal plate in proximity

8. FIRMWARE

In the previous chapters, the hardware component of this project was established. Consequently, one must now establish the software part of the project. In order for the RFID reader to work properly, a program has to be made for controlling the functions. As mentioned in chapter 5.2 (Conclusion of testing), programming interface STM32CubeIDE was used. Ultimately, there is an option to make a project using HAL libraries (This option was used in the making of this project), which enables the designer to set inputs/outputs, differing peripherals, and other properties via graphical interface (Pinout view) while automatically updating the code after the changes were made. This feature could be seen in figure 8.1. For example, when the UART needs to be configured, the tab in the Pinout & Configuration menu can be used. This tab brings up a UART configuration menu with basic parameters such as baud rate, which can be changed in any given moment. When change happens, a code in the main file will be automatically updated with the given properties. Inside the code of the main file, one can also find multiple spaces labeled the USER CODE which could not be changed by the automatic updates of HAL libraries and will always stay the way user writes them. Because of this, the user needs to be extremely cautious to only write their code in these spaces, otherwise it will be deleted or overwritten by the automatic update. This is not the only way to program ST's microcontrollers but for the purpose of this project, STM32CubeIDE is the easiest and most efficient way to utilize the program. The program is written in the C programming language as it is the default when it comes to programming hardware.

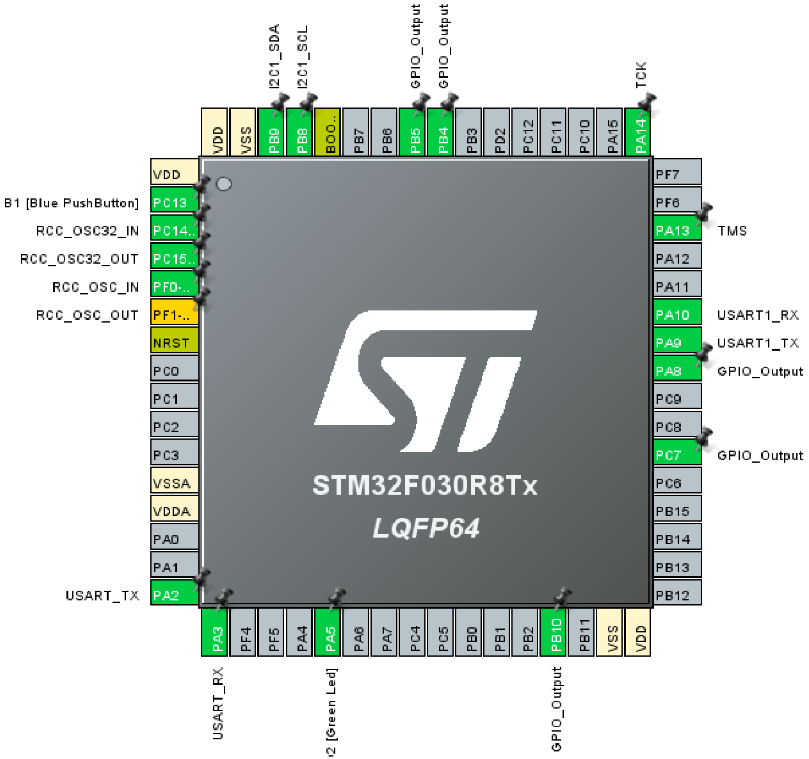


Figure 8.1: Graphical interface of STM32CubeIDE, pinout view

The program consists of a main file, which incorporates a source file with functions for operating the display, a source file containing the declaration of fonts for display and a source file with functions for operating the reader.

8.1 Communication interfaces

In the beginning, both UART 1 and 2 should be inspected, to ensure the correct properties for the communication are set. Since the main communication between computer and CR95HF is carried out by UART, it will be described first. UART 1 is set to a baud rate of 57600 Bits/s with word length of 8 bits, no parity and 2 stop bits. UART 2 in the other hand, is set to a baud rate of 38400 Bits/s with word length of 8 bits, no parity and 1 stop bits.

Secondly, the communication with display is carried out by I^{2}C interface. More precisely, data which is set to be displayed on the OLED display is sent via SDA wire. For timing configuration, I^{2}C speed mode is set to Fast mode with the frequency speed at 400 kHz.

8.2 Display

The library used for controlling the OLED screen made by Alexander Lutsai is available at his GitHub repository: https://github.com/SL-RU/stm32libs. With this library, is it possible to display characters (or string made out of regular characters), scroll through the screen in any direction, invert the colors of individual pixels and draw a line, rectangle, triangle, circle, and desired bitmap. For using the bitmap function, hexadecimal code with instructions for each pixel has to be saved in the program directory.

Part of the library also contains a file with fonts of 3 different sizes: 7x10, 11x18 and 16x26 pixel with a sets of basic characters. Each character has its information about each pixel stored in a hexadecimal code, similar to the bitmaps. Example of the code that will print “RFID SCANNER” on the display in the 11x18 pixels font:

```
SSD1306_Init (); // initialize the display
SSD1306_GotoXY (45,10); // go to x=45, y=10
SSD1306_Puts ("RFID", &Font_11x18, 1); // print RFID
SSD1306_GotoXY (30, 30); // go to x=30, y=30
SSD1306_Puts ("SCANNER", &Font_11x18, 1); // print SCANNER
SSD1306_UpdateScreen(); // update screen
```

Each function, which is changing the information displayed on the display is storing the information about each individual pixel in the internal RAM. After each set of changes, function *UpdateScreen* must be called, which toggles the pixel inversion stored inside the internal RAM.

8.3 Reader source file

On the top of reader source file called cr95hf.c, are multiple *#define* for variables which will be used throughout the file. After the declaration of variables, there are 3 functions which take care of the reading and writing into the UART buffers. The aforementioned functions allow the communication between the host computer and extension board to be possible as they write the values in the UART 1 buffer connecting the microcontroller and expansion boards from what the user types on their computer and sends into the UART 2. Ultimately, the functions read the responses from the CR95HF in UART 1 and send the messages into the UART 2 for the user to see on their screen.

8.3.1 Operating modes

The CR95HF has 2 operating modes: Idle and Active. In Active state, the CR95HF communicates actively with a tag or an external MCU. Idle state (wait for event) includes two low consumption states: Hibernate and Tag Detector. Following the operating modes, the wake-up function (low pulse on the IRQin pin) is then established as is shown in the Figure 8.2. This wakes up the transceiver from the idle state. On the other hand, to send the IC into an idle state, another function could be deployed. This function has a set of bytes that are sent to the IC, and depending on the values set in those bytes, the CR95HF can pick between the two idle states. If the third byte is set to 0x08, the IC switches into hibernate mode, while if the third byte is 0x0A it switches into Tag detector mode.

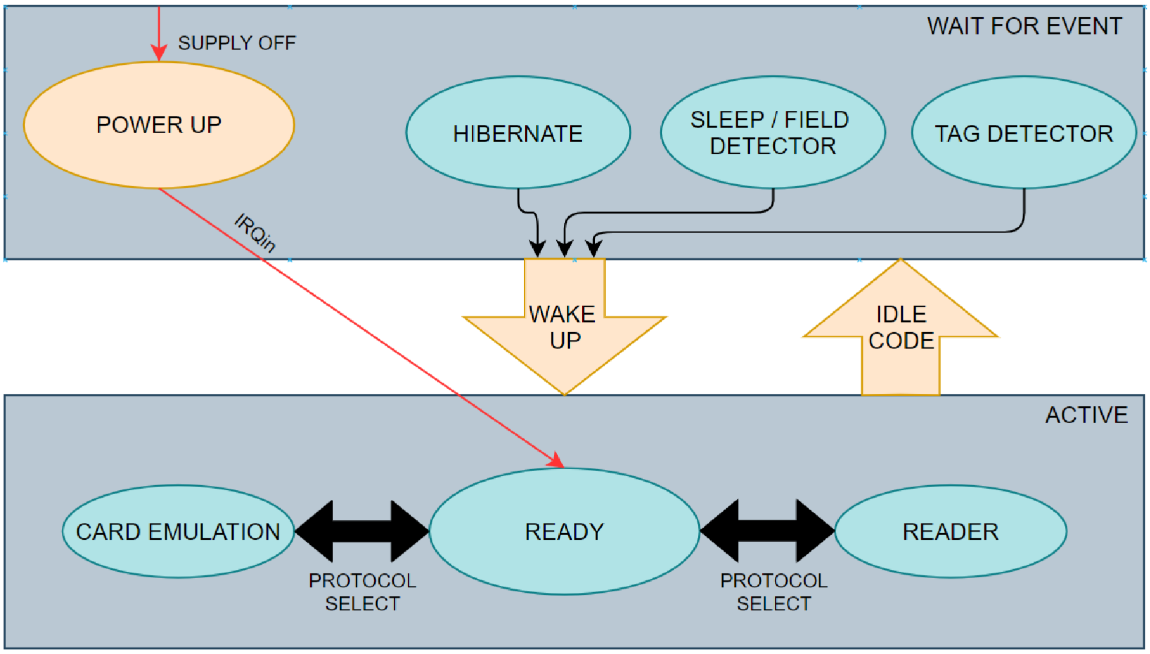


Figure 8.2: CR95HF initialization and operating state change – [11]

