Dominik Lämmerer, BSC

Proposing methods to improve the LPCD range of RFID/NFC systems by modifying the transponder

MASTER'S THESIS

to achieve the university degree of

Master of Science

Master's degree programme: Electrical Engineering

submitted to

Graz University of Techology

Supervisor

Univ.-Prof. Dipl.-Ing. Dr.techn., Bernd Deutschmann

Institute of Electronics

in cooperation with

NXP Semiconductors

Supervisor

Dipl.-Ing., Franz Amtmann

Graz, January 2019

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used.
The text document uploaded to TUGRAZonline is identical to the present master‘s thesis dissertation

_____ _____

Date Signature

Abstract

Most current RFID applications use a stationary reader with constant power supply, but with the recent increasing use of mobile readers and NFC devices such as smartphones, power conservation has become even more important. To address this problem a lot of devices implement a Low Power Card Detection, which enables them to detect if a transponder is present in the vicinity and reduce the time in which the field is turned on and therefore save power. In this thesis different methods to perform this LPCD are summarized and the underlying concepts identified. Then a Demonstrator Board is designed and manufactured to analyse the impact of electrical properties of the transponder on these methods. This is done to point out possible improvements in the transponder design that make the transponder easier to be detected. Finally, the findings are condensed, and suggestions given to optimize the performance.

Table of Contents

1 INTRODUCTION 7

1.1 RFID AND NFC 7
1.2 DIFFERENT RFID SYSTEMS 8
1.3 A TYPICAL PASSIVE SYSTEM 9
1.3.1 Reader 9
1.4 PASSIVE TRANSPONDER 10
1.5 AIR INTERFACE 12
1.5.1 Energy Transfer 13
1.5.2 Forward Link 13
1.5.3 Return Link 13
1.6 IMPORTANT PARAMETERS 14
1.6.1 Coupling coefficient 14
1.6.2 Hmin 15
1.6.3 Resonance and Quality factor 15
1.6.4 Operating Ranges 17
1.6.5 Transimpedanz 18

2 BACKGROUND 19

2.1 LOW POWER CARD DETECTION 19
2.1.1 Antenna Voltage 21
2.1.2 Oscillation Behaviour 22
2.1.3 PN5180 LPCD 23
2.2 FREQUENCY WOBBLING 24

3 IMPROVEMENT METHOD 25

3.1 MOTIVATION 25
3.2 CONCEPT 25
3.2.1 Simulation of Detuning 25
3.2.2 Simulation of Capacitor Switching 27
3.3 DESIGN 30
3.3.1 Antenna 31
3.3.2 Energy Sink 32
3.3.3 Capacitor Bank 33
3.3.4 Rectifier 34
3.3.5 Comparator 35
3.3.6 Supply 36
3.3.7 Circuit Protection 37
3.3.8 Arduino 38
3.4 SIMULATION OF THE DEMONSTRATOR 39
3.5 PCB LAYOUT 40
3.5.1 Electromagnetic Compatibility Aspects 40
3.5.2 Design Flow 41

4 EVALUATION 44

4.1 TEST SETUP 44
4.2 FIELD DETECTION 45
4.3 LPCD 46
4.4 DETUNING 48
4.5 EVALUATION BOARD 50
4.6 CARD DETECTION RANGE OF A SMARTPHONE 54

5 DISCUSSION 55

List of Figures

Figure 1: Simplified model of a RFID system 9
Figure 2: Simplified schematic of a RFID reader 10
Figure 3: Simplified schematic of a passive RFID transponder. 11
Figure 4a: Block diagram of the communication on the reader side. 12
Figure 4b: Block diagram of the communication on the transponder side. 12
Figure 5: Example resonance curve with different quality factors. 17
Figure 6: Oscilloscope picture of LPCD and polling pulses from the Sony Xperia X. 21
Figure 7: Behaviour of the reader antenna voltage after turning the field off. 22
Figure 8: Behaviour of the reader antenna voltage while performing frequency wobbling. 24
Figure 9: Circuit used for the simulation of detuning. 26
Figure 10: Effect of tuning on the reader antenna voltage. 27
Figure 11: Circuit used for the simulation of switching capacitors. 28
Figure 12: Effect of switching capacitors on the transponder. 29
Figure 13: Block diagram of the designed transponder substitute. 30
Figure 14: Schematic of the antenna block. 31
Figure 15: Schematic of the energy sink. 32
Figure 16: Schematic of the capacitor bank. 33
Figure 17: Schematic of the rectifier block. 34
Figure 18: Schematic of the comparator block. 35
Figure 19: Schematic of the supply block. 36
Figure 20: Schematic of the circuit protection block. 37
Figure 21: Example Arduino code for interrupt and trigger test. 38
Figure 22: Example Arduino code for port manipulation 39
Figure 23: Circuit used for the Demonstrator simulation. 39
Figure 24: Effect of switching capacitors on the transponder simulated with real models. 40
Figure 25: PCB Layout. 43
Figure 26: Assembled Demonstrator Board 43
Figure 27: Laboratory test setup 44
Figure 28: Field detection signals oscilloscope screenshot. 45
Figure 29: Card detection with normal transponder behaviour. 46
Figure 30: Card detection with modified transponder. 47
Figure 31: Equivalent circuit of the Demonstrator board. 48
Figure 32: Plot of Demonstrator board resonant frequencies. 49
Figure 33: NFC Cockpit LPCD GUI. 50
Figure 34: Plot of AGC value over capacitance. 51
Figure 35: Plot of AGC values for different tags. 52
Figure 36: Plot of AGC value improvement. 53
Figure 37: Plot of LPCD range improvement. 54

List of Tables

Table 1: LPCD parameter for different smartphones. 20
Table 2: Special devices used for the Demonstrator Board. 63
Table 3: Resonant frequency measurement data. 64
Table 4: Capacitance vs AGC Value measurement data. 65
Table 5: Distance vs AGC Value for different tags measurement data. 66
Table 6: Distance vs AGC Value for different tunings measurement data 67
Table 7: Detection ranges measurement data. 67

Glossary

AGC	Automatic Gain Control
ASK	Amplitude Shift Keying
DPC	Dynamic Power Control
EEPROM	Electronically Erasable Programmable Read Only Memory
IC	Integrated Circuit
IEC	International Electrotechnical Commission
ISO	International Standard Organisation
LPCD	Low Power Card Detection
NFC	Near Field Communication
OPA	Operational Amplifier
PCB	Printed Circuit Board
PSU	Power Supply Unit
RFID	Radio Frequency Identification
RTF	Reader Talks First
SMD	Surface Mounted Device
VCD	Vicinity Coupling Device
VICC	Vicinity Integrated Circuit Card

1 Introduction

1.1 RFID and NFC

The fundamentals of wireless power transmission have been researched as far back as the 19th century. The concept of transmitting energy through near field inductive and capacitive coupling has been demonstrated by Nikola Tesla's wireless light experiment and tesla transformer [1], which already used a resonant tank to increase the efficiency over longer distances. These systems were only used to transmit power, but not data as in modern applications. The fundamentals of Radio Frequency Identification (RFID) technology have been laid in 1948 by Harry Stockman's "Communication by Means of Reflected Power" [2] which proposed a way to communicate by reflecting a radar signal and transmitting information by modulating the radar cross section of the target. This principle is similar to backscatter RFID systems used today. With the upcoming of integrated circuit technologies in the late 1950s and early 1960s it was possible to develop the today known RFID systems. From there the wide spread application of RFID started with electronic article surveillance systems in the 1970s and are still widely used today. These systems use binary transponders that do not require any logic and are therefore easy and cheap to produce. Jürgen Dethloff and Helmut Gröttrup were the first to patent an identification card in 1969 [3] which allowed for identification at a gas station utilizing an integrated circuit on the card. In the 1990s proximity cards became widely used for ticketing and payment systems. These systems were conceived for local applications in the beginning and are gradually being standardised up to this day. Nowadays, there is a huge variety of systems utilizing the effects of coupled electromagnetic fields, where most of them use inductive coupling in a magnetic near field. These systems are referred to as NFC systems (near field coupling or near field communication). For compatibility reasons, the physical parameters as well as digital commands are defined in technical standards in the form of ISO/IEC standards. There is a big number of applications for which these systems are used today mostly being ticketing, contactless payment and access control, but also animal identification, toll collection, logistic systems etc. Another aspect of NFC is the concept of using it as a communication protocol like Bluetooth. This means that

the communication can be performed with a dynamically changing system structure, so that one device can act as a reader, passive transponder or Peer to Peer Device. The function of each device can be negotiated between multiple devices and changed during communication. The necessary technology is already implemented in newer smartphones and is sure to see a further increase in the near future.