8.3.2 Initializations

The next part of the code includes initializations of different standards for the CR95HF. According to the data sheet – [11], program have to send specific bytes (command) to the CR95HF, which will recognize from the bytes what standard will be used in the next reading (different standards have different reading procedures, therefore they need to be initialized specifically). There are 2 or 3 commands sent to the transceiver one by one and after each of them, the program has to wait for the positive response from CR95HF before sending the next command. The first command is the protocol select. The byte composure is as follows: first byte is the command code (protocol select = 0x02), second byte is the length of the data being sent, and third byte on is the data. For example, `cmd_init1[] = {0x02, 0x02, 0x02, 0x00}` is the command to select ISO/IEC 14443 Type A tag with 106 Kbps transmission and reception rates and 86/90 time interval. After the CR95HF successfully selects the protocol from the command, it will send a 0x00 (positive) response. The second command is usually for improving the RF performance. Adjusting the Modulation Index and Receiver Gain parameters helps improve application behavior. For this purpose, command Write register (WrReg with the code 0x09) is used. In the datasheet, a table for each standard with a default, recommended and possible values is presented, allowing the user to optimize for their application. For the ISO/IEC 14443 Type A standard, there is an extra third command that adjusts the synchronization between the digital and analog inputs by fine-tuning the Timer Window (TimerW) value. This is done for improving frame reception for the tags.

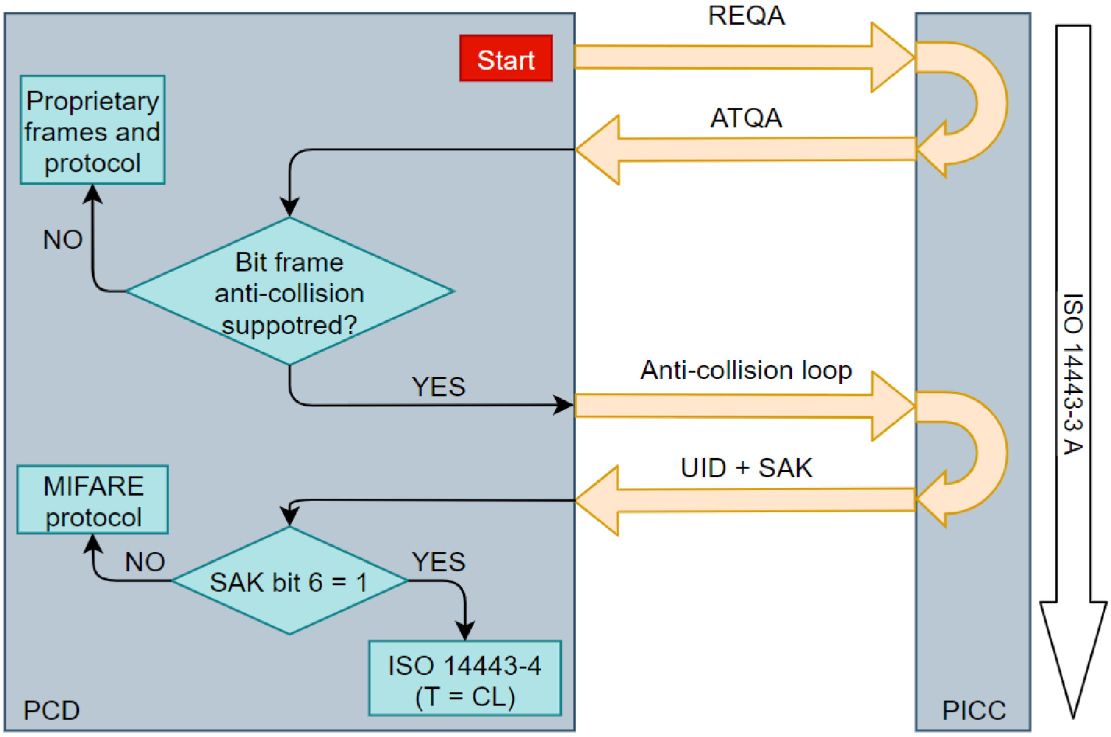


Figure 8.3: Principle of card activation sequence of ISO/IEC 14443A – [14]

8.3.3 Reading algorithms

After the initializations are carried out successfully, the reader is in its active mode and it is ready to read the tags. The next two functions allow for the reading of the tag to occur for both ISO/IEC 14443A and ISO/ IEC15693 standards. Similarly, as different protocols had different initializations, tags based on different protocols also require a various ways to read the UID and data. Based on the first standard (ISO/IEC 14443A), to read the tag, it first needs to be selected. This process is defined as card activation sequence in the standard. This card activation process is shown in the Figure 8.3.

8.3.3.1 Anti-collision loop of ISO/IEC 14443 Type A standard

In the beginning, the reader sends a REQA (Request command, type A) to which the transponder responds with a ATQA (Answer to request, type A). The content of the ATQA could be ignored in a real application, even though it suggests the length of the UID; and indicates that the tag supports the anti-collision scheme. After the reader receives the ATQA, the anti-collision loop can be started. This process is shown in Figure 8.4. The loop begins by the reader sending an anti-collision request number one, allowing the transponder to reply with either all four bytes of its UID or with a cascade byte followed up by three bytes of its UID. With a cascade byte being the first byte of the response (value 0x88 is used by ISO/IEC 14443 A standard), the reader can determine the length of the received UID information.

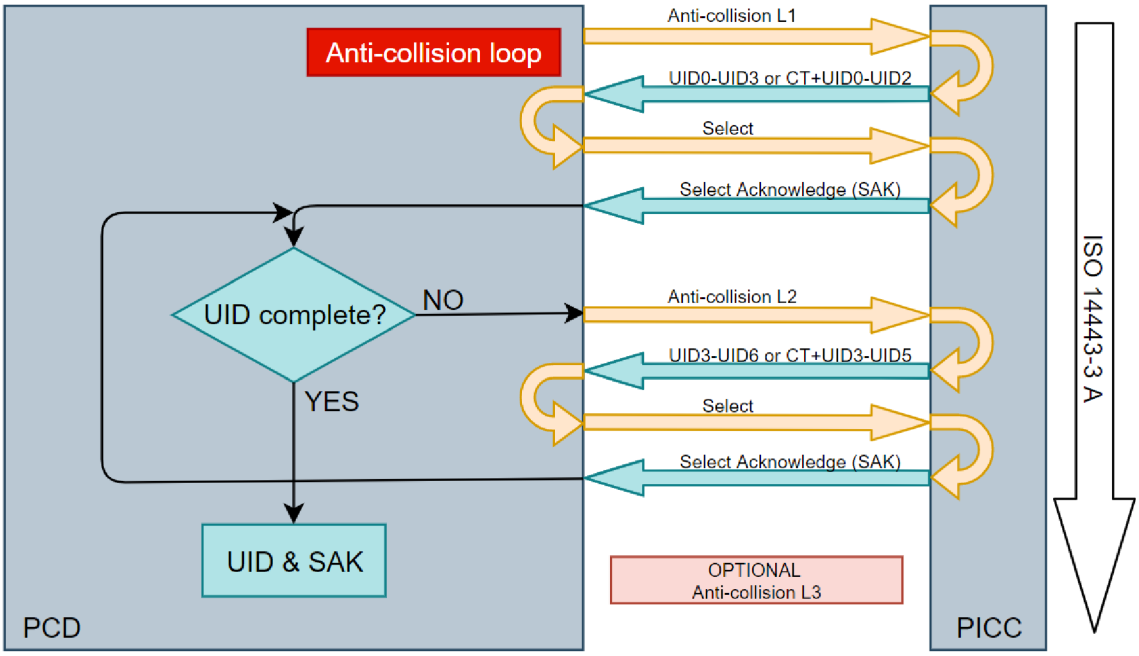


Figure 8.4: Principle of anti-collision loop – [14]

After the reader receives the response, it will send a select tag command. The tag will respond with the SAK (Select acknowledge) which contains various strategic information segments for the reader. Two bits are exceptionally important, and need to be investigated by the reader. These bits are third and sixth. The third bit showcases if the UID is (value = 0) or is not (value= 1) complete. The sixth bit displays if the tag is compliant with the ISO/IEC 14443-4 section (value = 1) or if it is compliant with other protocol (value = 0), as Figure 8.3 suggests.

For example, the SAK value of single Mifare classic card is 0x08. When this hexadecimal value is converted into binary (0000 1000), it is possible to notice both the third and sixth bits are 0, which reveals that the UID is complete, and it is compliant with Mifare protocol. Values for other Mifare tags can be found in [14]. If the third bit of the SAK turns out to be 1, the reader then sends anticollision request number two and the whole process repeats. If the third bit of SAK in the second Anticollision request is still 1, a third anticollision request must follow, and an UID will be 10 bytes. This, however, is very rarely used and most of the tags are either 4 or 7 bytes long.

8.3.3.2 Reading of ISO/IEC 15693 tag

In comparison to the much more complicated process of the anti-collision loop mentioned earlier, reading of ISO/IEC 15693 standard based tags is much easier. After initialization of the standard, all that is needed to receive an UID of the tag is to send a request to read inventory slot via SendRecv command.

8.3.4 Sending commands

Commands sent to the tag by the reader are called Send Receive commands (SendRecv) and their command code is 0x04. This command sends data to a tag and then waits for the reception of the reply. After the command code byte and length byte, data sent to the tag varies for each request or message sent by the reader for the tag it is communicating with. For example:

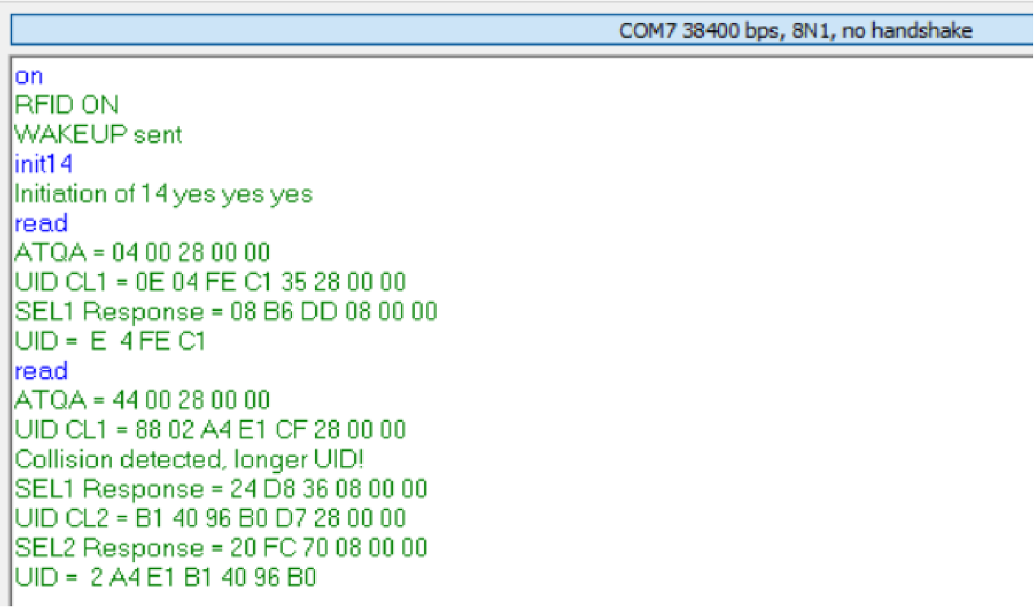
```
const uint8_t cmd_req15[] = {0x04, 0x03, 0x26, 0x01, 0x00};
cr95write(cmd_req15, sizeof(cmd_req15));
```

command will send a earlier mentioned request to read a inventory - 1 slot of the tag with uplink properties being 100% ASK, ¼ coding and downlink properties being high data rate and single sub-carrier. Composition of these commands and various related information and examples can be found in the datasheet either in the description of the commands or in the Appendix D – Examples [11].

8.3.5 UART Commands

Multiple approaches to control the actions of the reader can be implemented. One example of this approach is a reader reading in an endless loop with a pre-set delay; the second example being pre-programmed commands which will be sent to the reader for execution. For the development phase, the second option makes more sense as it is easier to debug each step of the program individually. The function *uart_process_command* was designed to serve such purpose. It reads the user's input into the UART 2 and executes any command assigned to the input. Here is the list of all the inputs and their commands:

- ON → Initializes UART 1, sends the wakeup command and turns on the LED.
- OFF → Deinitializes UART 1 and turns off the LED.
- ECHO → Verifies the possibility of communication.
- IDN → Requests short information about the CR95HF and its revision.
- INIT(standard) → Initializes the standard of user's choice.
- READ(standard) → Reads the UID of the tag .
- CALIBRATE → Turns on the Tag detection calibration procedure.
- IDLE → Sets the reader into Idle state.
- WAKEUP → Sends the wakeup command to the reader.
- AUTO → Sets the reader into Tag detection state.



```
COM7 38400 bps, 8N1, no handshake
```

```
on
RFID ON
WAKEUP sent
init14
Initiation of 14 yes yes yes
read
ATQA = 04 00 28 00 00
UID CL1 = 0E 04 FE C1 35 28 00 00
SEL1 Response = 08 B6 DD 08 00 00
UID =  E  4 FE C1
read
ATQA = 44 00 28 00 00
UID CL1 = 88 02 A4 E1 CF 28 00 00
Collision detected, longer UID!
SEL1 Response = 24 D8 36 08 00 00
UID CL2 = B1 40 96 B0 D7 28 00 00
SEL2 Response = 20 FC 70 08 00 00
UID =  2 A4 E1 B1 40 96 B0
```

Figure 8.5: Communication with the CR95HF provided by serial terminal

An example of the communication with the CR95HF can be seen in Figure 8.5. The user has full control of what is happening with the reader and could easily demonstrate the functions of the reader with pre-programmed commands. Entering the earlier mentioned inputs will carry out the desired command and displays the information as a response. It is worth mentioning that the final program will work with any serial terminal after setting up the right properties.

8.4 Tag detection calibration

According to the [11], when the transceiver CR95HF is set to the tag detection mode, it regularly emits RF bursts and measures the current in antenna (I_{DRIVE}). When transponder enters the readers field, it modifies the antenna loading characteristics and induces a change in I_{DRIVE}. This new value must be compared to the reference value established during the tag detection calibration process. (Note that values are converted to digital representation via 6-bit DAC.) This enables the transceiver to decide whether the tag has entered or not the field of reader. The calibration process must be done without any tag in the proximity of the reader in order to establish the correct reference value. The reference value (DacDataRef) will be reused to define the tag detection parameters (DacDataL and DacDataH).

During the process of calibration, DacDataL value is set to 0x00 and DacDataH value is changed by the program from its maximum (0xFE) to the minimum (0x00). The outcome of the calibration is a DacDataRef which correlates with DacDataH for which the wake-up event switches from time-out to tag detect. In the beginning, program forces the wake-up event to be both tag detect and time-out to test out proper the functionality:

```
uint8_t cmd_cal[] = { 0x07, 0x0E, 0x03, 0xA1, 0x00, 0xF8, 0x01, 0x18, 0x00,
0x20, 0x60, 0x60, 0x00, 0x00, 0x3F, 0x01 };

cmd_cal[13] = 0x00; //wake-up event (data[0]) must equal tag detect (0x02)
cr95write(cmd_cal, sizeof(cmd_cal));
printf("CAL #0 0x%02x %c, result 0x%02x\n", cmd_cal[13], (cr95read(data, &len)
== 0x00) ? 'y' : 'n', data[0]);
cmd_cal[13] = 0xFC; //wake-up event (data[0]) must equal time-out (0x01)
cr95write(cmd_cal, sizeof(cmd_cal));
printf("CAL #1 0x%02x %c, result 0x%02x\n", cmd_cal[13], (cr95read(data, &len)
== 0x00) ? 'y' : 'n', data[0]);
```

After the first two test calls, the program will start to decrease the DacDataH value until it reaches wake-up event to tag detect. Once it is reached, the value will be increased to find the precise point of the change. Steps for decreasing/increasing are as follows: -0x80, +/-0x40, +/-0x20, +/-0x10, +/-0x8, +/-0x4, -0x4 (1 DAC step equals 0x04, therefore it is the smallest change in calibration). Observe the code for one iteration of the calibration:

```
if (data[0] == 0x01) cmd_cal[13] -= 0x40; else cmd_cal[13] += 0x40;
cr95write(cmd_cal, sizeof(cmd_cal));
```

At the end of the calibration procedure, corresponding DacDataH is stored as a reference value DacDataRef. To avoid too much of sensitivity, [11] recommends using guard band of 0x08 for the DacDataL and DacDataH used in the idle command.

$$\mathit{DacDataL} = \mathit{DacDataRef} - \mathit{Guard}\ \textit{and}\ \mathit{DacDataH} = \mathit{DacDataRef} + \mathit{Guard}$$

8.5 Modes of reader operation

After powering up the device, the application can work in two modes: Manual operation and Automatic operation. These modes can also be switched by pressing a button. In manual operation, the reader is solely operated by the *uart_process_command* function. In this mode, the reader waits for each command made by the user to be executed. It is also ideal for debugging and testing of the functionalities possible within the CR95HF.

In automatic operation, the reader operates according to preset commands. Most of the commercially sold RFID readers usually work on their own without any input from the user needed. Therefore, in automatic operation, after powering up the device and running through the echo command to make sure communication is established, the reader goes directly into the tag detection mode. The preset commands are as follows:

```
uart_process_command(“on”);
HAL_Delay(5000);
uart_process_command(“echo”);
uart_process_command(“auto”);
```

It is also worth mentioning, that the serial terminal does not have to be used at all in this case. This is possible due to the reader being in the tag detection mode, which operates on its own, and also having a display showing the data which would be normally shown in the terminal. Due to the size of the display, it does not show all of the data, but works more like a conventional reader only showing the most important information (UID or Error). Another possibility is to have LEDs show the outcome of the reading (Green = successful reading, Red = error) or a buzzer signaling the reading process was carried out.