1.2 Different RFID Systems

In order to categorize the different RFID systems, it is helpful to distinguish them by their operating frequencies, which is crucial for their functionality. In the low frequency range are systems that operate at DC level up to 30 MHz having a very short range. They are therefore referred to as close coupling systems and are used mostly in smart cards like credit cards or access control cards with ID1 format specified in ISO/IEC10536 [4] with a typical range of 1cm. Because of the small range, it is well suited for these security sensitive applications as spying on the communication becomes more difficult. Also, it simplifies the energy transfer to an extend that a passive transponder does not have to be power consumption optimized and can perform sophisticated operations like encryption. Opposed to longer range systems these can use both, electric and magnetic coupling.

The next higher tier in terms of range are remote coupling systems and account for the majority of currently used systems. These systems use magnetic coupling and operate at frequencies up to 135kHz or at special ISM Band frequencies of 6.78MHz, 13.56MHz and 27.12MHz, where 13.56MHz is the most widely used. The technical properties of these systems are specified in standards that are specific to the application, including proximity coupling cards (ISO/IEC 14443) [5] with a range up to 10cm and vicinity coupling cards (ISO/IEC 15693) [6] up to 1m. The highest ranges are realized by so called long range systems with a range of above 1m up to about 15m with passive transponders and even up to a few hundred meters with active and battery assisted transponders. They operate at frequencies in the UHF and Microwave spectrum 868MHz band, 915MHz band, 2,5GHz band and 5,8GHz band. The transponders operate outside of the near field region and are therefore not magnetically coupled. Most systems operate with the backscatter principle, where a

part of the electromagnetic wave is reflected by the transponder antenna similar to a RADAR application. Other systems utilize surface wave effects. One application for long range systems are for example toll control systems on highways, where a long range is needed.

1.3 A typical passive System

For the scope of this thesis a typical RFID System consist of a handheld NFC Device (Smartphone) functioning as a Reader operating at a frequency of 13.56MHz and a passive transponder (also referred to as tag or label). In Figure 1 the function of such a system is shown in a simplified form.

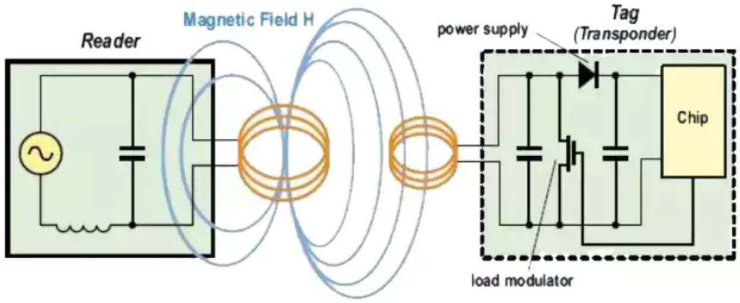

Figure 1: Simplified model of a RFID system.

Source: https://www.mouser.at/images/microsites/rfid-gains-figure-1.jpg

Usually the reader is a stationary device embedded in some kind of structure like a gate or an ATM. The usage of a handheld reader adds additional constraints to the systems, the most critical being the power consumption, but also antenna size and additional metal objects like batteries that can obstruct the field. As a result, the implementation of these readers is different for every smartphone. The appearance of the transponder mainly depends on the antenna size whereas in this thesis an ISO/IEC14443 class 1 compliant antenna also known as an ID1 antenna is used.

1.3.1 Reader

The reader is the active part of the communication system as it generates the magnetic field. This is done by an AC current with 13.56MHz that is send through the antenna. In order to increase the current in the antenna a resonant circuit is formed. This is done by placing a capacitance parallel to the inductance of the antenna loop, as shown in

Figure 2, or by an appropriately designed matching network.
This carrier signal can be modulated to transmit data through the field. The reader is also the communication initiating device (RTF reader talks first), meaning that all communication is done by sending commands to the transponder and then waiting for a response. This response is received by observing the antenna voltage and detecting small changes that are caused by the load modulation of the responding transponder. This is effectively described by a change in the transimpedanz of the antenna coil.

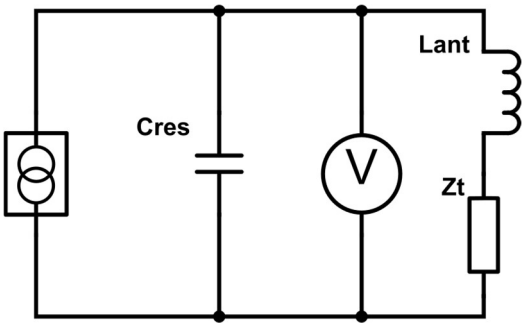

Figure 2: Simplified schematic of a RFID reader

Lant: The inductance of the reader coil.

Zt: The feedback of the transponder on the reader is described by this transimpedance.

Cres: This capacitance forms the resonant tank in the reader.

V: This voltmeter represents the measurement of the antenna voltage which always includes the transimpedance since it is a part of the reader coil.

1.4 Passive Transponder

The transponder basically consists of the antenna which is implemented with a parallel capacitance to form a parallel resonant tank like in the reader antenna. It is crucial that the resonant frequency is equal to the frequency of the carrier signal to ensure an optimal energy transfer between the antenna coils. But this circuit can be easily detuned by additional tags or metal objects present nearby. Usually the resonance frequency of the tag is trimmed to an application specific value based on the expected environment in which the tag will be used.
Furthermore, the transponder contains a chip which implements a variety of functions. The received signal is demodulated and processed by the digital logic which can

perform various procedures, like authentication protocols, Electronically Erasable Programmable Read Only Memory (EEPROM) access, data encryption and load modulation. The specifications of the chip have to be considered when designing the transponder. The resistance of the chip is a crucial factor for the quality of the resonant tank which determines the voltage on the transponder. The limiting factor for this is the supply current that is needed by the chip, which is equivalent to the chip resistance and in succession the transponder voltage. Because this voltage is a 13.56MHz AC voltage, it has to be converted to a DC supply of the chip. This means rectifying and storing the received voltage but also limiting it, because the voltage in the resonant circuit can get very high when placed close the reader antenna. To ensure the functionality of the chip the voltage is kept to a constant maximal value by an additional limiter circuit which sets the parallel resistance of the resonant circuit accordingly. Figure 3 shows the equivalent circuit model of a typical transponder.

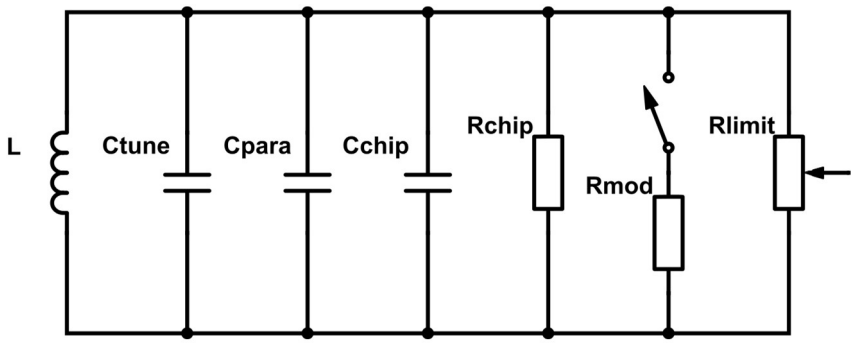

Figure 3: Simplified schematic of a passive RFID transponder.

L: The coil L represents the inductance of the transponder antenna.

Ctune: The exact value of the tuning capacitance is determined after production, so that the voltage becomes a maximum.

Cpara: The coil has a parasitic capacitance that detunes the resonant tank. This capacitance is later compensated by Ctune.

Cchip: The parasitic capacitance of the chip including pins, pads etc.

Rchip: The resistance of the chip.

Rmod: While performing load modulation a resistance smaller than the chip resistance is switched on and off.

Rlimit: This resistance represents a circuit which alters its resistance to keep the voltage below a maximal value.

1.5 Air Interface

On an abstract level the system consists of the two devices which are connected via the so-called air interface, which allows communication between the devices. As the transponder is purely passive the energy needed for operation is transmitted wirelessly from the reader through the air interface. The transfer of data is possible in both directions, whereas the communication from the reader to the transponder is called forward link and from the transponder to the reader return link. Furthermore, the transponder is also synchronised with the reader by reconstructing a clock signal from the carrier frequency.

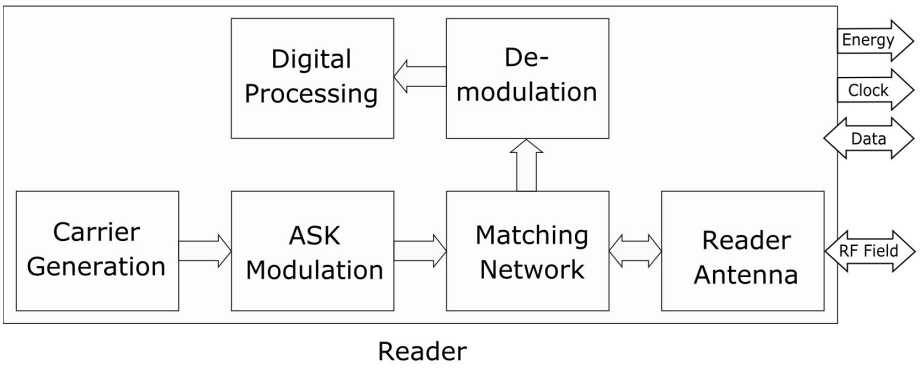

Figure 4a: Block diagram of the communication on the reader side.