8.6 Source codes

The entire application with all of its source codes, libraries and other files is available at GitHub repository https://github.com/MichalObs97/RFID_CR95HF_VUT/. This program is a free software: you can redistribute it and/or modify it under the terms of the GNU General Public license as published by the Free Software Foundation, either version 3 of the License, or any later version.

9. TESTING OF THE READER

After designing and assembling the RFID reader together, it is required to test out the functionality, tag detection calibration and read ranges of the antennas. As the test of the functionality is fairly simple, this chapter will focus mainly on comparing the read ranges of antennas and tag detection calibration procedure. As mentioned in chapters 6 and 7, part of this project is to have multiple antennas in order to compare how different parameters influence the reading ability of the antenna. Therefore, two different sets of experiments (antennas tuned by ST software and network analyzer) were performed, assuring that the wider scope of comparisons is included.

In theory, antennas with higher inductance values offer a wide band matching, which is supposed to be an improvement for communication. Along with this, higher inductance is caused by more turns of the conductive trace, and more turns allows for a better coupling factor with the transponder. Contrarily, antennas with lower inductance offer a much narrower band in combination with large Q factor. The generated field becomes higher, in part to much lower impedance; therefore, the reading distance should be higher, and the transponders based on ISO/IEC 15693 should theoretically work better.

9.1 Antennas tuned by software

Testing of the antennas tuned by ST software mentioned in chapter 7.3.

9.1.1 Comparison of reading ranges using different transponders

In the Experiment number 1, comparison between antennas using 5 different transponders, based on different standard and technologies was carried out. The transponders used in experiment 1 were:

1. ISIC School card – Mifare Classic 1k, NFC-A
2. Bank Card – Mifare Classic 1k, IsoDep, NFC-A
3. Bank Card – Mifare Plus, IdoDep, NFC-A
4. Circle tag – Mifare Classic EV1
5. ISO/IEC 15693 tag – NFC-V

The first transponder is a basic Mifare classic school card, similar to other access cards used throughout the world. Alternatively, the next two card transponders, are bank cards used for contactless payments with one being Mifare classic and other being Mifare Plus. The next transponder used in this experiment is circle tag normally used as a access key to an apartment building. In this case, the size and shape of the transponder is different to the cards used earlier, therefore comparing how different shaped and sized tags work with different shaped and sized antennas. The last transponder is ST25TV-eSEAL, a tag based on ISO/IEC 15693 standard and NFC Forum type 5.

The diversity of using various shapes, standards and technologies will serve as a strong indication for testing the maximum possible reading range of antennas in various scenarios. The reader was set in tag detection mode, which automatically detects the presence of the transponder in its field. For each combination of transponder and antenna individually, 2 sets of 10 measurements were performed. For each set, the maximum reading distance was recorded (distance obtained by using electronic digital caliper) and then averaged with the value from the second set. Results of the experiment 1 are as follows in the Table 13.

Size [mm] / turns	Inductance	ISIC – Mifare classic 4B [mm]	Bank – Mifare classic 7B [mm]	Bank – NXP Mifare Plus [mm]	Circle – Mifare classic [mm]	ISO 15693 tag [mm]
60x18 / 2	357.66 nH	21.8	18.6	18.7	9.3	26.6
60x18 / 4	932.95 nH	15	13.7	14.5	6	20
60x18 / 6	1.38 µH	11.9	12	11.9	4.3	15.7
47x34 / 2	426.68 nH	21.3	18.2	18.9	9.8	26.8
47x34 / 4	1.22 µH	17.9	18.1	18.5	8.2	26.9
47x34 / 6	2.1 µH	15.4	14.2	16.8	7.1	24.3

Table 13: Comparison of maximum reading distances using different transponders

From the results of experiment 1, is it possible to determine that the ISIC school card was in most cases detected slightly earlier than other two bank cards. Although the bank cards were detected slightly later than school card, the reading process was successful in almost 100% cases with only 4 out of 240 readings resulting in error. This cannot be said about the school card rate of success. While both 6 turns antennas were approximately 95% successful in their readings at the maximum distance, the other two 47x34 antennas were successful in only 50% of the cases and other two 60x18 antennas were only successful a meekly 10% of the time. The 47x34/4 antenna started to work reliably with almost a 100% success rate at around 15.5 millimeters and the 47x34/2 antenna at around 18 millimeters. This loss of 1/7 from maximum reading distance to have reliably working antenna is a fair tradeoff. The remaining two 60x18 antennas were not so generous with their tradeoffs. They both started to work with almost 100% success rate at around 6 millimeters and were very dependent on rotation and position of the transponder. The circle transponder had in comparison to other transponders had a much lower maximum reading range. The success rate of every antenna was 100% when the tag was as close as 5 millimeters. With ranges over 5 millimeters, the success rate went down with inductance, as also shown with the school card.

It is important to note that in all of the test cases regarding ISO/IEC 14443A tag, REQA and ATQA went through successfully. Later, in the cases resulting in error, the problem occurred solely inside the anti-collision loop. That proves that even tags which were not successful in the whole communication process were at least detected and acknowledged by the reader. Since tags based on ISO/IEC 15693 do not have to go through the process of anti-collision, the success rate of readings was 100% throughout all of their test cases. Also worth mentioning is that the maximum reading distance was approximately 5 millimeters more than the best ISO/IEC 14443A tag, which is a significant improvement.

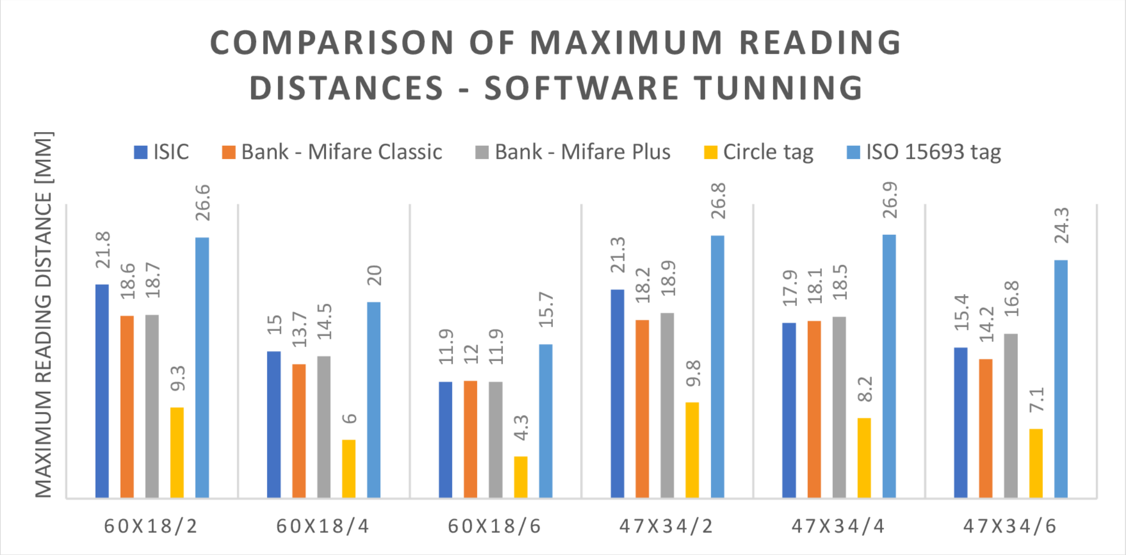


Figure 9.1: Comparison of maximum reading distances using different transponders

Another observation from the experiment is that, while antennas with 6 turns were successful in completing the communication procedures, they were slightly more inconsistent in keeping the maximum distance on the same value. While other antennas started to work in all 20 measurement around same value, antennas with 6 turns differed in some cases as much as 1 millimeter.

9.1.2 Testing of the Tag detection calibration procedure

As described in chapter 8.4, tag detection calibration determinates the reference I_{DRIVE} value for current in the antenna without any tag in proximity. This value is represented by the DacDataRef variable in the program, which is calculated in the calibrate command of the *uart_process_command* function. This value could differ for each antenna, so in the Table 14, it is possible to see the results for each antenna, respectively. For each antenna, a calibration procedure was performed 10 times to ensure the repetition aspect of the experiment.

Antenna	X-NUCLEO-NFC03	47x34 / 2 turns	47x34 / 4 turns	47x34 / 6 turns	60x18 / 2 turns	60x18 / 4 turns	60x18 / 6 turns
Reference value	0x80	0x44	0x74	0x74	0x4c	0x5c	0x5c

Table 14: Reference values from calibration procedure

Out of 10 repetitions, X-NUCLEO-NFC03 and antennas with 2 turns kept the same reference value throughout all of them. In the case of remaining antennas, they shifted the reference value as one step of DAC (+/- 0x04) in 1 or 2 out of 10 measurements. This occasional shift does not have any effect in real use of the reader because of guard band (4 steps of DAC wide) mentioned earlier. Another observation visible from the results is that antennas with lower inductance have also lower reference values, meaning lower I_{DRIVE} needed to trigger the wake-up event to tag detect.

9.2 Antennas tuned by network analyzer

Testing of the antennas tuned by network analyzer mentioned in chapter 7.4.

9.2.1 Comparison of reading ranges using different transponders

The second set of experiments is fundamentally the same as the previous set with the only difference between the sets being the calibration of antennas. In the first set of experiments, antennas used were based solely on software calculations. In this set of experiments, antennas were measured on a network analyzer to ensure that performance of the antenna is at its finest. The goal was to compare how much the software calculator can match values that are measured and tuned on the actual antenna. The results of the second set of experiments are as follow:

Size [mm] / turns	Inductance	ISIC – Mifare classic 4B [mm]	Bank – Mifare classic 7B [mm]	Bank – NXP Mifare Plus [mm]	Circle – Mifare classic [mm]	ISO 15693 tag [mm]
60x18 / 2	414 nH	22.5	20.8	20.7	11.3	32.6
60x18 / 4	1.04 µH	17.6	15.8	15.5	7.3	24.3
60x18 / 6	1.53 µH	14.1	13.8	13.9	6.2	18.6
47x34 / 2	474 nH	29.3	24.6	24.9	12.9	36.7
47x34 / 4	1.29 µH	24.5	22.1	22.8	11.2	34.5
47x34 / 6	2.15 µH	22.3	19.2	19.0	10.4	32.2

Table 15: Second comparison of maximum reading distances using different transponders

The results show a small improvement in the reading range on all of the 60x18 antennas and decent improvement on all of the 47x34 antennas. However, not only did the reading range improved, but the biggest improvement happened in the success rate of readings. Previously, the school card in combination with antennas 60x18/2 and 60x18/4 worked only at 10% of the times. After tuning antennas on the network analyzer, the success rate jumped to approximately 85%. The same occurred with the rest of the transponders that only worked 50% of the times before the tuning and went up to 95% after the tuning. As far as usability of the reader, raising the success rate of reading is the most important improvement, because the anti-collision process goes fully through. Without tuning, it would be fatal error, that would make the reader practically unusable. Improvement in reading range is not very substantial when it comes to the everyday use of the RFID reader and the user would hardly notice any difference.

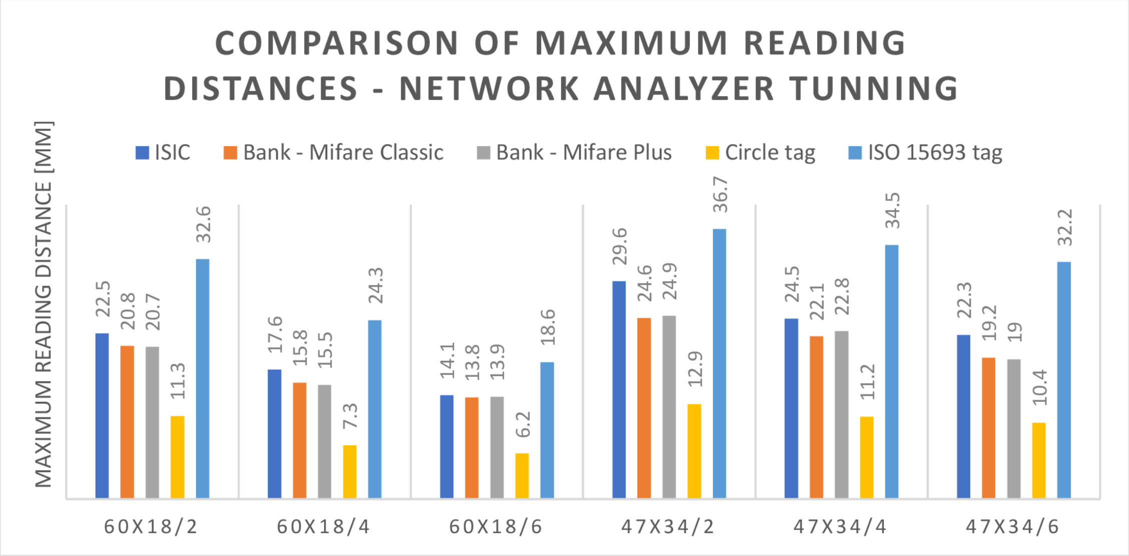


Figure 9.2: Second comparison of maximum reading distances using different transponders

9.2.2 Testing of the Tag detection calibration procedure

Another experiment was executed to notice the changes in the tag detection calibration process. It is possible to observe that tuning also influenced the DacDataRef value converted from I_{DRIVE}. Full results are displayed in the Table 16.

Antenna	X-NUCLEO-NFC03	47x34 / 2 turns	47x34 / 4 turns	47x34 / 6 turns	60x18 / 2 turns	60x18 / 4 turns	60x18 / 6 turns
Reference value	0x80	0x6C	0x7C	0x7C / 0x80	0x60	0x78	0x78

Table 16: Reference values from calibration procedure after the antenna tuning

The results of the second experiment indicate the fact that each antenna's hexadecimal value raised couple of DAC steps. When comparing all 6 of the antennas, it is clear to see that lower inductance antennas still have a smaller number than the rest of them. Also worth mentioning is the fact that apart from the 47x34/6 antenna which kept switching between values 0x7C and 0x80 with 50% chance of each, other antennas did not move a single DAC step and kept the same values throughout all 10 measurements this time. That is again an significant improvement and with the combination of guard band will make the antennas more stable.

9.3 Test results

It is safe to say that tuning the antennas to the best possible result will greatly improve their usability. While software tuning provided a decent working solution with decent reading range, tuning the resonant frequency closer to the desired 13.56 MHz proved to make the antennas more stable with slight reading range improvement.

Table 17 shows the impact, network analyzer tuning had on the results in comparison to the tunning by software calculators. It is worth mentioning that the change in reading range for 43x34 antennas might appear as a notable change, however the improvements were realistically in the range of 6-8 millimeters, which is negligible change for real life application. The biggest difference between the results for the tuning procedures was in the repeatability and success of communication. As mentioned before, this change has an enormous impact on the final product making it a stable, reliable device. For a commercially sold products like RFID door openers, school card readers etc., it is a must to be able to read the transponders consistently. When a customer places their card/key into the reader's field, they will not be bother about the millimeters change in reading range, but if the reading fails multiple times before first successful reading, he will most likely look for another more stable option. Therefore, the designer should always consider tuning the antennas with the network analyzer.

Antenna	60x18 / 2 turns	60x18 / 4 turns	60x18 / 6 turns	47x34 / 2 turns	47x34 / 4 turns	47x34 / 6 turns
Change in inductance	+15.5%	+12%	+11.6%	+11.3%	+5.7%	+2.4%
Change in reading range	+3.2%	+17.3%	+18.5%	+39%	+36.9%	+44.8%
Change in success rate	15→85%	15→85%	95→95%	50→95%	50→95%	95→95%

Table 17: Comparison on how tuning by the network analyzer affected the results. Change in success rate and reading range are from testing of ISIC school card

10. CONCLUSION

The topic of my master's thesis was the RFID Reader for 13.56 MHz Band. My focus was to describe the general problematics of RFID and NFC technology. To begin, I introduced the RFID technology, while describing the basics, physical and operating principles, frequencies on which the usual systems work, and went over the standards ISO/IEC 14443 Type A/B and ISO/IEC 15693, which set the worldwide standards used in this technology.

Secondly, I described the technology of NFC, as it is in relation with RFID. It operates on similar physical and operating principles, the same frequency as HF RFID systems and NFC tags are able to interact with the RFID readers. Near field communication tags can be divided into multiple categories, depending on its data transfer, mode of operation, or according to the NFC forum (non-profit association). All of these categories are described in the theoretical part of my thesis. There are also new standards for specifically this technology, and those are ISO/IEC 18092 or ECMA-340 (NFCIP-1) and ISO/IEC 21481 or ECMA-352 (NFCIP-2).

The following chapter describes the transceiver integrated circuits made by three different companies (ST, NXP, Texas Instruments). This chapter goes over their main features and characteristics to compare three of the most used ICs on the market. The comparation reveals that these transceivers are very similar with just small differences, which could make them unique and separate them from the competition for some specific applications.

For the practical part of semestral project, I first tested the CR95HF transceiver integrated on expansion board X-NUCLEO-NFC03. This is an already working education board for users to get to know the functions of the transceiver. I have designed a program that could read the UID of the basic ISO/IEC 14443 A tags and Mifare classic tags, with the anti-collision process up to 7 byte UID.

For my master's thesis project, I designed a working prototype of a RFID reader board, which connects on top of any microcontroller with Arduino connectors. It contains the transceiver, OLED display, 2 signaling LED's, buzzer for audible signaling, and a button to switch between the working modes and passive components required for operation. On the bottom of the reader is a connector for interchangeable antennas. I designed 6 different antennas (2 different sizes, each having 3 different inductance value) to be able to compare them in different scenarios and how different tuning procedures affects them.

I took the control program made for the semestral project and built upon it. I tweaked the program to fit my reader board and added the option to choose from manual or automatic operation of the reader. I have also added support to read transponders based on ISO/IEC 15693, added support for OLED display and moved all functions that control the CR95HF into its own library file.

With the boards assembled and the control program running, I have performed a calculations of matching circuits trough the software provided by STMicroelectronics and afterwards tested the functionality of each antenna. Eventually, I tuned the antennas on Agilent E5071C Network Analyzer and tested the tested the functionality of each antenna again.