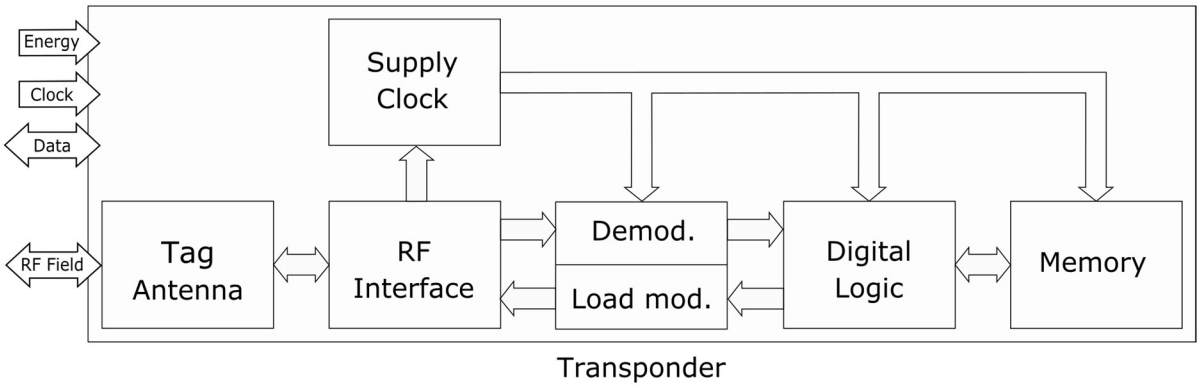

Figure 4b: Block diagram of the communication on the transponder side.

1.5.1 Energy Transfer

The reader as the active part generates the RF field or more exact a magnetic field by sourcing a current through the reader antenna. This field induces a voltage in the antenna of the transponder which is amplified by its resonant tank and then converted to a DC voltage, which is stored to power the chip in the transponder. By this, energy is transferred from the active to the passive side. Because the field intensity gets weaker over distance, the range of the system is limited, where the limiting parameters are the minimal field intensity Hmin required by the transponder and the transmitting power of the reader antenna.

1.5.2 Forward Link

In the forward link, the Carrier signal is 100% or 10% Amplitude Shift Keying (ASK) modulated. A 100% modulated signal has the advantage that it can be easier detected by the transponder, but effectively turns off the carrier field and therefore additional capacitors for energy storage are needed on the tag. With 10% modulation, the transponder can be continuously supplied during Downlink communication. Also for this reason, modified Miller coding is used to code the data on the carrier. Where a binary 1 is represented not by a level change, but by a short pulse of the signal. This reduces the time where the lower field intensity is present to a minimum. Hence most smartphones implement 100% ASK. In the transponder, the data is demodulated by the chip and the received command executed.

1.5.3 Return Link

For the return link load modulation on the transponder side is performed. Because the magnetic flux of the field flows through both antennas they act as 2 coupled inductances. Meaning that the current flowing on the transponder side influences the current in the reader antenna. By switching between different resistances on the tag the current is changed and effectively an amplitude modulation of the reader antenna voltage is achieved. This is called load modulation. In reality, the phase of the current in the transponder also has an influence, so the impact of the transponder is described as a transformed impedance on the reader side. The data is coded with Manchester

coding where a binary 1 is represented by a negative and a binary 0 by a positive edge. Because the voltage in the reader antenna is very high compared to the voltage change caused by the transponder the data is transmitted in a different frequency band called sideband. This is done by modulating the data on a subcarrier which then gets modulated on the carrier. This way it is possible to filter the signal for the subcarrier in the matching network and the Reader IC. The filtered signal can then be demodulated.

1.6 Important parameters

1.6.1 Coupling coefficient

The coupling coefficient is one key parameter for RFID and NFC systems when describing the interaction between reader and transponder as well as designing the antennas. It describes the strength of the underlying effect of inductive coupling which is used in these devices. To understand inductive coupling, it is helpful to take a look at the discrimination between near and far field of electromagnetic waves. In the near field inductive coupling is the dominant mechanism. For a 13.56MHz system the transition between near and far field happens at λ/2π ≈ 3m. Since inductive systems operate at distances at the very most of 1 or 2m far field considerations are only needed at higher frequencies for long range systems. So, the focus when observing the near field is that the magnetic field lines and therefore also the magnetic flux flow through both antenna coils. Effectively making the system a transformer with a bad efficiency, due to the magnetic flux propagating in all directions through air instead of being guided by a ferrite core. The coupling coefficient k is defined like for a normal transformer.

$$k = \frac{M}{\sqrt{L_1 * L_2}} \tag{1}$$

Since the inductances L1 and L2 are constant for an existing system, during operation k changes only with M, which is the mutual inductance of the two antenna coils.

$$M = \frac{\mu_0 * N_1 * {R_1}^2 * N_2 * {R_2}^2 * \pi}{2\sqrt{\left({R_1}^2 + x^2\right)^3}} \tag{2}$$

The mutual inductance is the relation between the current in one coil and the magnetic

flux flowing to the other coil which only depends on the geometric arrangement of the coils in a harmonic field. Where N_1 and N_2 are the number of turns on the coils and R_1 and R_2 the radii. Since in normal applications or standard tests the transponder is placed in a way that the antenna coils are aligned on one axis, the field can be considered harmonic. Meaning that the final impact on k during operation emerges from the distance x between the transponder and the reader. Therefore, the influence of the distance can be modelled by changing the k factor in simulations.

1.6.2 Hmin

In order to supply the chip on the transponder a minimal voltage is required. The minimum field strength Hmin is defined as the field strength where enough voltage can be delivered to the chip. This is before rectification and voltage control are performed, therefore the voltage in the resonating circuit is observed while the chip is in "Power on Reset" state and therefore has a maximal parallel resistance. This value can be used to compare the performance of different tags or estimate the maximal operating range x of a system.

$$x = \sqrt{\sqrt[3]{\left(\frac{I * N * R^2}{2 * H_{min}}\right)^2} - R^2} \tag{3}$$

The range hereby depends mainly on the geometry of the reader antenna with the radius R and number of turns N and the antenna current I of the reader. All influences of the tag are described by Hmin.

1.6.3 Resonance and Quality factor

When a capacitance and an inductance are connected an oscillating circuit a so called resonant circuit or resonant tank is formed. To be more precise the electromagnetic energy oscillates between the magnetic field of the inductor and the electric field of the capacitor. Like with a mechanical oscillation the circuit shows a resonance effect when excited with certain frequency called the resonance frequency f_{res} of the circuit.

$$f_{res} = \frac{1}{2\pi\sqrt{L * C}} \tag{4}$$

This is due to the impedance of the capacitor C and the inductor L, which cancels each

other out at the resonant frequency. The impedance of the circuit therefore becomes a minimum and the amplitude a maximum (for serial resonance and vice versa for parallel resonance). At this resonance frequency the amplitude of the oscillating signal becomes bigger than the amplitude of the exciting signal, where the actual value is dependent on the damping. In electrical circuits this is expressed by the quality factor Q. In each period of the oscillation energy is shifted between the imaginary parts of the components, but there is also a certain ohmic resistance where energy is lost. The ratio of oscillating energy to lost energy in each cycle is defined as the quality factor of the circuit and is calculated with the values of its components, where serial circuit quality factor Q_S and the parallel circuit quality factor Q_P are calculated differently.

$$Q_S = \frac{1}{R_S}\sqrt{\frac{L}{C}} \qquad Q_P = R_P\sqrt{\frac{C}{L}} \tag{5a) (5b}$$

The quality factor determines not only the gain of the circuit, but also the narrowing or widening of the resonance curve, which is called the bandwidth B and is defined as the frequency range between the two -3dB frequency limits f_{-3dB_1} and f_{-3dB_2} and can be calculated from the frequency of the carrier signal f_C and the quality factor Q.

$$B = f_{-3dB\_2} - f_{-3dB_1} = \frac{f_c}{Q} \tag{6}$$

This resonance curve is shown in Figure 5 for a serial resonant circuit. The different quality factors in the Figure are: Qs=50 (violet), Qs=25 (green), Qs=12.5 (blue). As described by the formula a higher Q causes the curve to become narrow and the bandwidth becomes smaller while the amplitude becomes bigger.

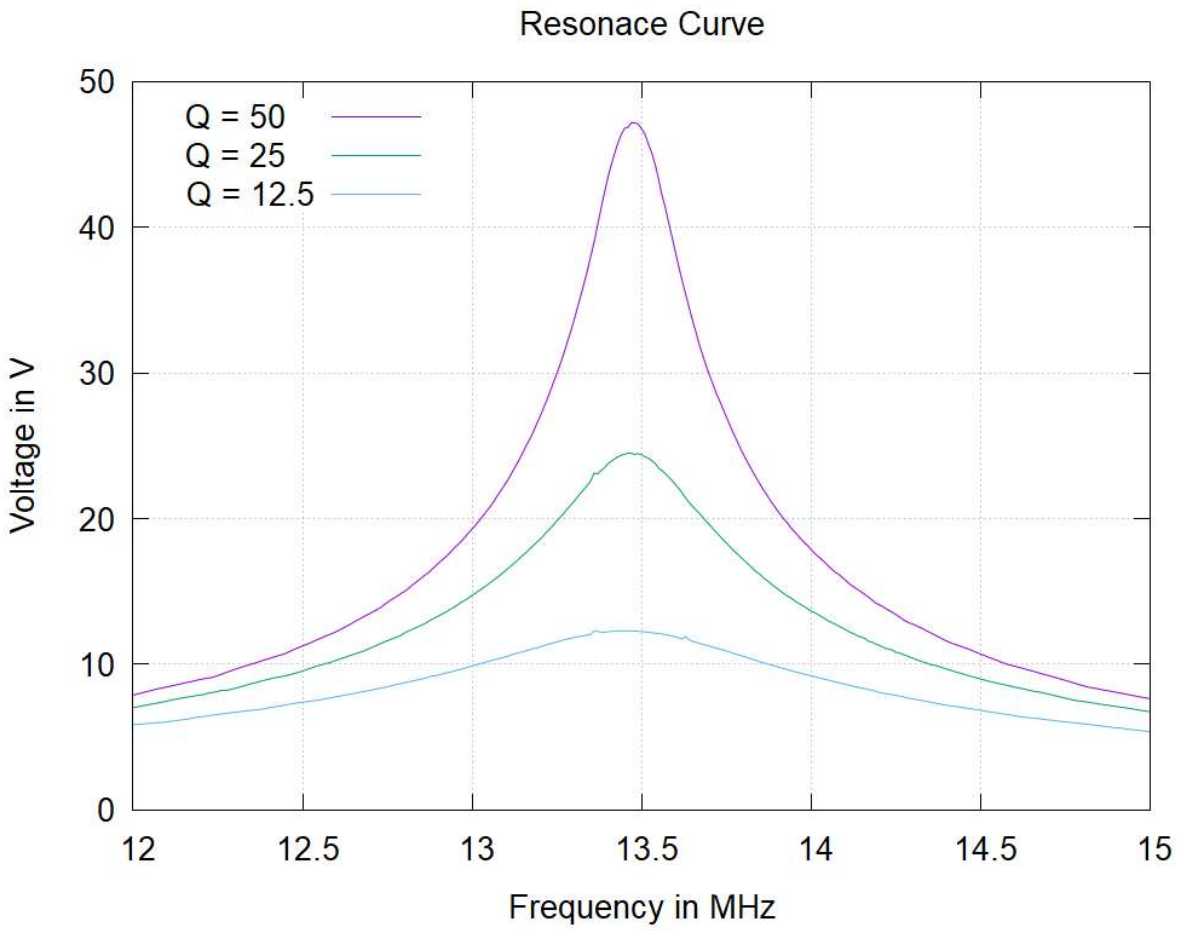

Figure 5: Example resonance curve with different quality factors.

These circuits are used for a lot of applications like bandpass filter, notch filter, etc. But in the scope of this thesis mainly for the amplification of a carrier signal with a certain frequency.

1.6.4 Operating Ranges

The energy range of a reader transponder system is the range where the transponder receives enough energy through the field to receive a command from the reader, formulate a response and transmit it by load modulation. This range is theoretically limited by Hmin. The data range is the maximum range at which the reader can recognize an answer from the transponder. At best, this distance is equal to the energy range but can be lower. It depends on the sensitivity of the reader or its ability to demodulate the received signal.

1.6.5 Transimpedanz

The transimpedanz is a fictive quantity used to model the impact of the transponder to the reader antenna. Most techniques, for example Load Modulation can be described by a change in the transimpedance. This effect originates from the mutual inductance of the coils. Therefore, the transimpedanz is zero if the coils are not coupled and increases with the coupling factor. The transimpedance is a complex term, where the imaginary part can be looked at as an additional capacitor or inductor which detunes the circuit. If the circuit is tuned properly the imaginary part of the transimpedance is zero. Otherwise it acts as a capacitor if the operating frequency is above the resonant frequency and as an inductance if the operating frequency is below the resonant frequency.

2 Background

2.1 Low Power Card Detection

Implementing NFC functions in smartphones comes with the side effect of a higher energy consumption. On one hand, a continuously switched on RF field can degrade battery duration, on the other hand for user convenience automatic communication without manual activation of services is desired. It is obvious that the solution to this is to detect if a card is present first and only switch the field on as a card is detected. To do this the feedback of the transponder on the reader side has to be measured and compared to a reference value which is measured while no transponder is present [7]. This feedback is effectively described by the transimpedanz and can be evaluated in different ways. All these methods still require a field to be emitted from the reader, but it only has to be active for a minimal time. This is similar to card polling, where a card is detected by sending a command and waiting for a response. When no response is given, the field is turned off until the next poll. Most smartphones use a combination of card polls and Low Power Card Detection (LPCD) pulses, but considering the scope of this thesis card polls are ignored as far as possible. LPCD has the advantage that the active period can be much shorter than for a full command and there is also no need to wait for a response, as seen in Figure 6. This reduces the average current and therefore the energy consumption of the system. In the scope of LPCD the transponder is usually referred to as card since the majority of currently used transponders are ID1 format cards but the method is applicable to any transponder. As of now there is no universal standard for LPCD pulses, detection principles or protocols so almost every smartphone uses different specifications. Table 1 shows a selection of current Smartphones with relevant LPCD parameter that were measured in the scope of this thesis to show the different functionalities.

	Google Pixel	LG Nexus	Samsung Galaxy S7	Sony Xperia X
Pulse Length	190 µs	328 µs	10 ms	340 µs
Pulse Strength	100%	100%	38%	100%
Pulse Interval	590 ms	210 ms	562 ms	210 ms
Poll Interval	random	3	4	4

Table 1: LPCD parameter for different smartphones.

Pulse Length: The duration in which the field is activated when trying to detect a card. This parameter is decisive for developing an improvement method as it sets the time frame in which actions must take place. To be compliant with most smartphones a pulse length of 200 µs is considered during development of the demonstrator in this thesis.

Pulse Strength: This parameter specifies the field strength during card detection relative to the field strength to normal operation. Since most smartphones use 100% field strength this is also applied for the simulations in this thesis, but it is notable that not all smartphones implement it this way.

Pulse Interval: This time describes the duration between detection pulses.

Poll Interval: This parameter describes how often the smartphone tries to poll for a card, 3 meaning that every third LPCD pulse is replaced with a card poll.