In a conclusion, transponders with antennas which size and shape are comparable to the antennas on reader are recognized in greater distance (for example school card was detected at maximum distance of 29.3 mm while circle key tag only 12.9 mm with the same reader antenna). Another observation I made was that the software solution for impedance matching is not far from reality and provides usable results in the case of reading distance and debugging the functionality. However, in case of the repeatability, software solution lacks a significant amount behind tuning on network analyzer. While difference in the reading distance is negligible, antennas tuned on the network analyzer were successful in more than 90% of their readings overall, which a significant improvement to previous dismal 50%, in some cases even 10% recorded with software solution.

Different scenarios happen when inserting a conductor in the proximity of the reader. Because antennas' inductance is lowering, resonant frequency shifts upwards and even a perfectly tuned antenna will get detuned. Therefore, it is recommended to avoid any conductors in the proximity of an antenna, or in case it is necessary to use the conductor close by, as the antenna must be tuned in the environment it will later be used in.

BIBLIOGRAPHY

[1] CARDULLO, Mario. *Genesis of the Versatile RFID Tag*. 1969. Available at: https://www.rfidjournal.com/genesis-of-the-versatile-rfid-tag?print=pdf

[2] WALTON, Charles. *Portable radio frequency emitting identifier*. USA. US4384288A. Available at: https://patents.google.com/patent/US4384288

[3] LEHMPAMER, Harvey. *RFID Design Principles*. USA: Artech House, 2008, 293 s. ISBN 978-1-59693-194-7.

[4] FINKENZELLER, Klaus. *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. 3rd edition. Munich: John Wiley & Sons, 2010, 462 s. ISBN 978-0-470-69506-7.

[5] DOĞAN, Habib, Mehmet CAGLAR, Musa YAVUZ a Mahmut GÖZEL. Use of Radio Frequency Identification Systems on Animal Monitoring. *SDU International Journal of Technological Science*. 2016, 8, 38-53. Available at: https://www.researchgate.net/publication/308167938_Use_of_Radio_Frequency_Identification_Systems_on_Animal_Monitoring

[6] How to Select a Correct Tag – Frequency. *RFID4u* [online]. [cit. 2020-12-01]. Available at: https://rfid4u.com/rfid-frequency/

[7] About MIFARE: MIFARE - The Brand of Contactless IC Products. *MIFARE* [online]. [cit. 2020-12-01]. Available at: https://www.mifare.net/en/about-mifare/

[8] MIFARE. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-12-01]. Available at: https://en.wikipedia.org/wiki/MIFARE

[9] STMICROELECTRONICS. *TN1216: ST25 NFC guide*: Technical note [online]. [cit. 2020-12-01]. Available at: https://www.st.com/resource/en/technical_note/dm00190233-st25-nfc-guide-stmicroelectronics.pdf

[10] ECMA-352: *Near Field Communication Interface and Protocol -2 (NFCIP-2)*. 3rd edition. Geneva: EMCA international, 2013, 12 s. Available at: https://www.ecma-international.org/publications/files/ECMA-ST/ECMA-352.pdf

[11] STMICROELECTRONICS. *CR95HF: 13.56-MHz multi-protocol contactless transceiver IC with SPI and UART serial access*: Datasheet [online]. [cit. 2020-12-01]. Available at: https://www.st.com/resource/en/datasheet/cr95hf.pdf

[12] TEXAS INSTRUMENTS. *TRF7970A: Multiprotocol Fully Integrated 13.56-MHz RFID and Near Field Communication (NFC) Transceiver IC*: Datasheet [online]. [cit. 2020-12-01]. Available at: https://www.ti.com/lit/ds/symlink/trf7970a.pdf?ts=1602840692892&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FTRF7970A

[13] NXP. *PN532/C1: Near Field Communication (NFC) controller*: Datasheet [online]. 2017 [cit. 2020-12-01]. Available at: https://www.nxp.com/docs/en/nxp/data-sheets/PN532_C1.pdf

[14] NXP. *AN10833: MIFARE Type Identification Procedure*: Application note [online]. 2016 [cit. 2020-12-01]. Available at: https://www.nxp.com/docs/en/application-note/AN10833.pdf

[15] SOLOMON SYSTECH. *SSD1309*: *Advance Information*: Datasheet [online]. 2011 [cit. 2021-05-01]. Available at: http://www.hpinfotech.ro/SSD1309.pdf

[16] TEXAS INSTRUMENTS. *Antenna Design Guide for the TRF79xxA*: Application note [online]. 2020 [cit. 2020-12-01]. Available at: https://www.ti.com/lit/an/sloa241c/sloa241c.pdf?ts=1604262384140&ref_url=https%253A%252F%252Fwww.google.com%252F

[17] NXP. AN11564: *PN7120 Antenna Design and Matching Guide*: Application note [online]. 2016 [cit. 2020-12-01]. Available at: https://www.nxp.com/docs/en/application-note/AN11564.pdf

[18] STMICROELECTRONICS. *EDesign Antenna* [online]. [cit. 2020-12-01]. Available at: https://eds.st.com/antenna/

[19] STMICROELECTRONICS. *AN4327: CR95HF transceiver antenna tuning circuit with EMI filter*: Application note [online]. 2019 [cit. 2020-12-01]. Available at: https://www.st.com/resource/en/application_note/dm00089926-cr95hf-transceiver-antenna-tuning-circuit-with-emi-filter-stmicroelectronics.pdf

[20] STSW-ST25R003: ST25R95 EMI filter calculation tool. *STMICROELECTRONICS* [online]. [cit. 2021-05-01]. Available at: https://www.st.com/content/st_com/en/products/embedded-software/st25-nfc-rfid-software/stsw-st25r003.html

LIST OF SYMBOLS AND ABBREVIATIONS

Abbreviations:

FEKT	…	Fakulta elektrotechniky a komunikačních technologií
VUT	…	Vysoké učení technické v Brně
RFID	…	Radio frequency identification
NFC	…	Near field communications
UID	…	Unique identifier
UART	…	Universal Asynchronous Receiver/Transmitter
SPI	…	Serial Peripheral Interface
HDX	…	Half duplex
FDX	…	Full duplex
EEPROM	…	Electrically erasable programmable read-only memory
FRAM	…	Ferroelectric random-access memory
LF	…	Low frequency
HF	…	High frequency
UHF	…	Ultra-high frequency
ISO	…	International Organization for Standardization
IEC	…	International Electrotechnical Commission
EMI	…	Electromagnetic interference
IC	…	Integrated Circuit
MCU	…	Microcontroller unit
GPIO	…	General purpose input output
LED	…	Light emitting diode
OLED	…	Organic light emitting diode
SAK	…	Select acknowledgement
DAC	…	Digital to analog converter

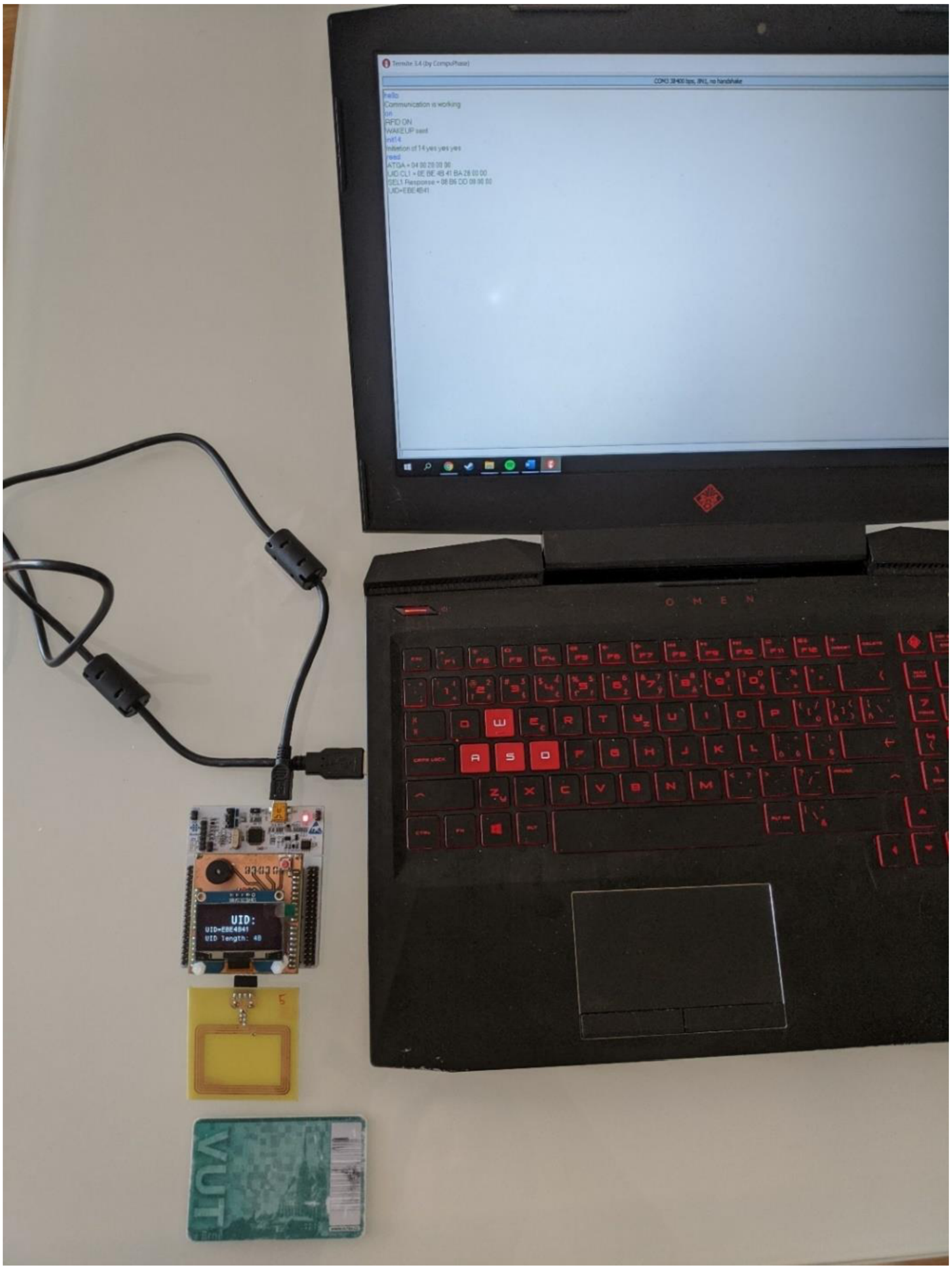
Symbols:

U	…	Voltage	[V]
I	…	Current	[A]
f	…	Frequency	[Hz]
L	…	Inductance	[H]
C	…	Capacitance	[F]

LIST OF APPENDICES

Appendix A – Final connection + list of readings 63
Appendix B – Return loss of tuned antennas 64
Appendix C – Smith charts of tuned antennas 65
Appendix D – OLED display interface 66

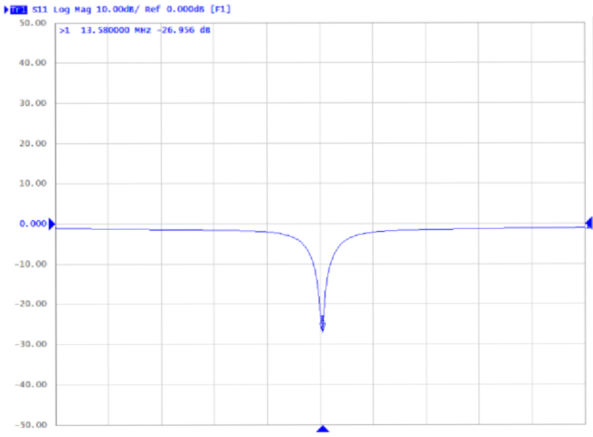
Appendix A – Final connection + list of readings


Termite 3.4 (by CompuPhase)
COM3 38400 bps, 8N1, no handshake
UID:
UID=EBE4841
UID length: 48
OMEN
5
VUT

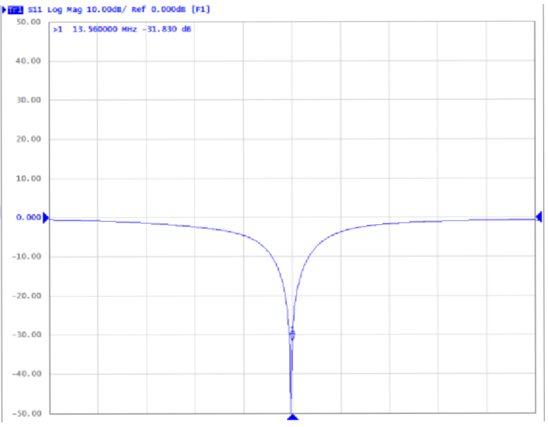
```
hello
Communication is working
on
RFID ON
WAKEUP sent
init14
Initiation of 14 yes yes yes
read
ATQA = 04 00 28 00 00
UID CL1 = 0E BE 48 41 BA 28 00 00
SEL1 Response = 08 B6 DD 08 00 00
UID=EBE4841
```