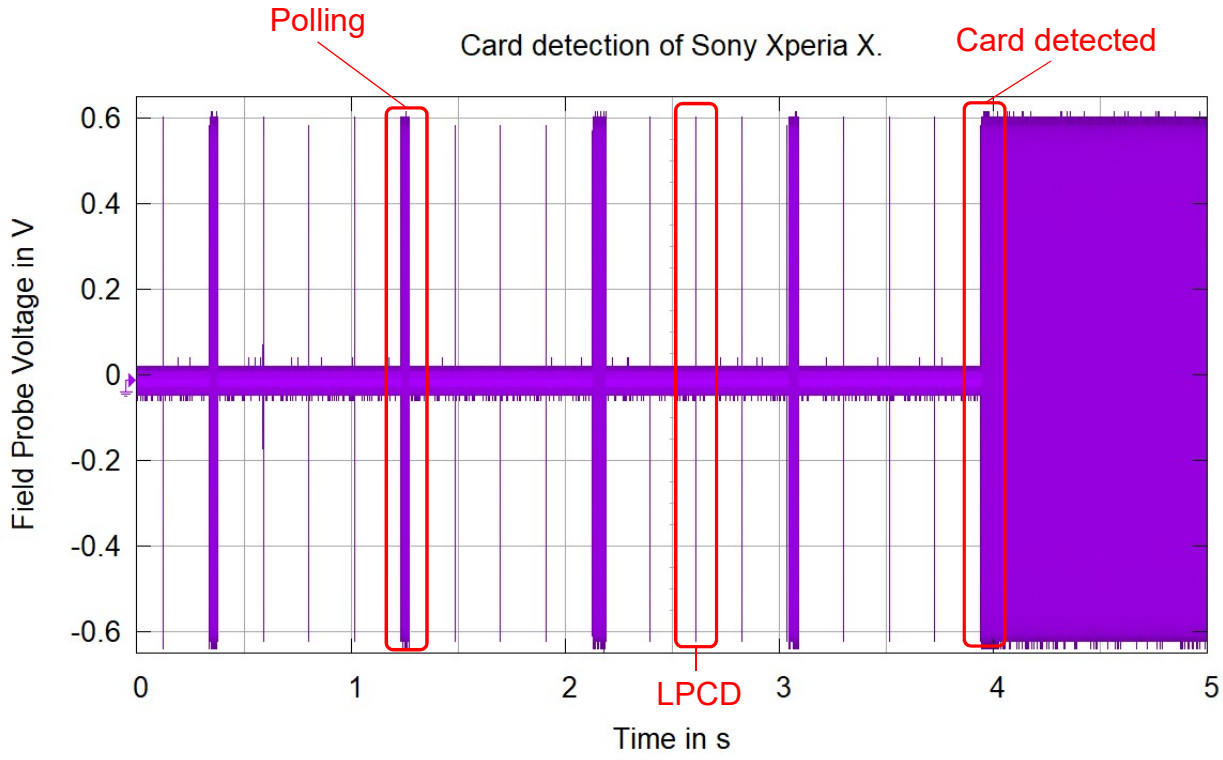

Figure 6: Oscilloscope picture of LPCD and polling pulses from the Sony Xperia X.

2.1.1 Antenna Voltage

The most common way to measure the transponder feedback is to measure the voltage of the reader coil [P1] [P2] [P4] [P8]. When a transponder or a metal object enters the near field, the resonant tank becomes slightly detuned which causes the antenna voltage to drop. This change can be measured analog by using a comparator [P1] [P2] or digital by using a A/D converter and comparing the digital code to the reference code [P8]. In a similar way it is also possible to measure the current of the driver stage supplying the reader coil [P4] [P6]. These changes can also be modelled by a change in the transimpedanz and therefore detected by observing the transimpedanz of the reader coil [P3] [P7].

2.1.2 Oscillation Behaviour

When turning off the carrier signal the antenna voltage starts to decay over time. But when a transponder with a resonant tank is present in the field it affects the resonant tank in the reader and the antenna voltage oscillates while decaying [8]. The shape of this oscillation is dependent on the coupling factor and therefore the distance to the transponder This is shown in Figure 7 for three distinct values: k=0 (top), k=0.01 (middle) and k=0.02 (bottom) where the field is turned off at t_0 It is also possible to measure the resulting decay time of the voltage to detect a transponder [9].

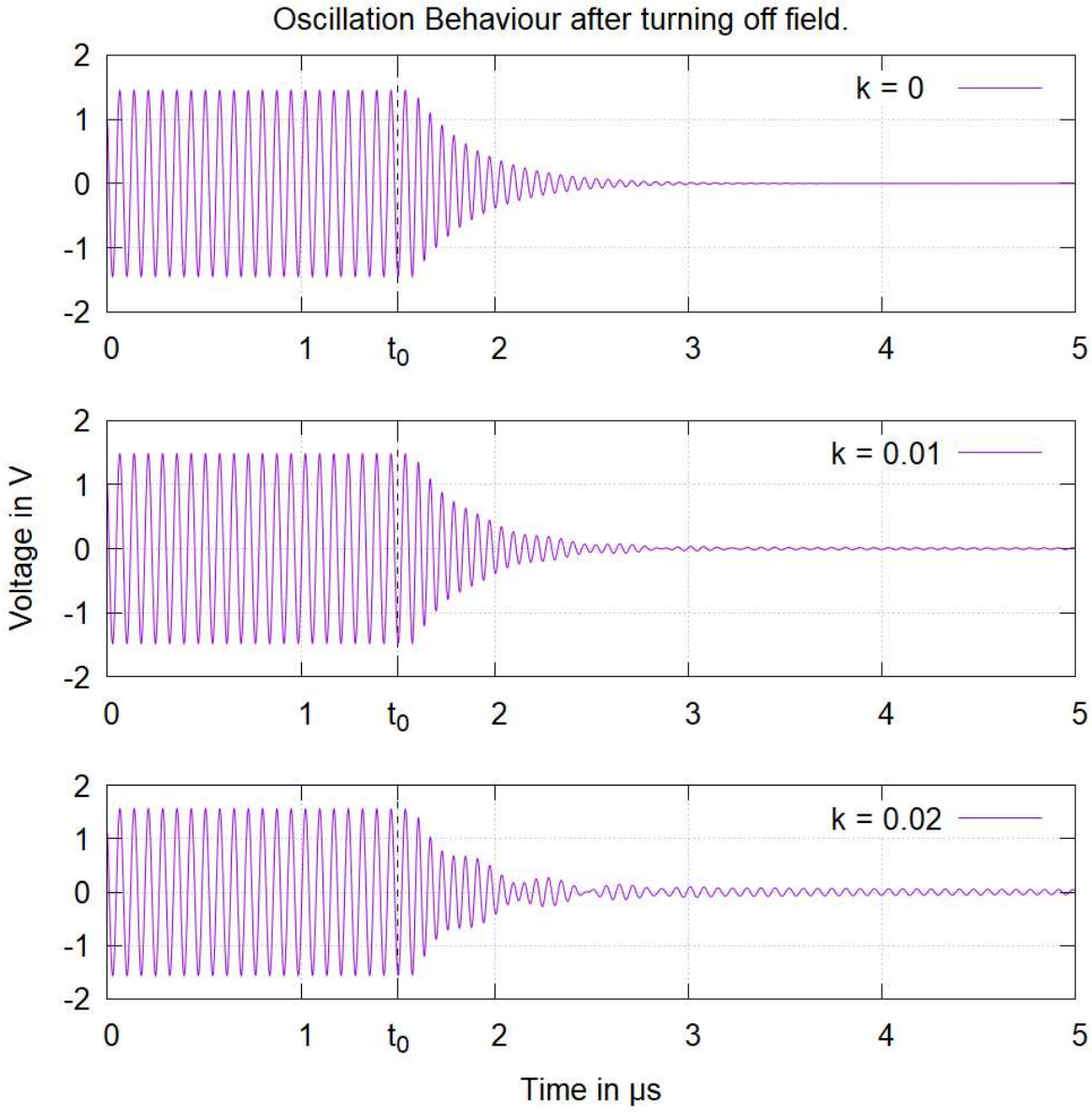

Figure 7: Behaviour of the reader antenna voltage after turning the field off.

2.1.3 PN5180 LPCD

The PN5180 is a high-performance full NFC Forum-compliant frontend IC for various contactless communication methods and protocols. It is widely used in Point of Sale terminals and smartphones. It performs the LPCD by observing the voltage on its RX pins. The RX voltage is controlled to be within a range of 1.5V to 1.65V internally by the Automatic Gain Control (AGC), to optimize the following signal processing. For this the voltage is connected to a resistive voltage divider consisting of external and internal resistors. These internal resistors are implemented as a digital variable resistor with a resolution of 10 bit and a range of 10k to 20Ohm [10]. The 10 bit digital value setting the resistance is referred to as AGC value and is always set by the internal logic in a way that the RX voltage is in the desired range. The LPCD uses this value to determine the antenna tuning. In order to detect a card a reference AGC value is measured and saved in the EEPROM and then compared with the actual value during the LPCD pulse. Usually also a certain threshold is defined in the EEPROM which specifies the needed deviation to recognize a card. The moment of the reference measurement as well as the threshold and the timings are controlled by the host, which results in different LPCD implementations in different applications.

2.2 Frequency Wobbling

Frequency wobbling is an easy method used for the detection of binary transponders [11 p.34-37]. This means that the objective is not to perform a communication with the transponder, but rather to detect if a transponder is present in the range of the reader or not, which is the same principle as LPCD, but with a higher energy consumption. This is done by varying the operating frequency over time instead of using a constant one. As a result, the voltage in the reader coil shows a characteristic dip when passing the resonant frequency of the transponder. This method is commonly used in electronic article surveillance applications. These systems usually use very cheap labels which are not tuned accurately. This is compensated by choosing the spectrum of the reader frequency accordingly while considering the production deviation. The same effect is also used in so-called “Dip-Meters” which use it to measure the resonant frequency of antennas. Figure 8 shows a simulation of the reader voltage while performing frequency wobbling with a transponder present.

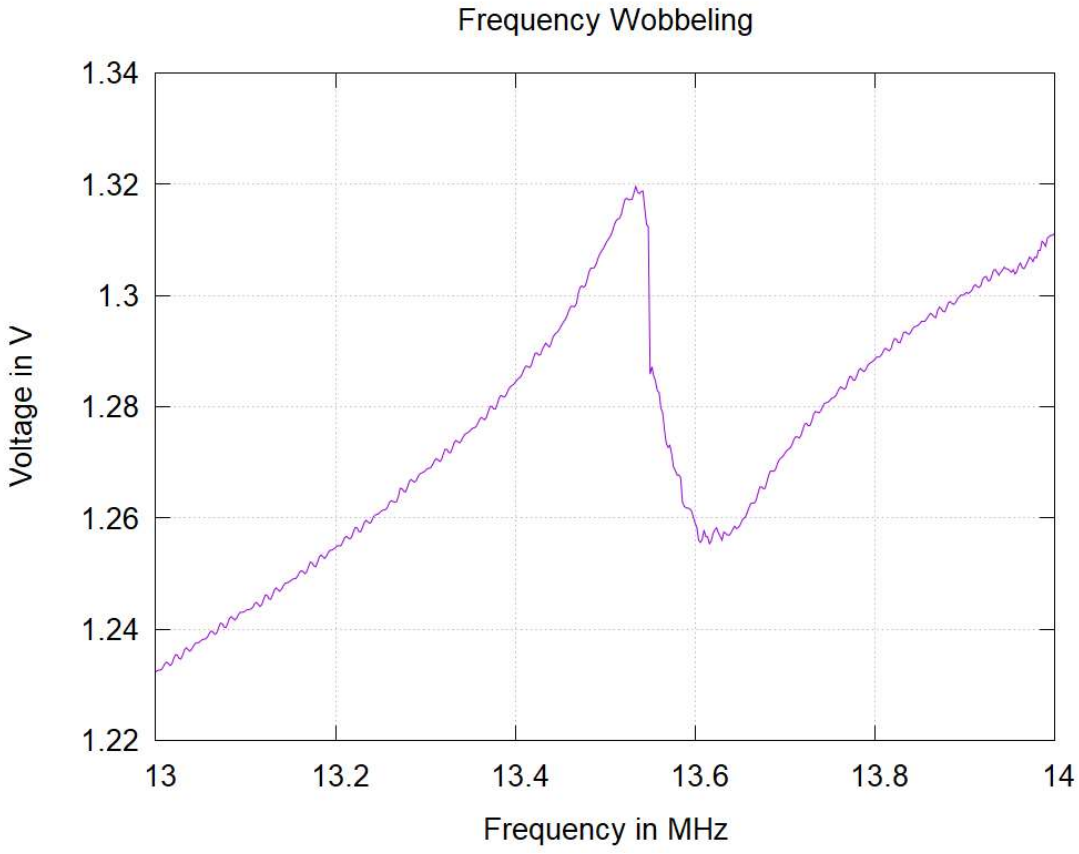

Figure 8: Behaviour of the reader antenna voltage while performing frequency wobbling.

3 Improvement Method

3.1 Motivation

The performance of NFC in smartphones can be evaluated by the operating range of the system for example. Typically, the limiting range is the data range but in most NFC applications the phone enters a detection mode with reduced energy consumption after a given time. In this mode, no communication is made and in order to do so, a transponder must be detected first. This effectively makes the detection range the limiting range which is often smaller than the data range. Until now LPCD has mostly been focusing on the measurement of quantities on the reader side while the transponder operates in a normal state. But if the transponder takes actions by reconfiguring himself, the feedback in the reader could be increased and therefore also the detection range.

3.2 Concept

To change the feedback of the transponder the topology of the resonant circuit is changed. In practice, this is implemented by switching between different capacitors and consequently changing the tuning of the resonant circuit and in succession the antenna voltage in the reader. Eventually the necessary threshold will be exceeded and the LPCD of smartphones, that monitor the antenna voltage or transimpedanz as part of the card detection, triggered.

3.2.1 Simulation of Detuning

As a first demonstration a simple transient simulation of a reader transponder system is performed. The exact circuit used is shown in Figure 9. To model the reader the matching network of the PN5180 evaluation board [12] is used and supplied with a 13.56MHz sinusoidal current source at the TX ports. Also, the so-called EMC filter of the source is considered, which has the function to shape the rectangular output signal of the chip into a sinusoidal signal. The ANT1 and ANT2 ports are used for active load modulation and therefore not needed in this thesis, so they are connected with a 10Ω

resistance to represent the connection inside the reader chip. The voltage on the RX ports is the voltage the reader IC is receiving and is therefore the focus of observation. The transponder IC is modelled very simply with only a resistance Rchip and a capacitance Cchip representing its equivalent circuit values. Therefore, no voltage regulation or load modulation is implemented in the simulation. The coils of the reader L1 and the transponder L2 are coupled with a spice model. By varying the coupling factor different distances between the coils can be modelled (assuming the coils are on top of each other). While the tuning of the reader circuit is fixed by the matching network the tuning of the transponder can be varied with the capacitance Ctune and by doing so the effects of a detuned transponder on the reader can be observed.

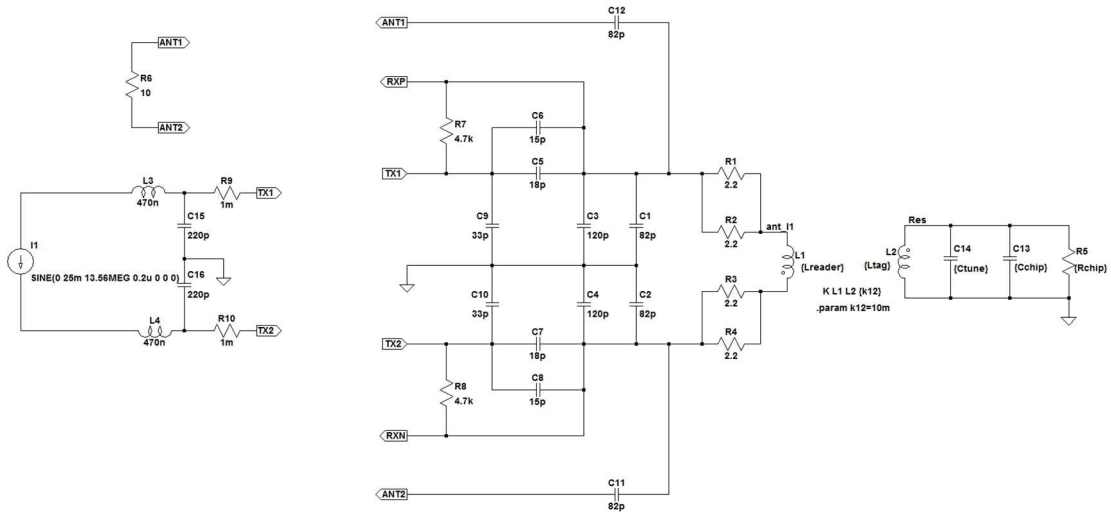

Figure 9: Circuit used for the simulation of detuning.

The tuning capacitance is swept uniformly around the resonance capacitance and the results are shown in Figure 10. The different curves are simulated with different resistances of the transponder and therefore different quality factors being 500 150 80 and 0. For higher quality factors the voltage drop in the reader coil increases. It can also be seen that the maximum feedback occurs when to resonant frequency of the transponder is exactly tuned to the frequency of the carrier signal.