Appendix B – Return loss of tuned antennas

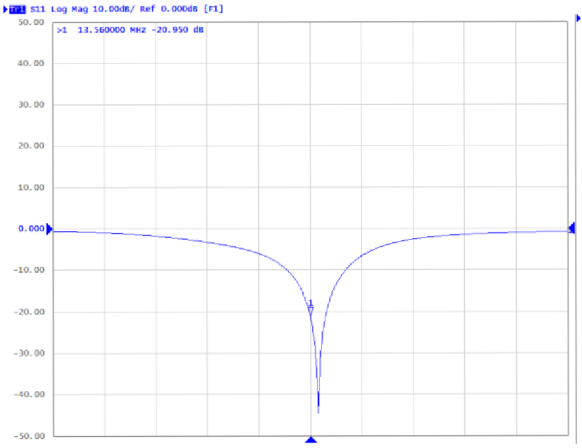
60x18 / 2



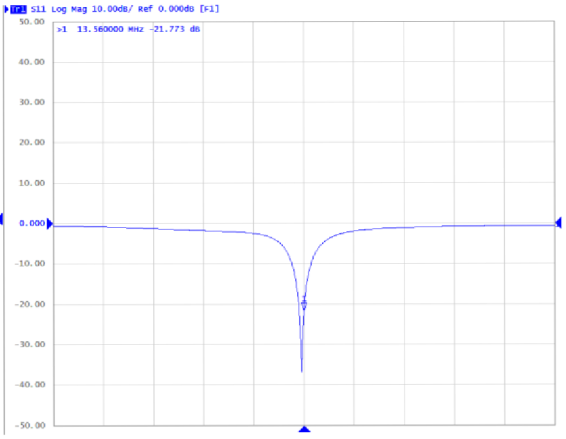
60x18 / 4



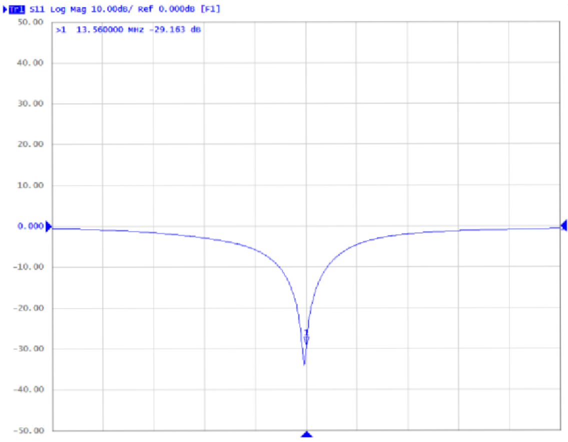
60x18 / 6



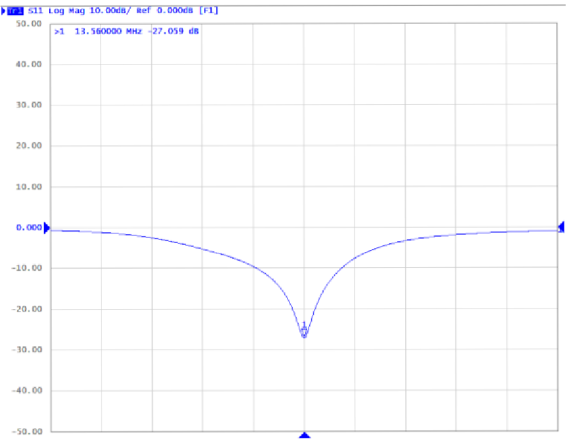
47x34 / 2



47x34 / 4

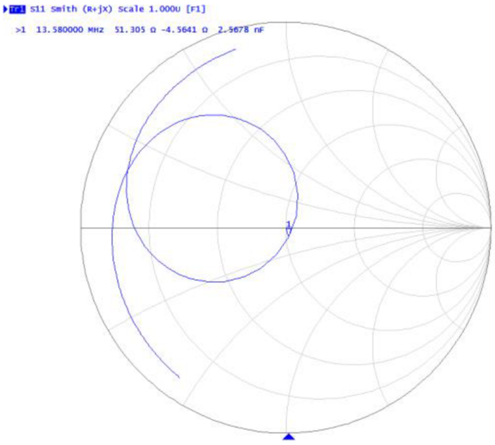


47x34 / 6

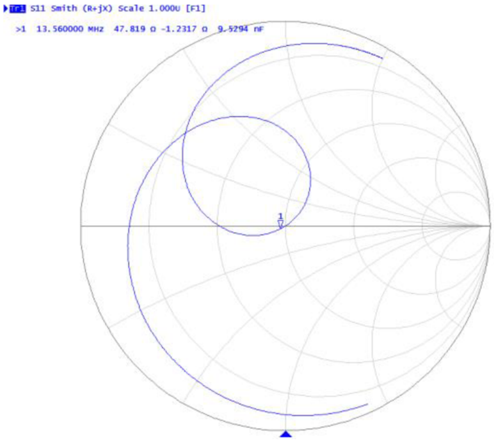


Appendix C – Smith charts of tuned antennas

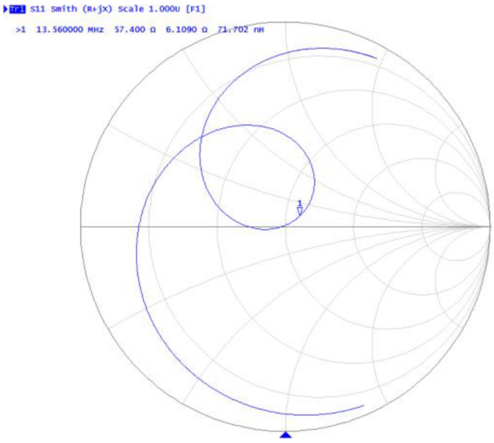
60x18 / 2



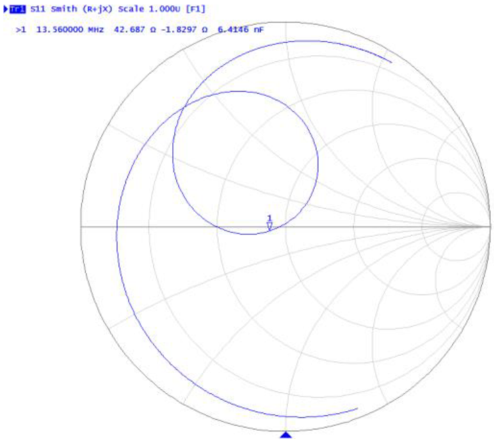
60x18 / 4



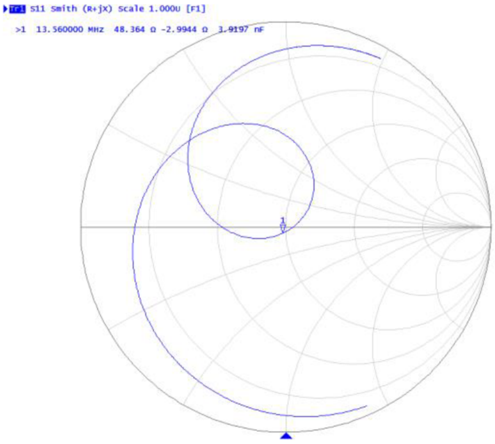
60x18 / 6



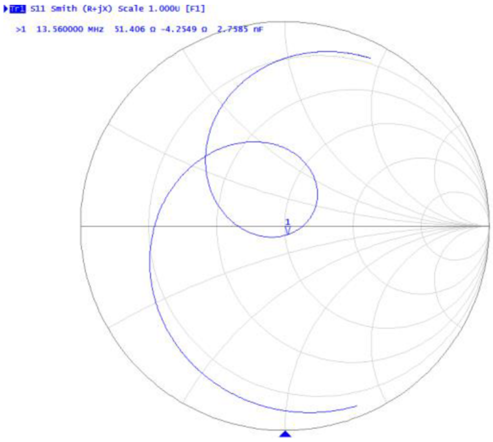
47x34 / 2



47x34 / 4

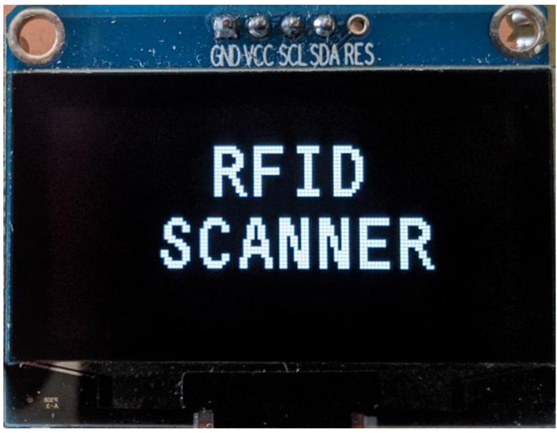


47x34 / 6



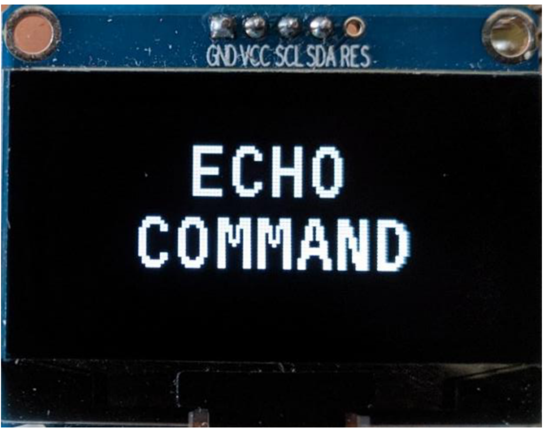
Appendix D – OLED display interface

a) Home screen



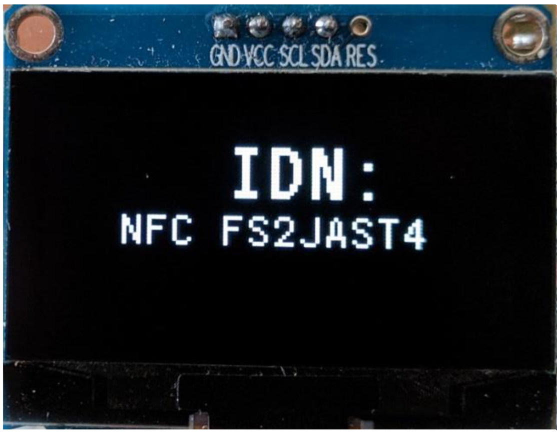
RFID
SCANNER

b) Executing Echo Command



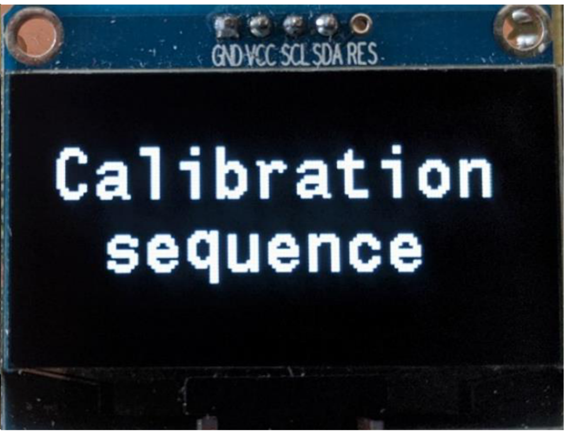
ECHO
COMMAND

c) Executing IDN Command



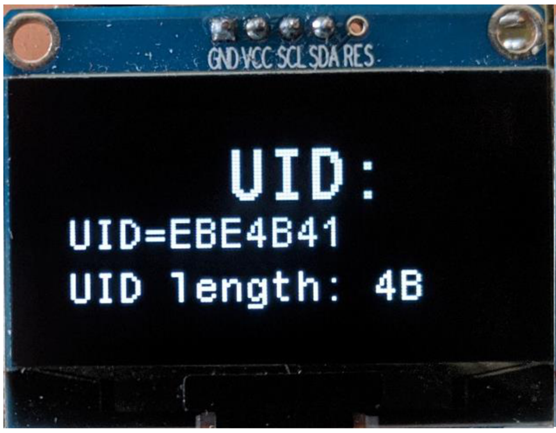
IDN:
NFC FS2JAST4

d) Calibration process



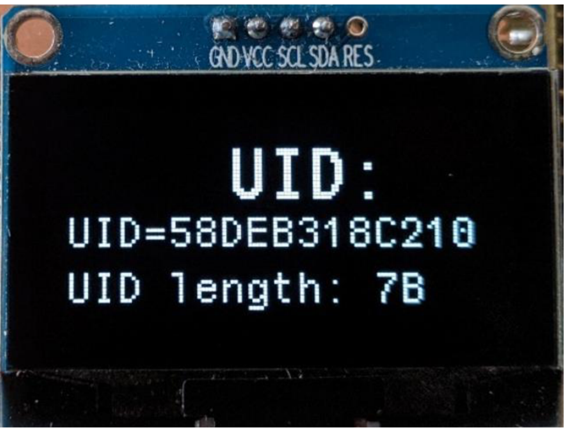
Calibration
sequence

e) Transponder with 4B long UID



UID:
UID=EBE4B41
UID length: 4B

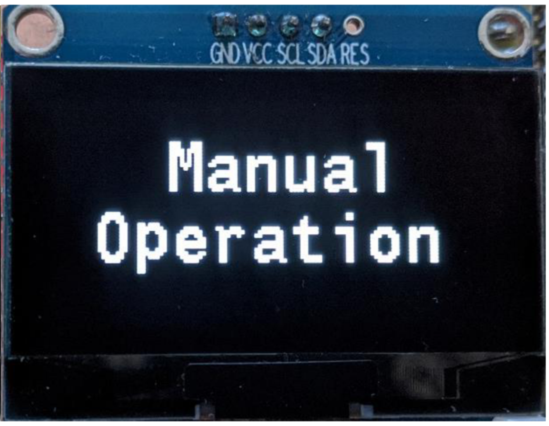
f) Transponder with 7B long UID



UID:
UID=58DEB318C210
UID length: 7B

g) Error occurred during reading

h) manual operation



i) Automatic operation