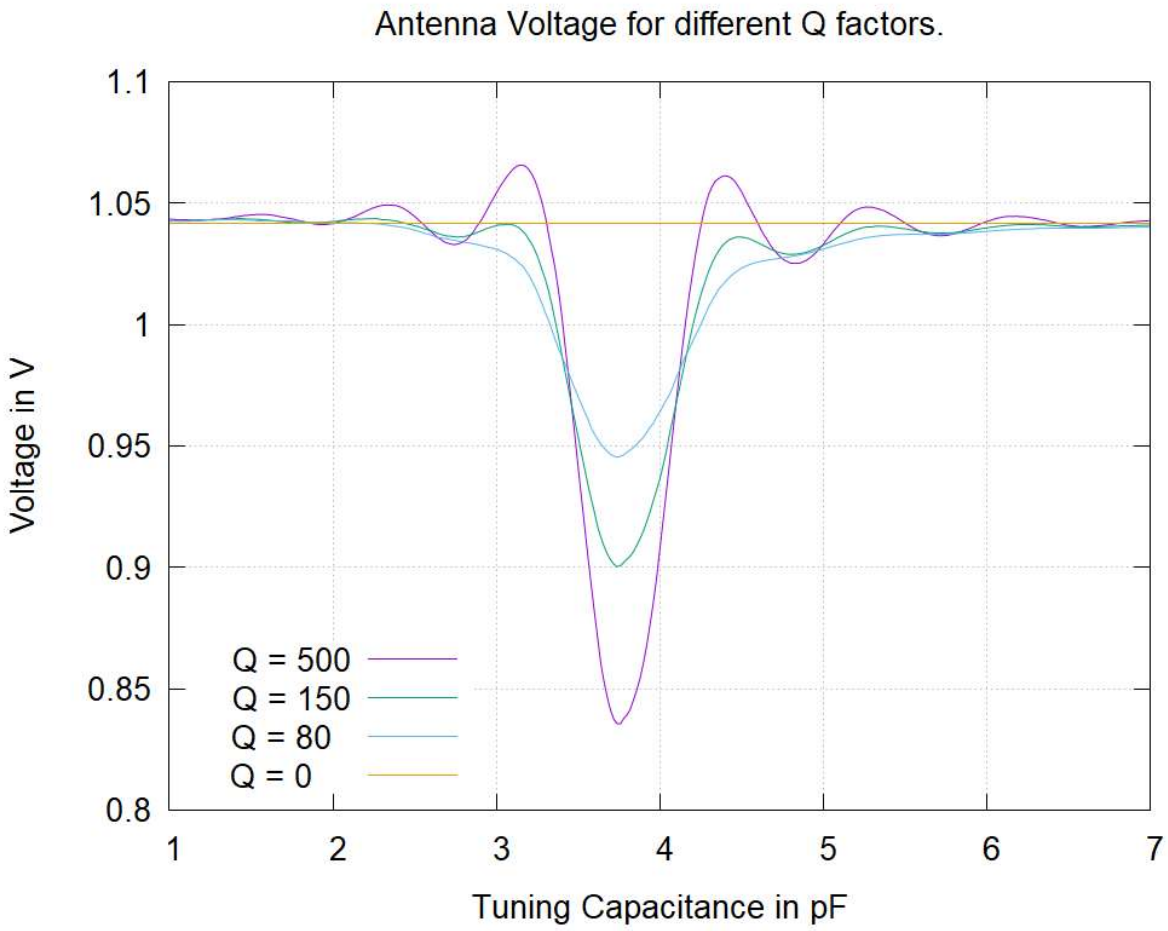

Figure 10: Effect of tuning on the reader antenna voltage.

3.2.2 Simulation of Capacitor Switching

Another simulation is conducted in which capacitances are switched on and off during runtime to observe the transient behaviour. This is done by setting the tuning capacitance to a fixed value and adding a binary weighted sequence of 5 capacitors ranging from 0.1pF to 1.6pF in parallel as seen in Figure 11. The capacitors are switched with an ideally modelled switch. On the reader side the same matching network as before is used.

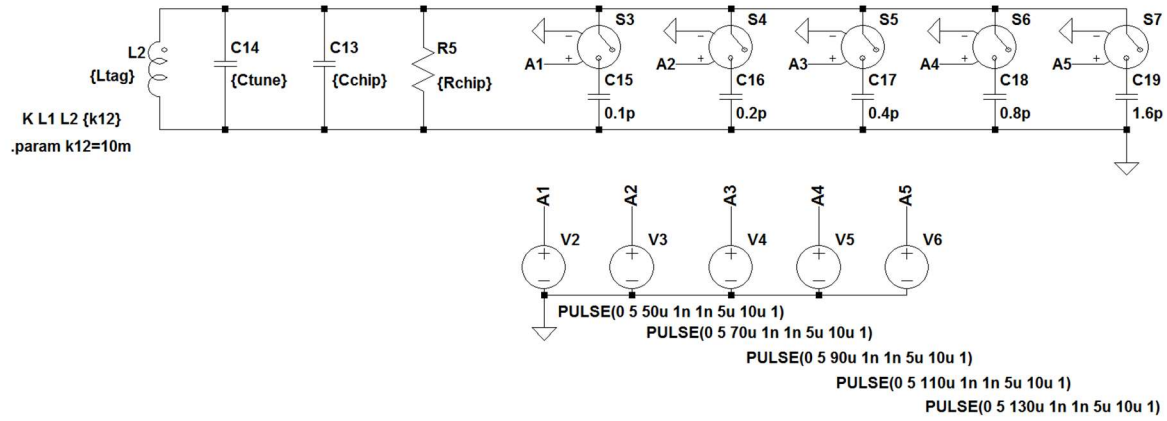

Figure 11: Circuit used for the simulation of switching capacitors.

Figure 12 shows the reader antenna voltage at the top, the transponder voltage in the middle and the signals activating the switches at the bottom. It can be seen from the result that adding a capacitor causes the antenna voltage to change to a new level and it returns to the previous when the capacitor is switched off again. It can also be seen that adding the capacitance, the voltage in the transponder decreases because of the detuning of the resonant circuit.

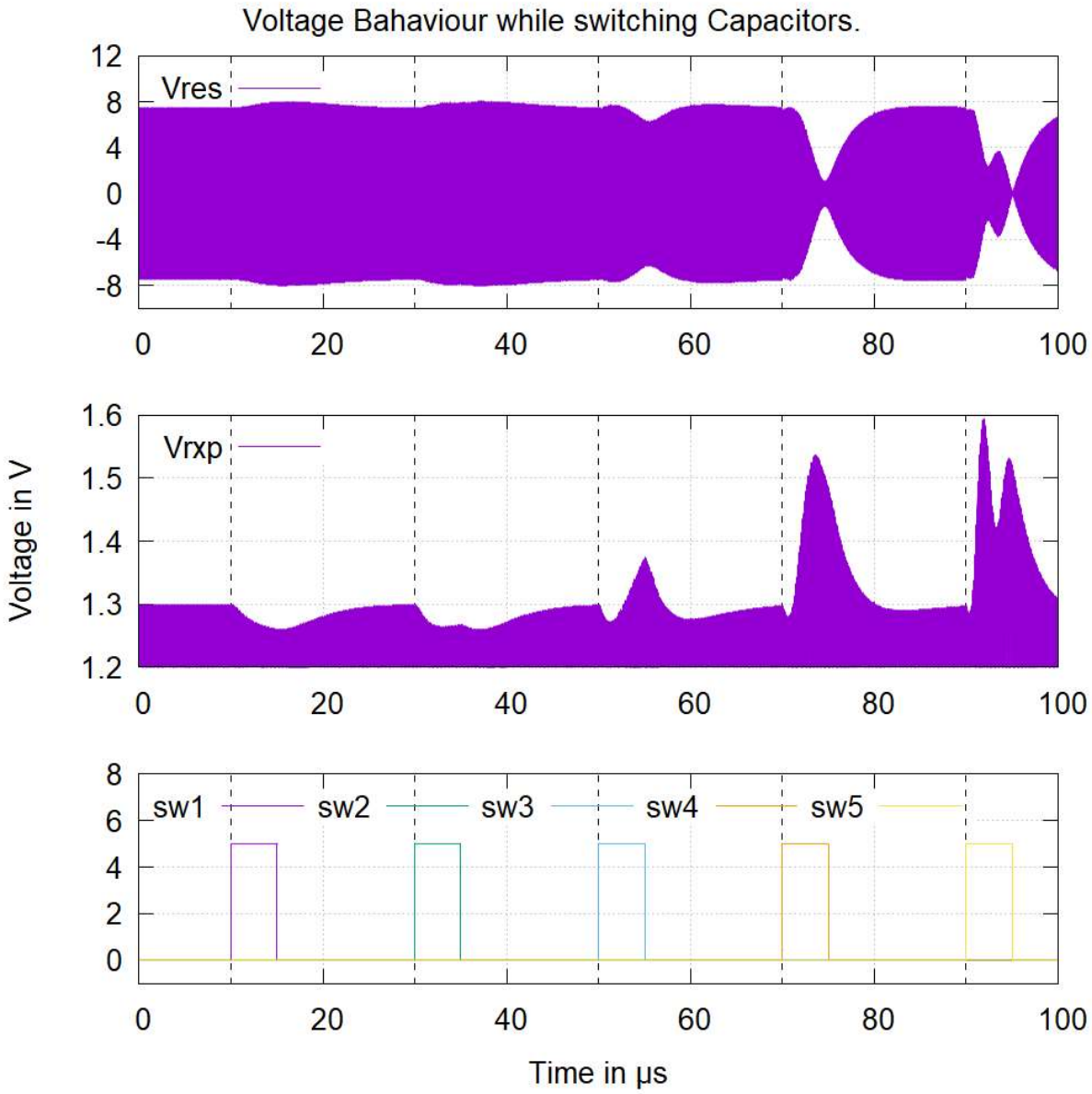

Figure 12: Effect of switching capacitors on the transponder.

3.3 Design

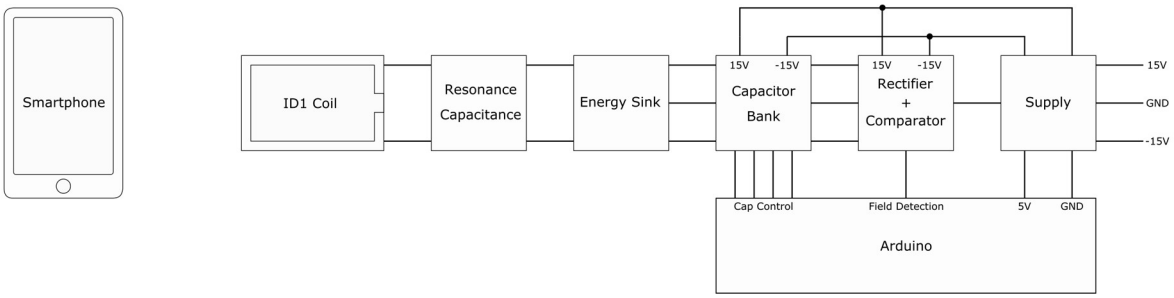

Figure 13: Block diagram of the designed transponder substitute.

Up to this point all observations have been theoretical, based on simulation results using ideal elements not including parasitics. To test this concept practically a demonstrator is designed on a Printed Circuit Board (PCB) to resemble a transponder in terms of electric properties, but without implementing a chip. Instead it utilizes a capacitor bank that is controlled by an external Arduino microcontroller board, which allows for testing a variety of different switching behaviours. To signal the Arduino when to start the procedure the antenna voltage is rectified and if a certain threshold is exceeded a Field Detection Signal is generated. In order to supply all these additional blocks, the tag is externally supplied with symmetrical 15V and internally it generates 5V for the digital parts This external supply does not influence the antenna signal so the tag still behaves like a passive transponder. The design is set up differentially so that the impact on the antenna voltage from the capacitor bank and the parasitic capacitances is symmetrical. Also, it allows to refer the rectified DC voltage to a ground signal that can also be used for the external components. In general, the components used were chosen with a focus on low parasitic capacitances and a frequency behaviour suited for 13.56MHz.

3.3.1 Antenna

The antenna size meets the requirements of the in ISO/IEC14443 specified standard ID1 size and has a resonance capacitance connected in parallel consisting of up to 2 SMD capacitors (Surface Mounted Device) and 2 in series connected trim capacitors for fine-tuning. In order to adjust the capacitance easier the parallel capacitors are not implemented differentially. Two BNC connectors are placed on the antenna signals so that the antenna voltage can be viewed with an oscilloscope. The capacitance of the probes contributes to the total parasitic capacitance of the circuit and has to be accounted for when choosing the SMD capacitors.

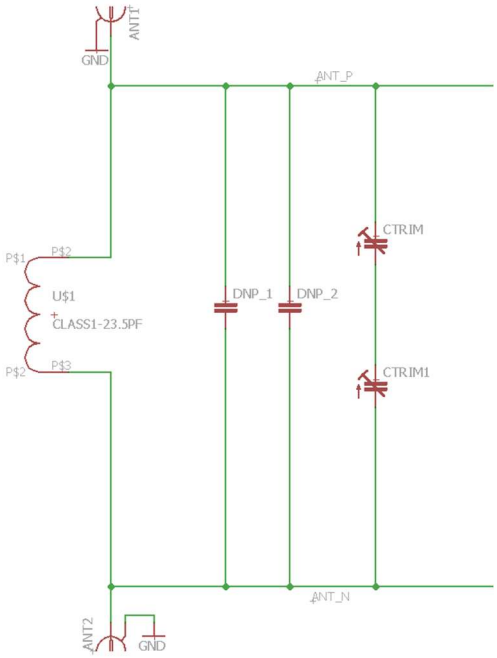

Figure 14: Schematic of the antenna block.

3.3.2 Energy Sink

The chip is modelled same as in the simulation, basically consisting only of 2 differentially implemented resistors that model the energy consumption of the transponder. They are also used to define the ground between the two antenna sides. The chip capacitance is not implemented. The additional elements in the circuit like the switches or the connectors for the oscilloscope bring a certain amount of parasitic capacitance to the board. In the end the total capacitance of the tag should be fine-tuned manually.

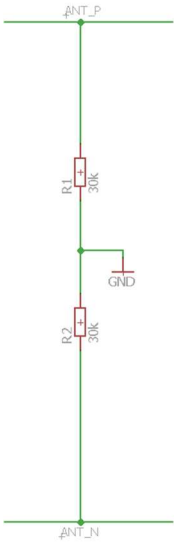

Figure 15: Schematic of the energy sink.

3.3.3 Capacitor Bank

The switches used on the PCB have special requirements and are the most critical elements in the design. They have to connect the analog antenna signals to the capacitors. Since the signal is an AC voltage with no DC offset, the use of conventional transistor ICs (non-monolithic) as switches is not possible, because of the parasitic drain-source diode. Therefore, an analog switch is used, which is configured as a low side switch. Each switch is used with two in series connected capacitors, so that the total capacitance can be set more exactly. Another important requirement is a low parasitic capacitance of the switch. Standard analog switches can have relative high capacitances of a few hundred picofarad, this would defy the function of the board because the capacitances, that are switched, are designed to be in the order of picofarad. Therefore, the ADG1212 is chosen, which is a special low capacitance analog switch [13] [14].

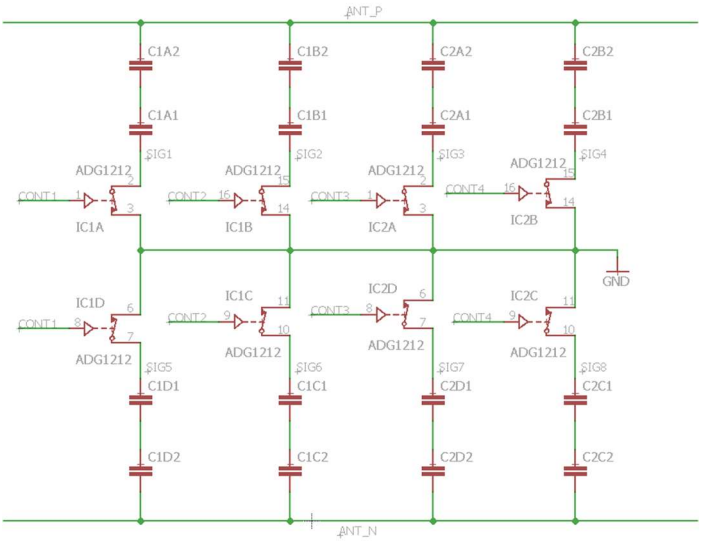

Figure 16: Schematic of the capacitor bank.

3.3.4 Rectifier

The rectifier block is used to generate a DC signal out of the antenna voltage, so that the microcontroller can detect the status of the field. This block is based on the reference Vicinity Integrated Circuit Card (VICC) for Vicinity Coupling Device (VCD) power test specified in ISO/IEC10373-7 [15]. For lower parasitic capacitances the diodes MMBD301LT1G are chosen. Two Zener Diodes are added to limit the antenna voltage to around 12V in order to protect the analog switches form voltages greater than the supply voltages. The smoothing capacitor is chosen to have a much smaller value, because a fast field detection is needed and there is no considerable load on the capacitor voltage. The resistor parallel to the capacitor is to set the time it takes to discharge, so that the voltage is fully depleted at the next LPCD pulse. The capacitor voltage is also routed to a pin on the board and allows for measuring the effective antenna voltage without connecting an oscilloscope.

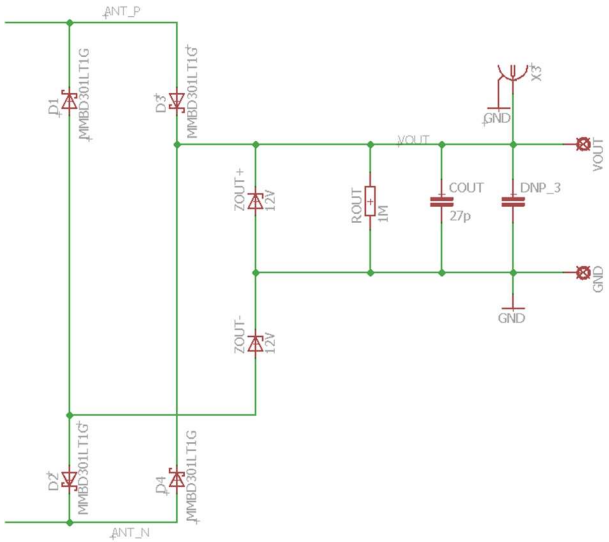

Figure 17: Schematic of the rectifier block.

3.3.5 Comparator

Because the antenna voltage and therefore also the capacitor voltage can be too high for the microcontroller a comparator block is added. This block compares the capacitor voltage with a tuneable reference voltage and generates a digital signal. A LM311 is used with an open drain configuration. This allows to use the Arduino's on board pull up resistors. Additionally, also a pull up resistor to the boards internal 5V is implemented. Furthermore, the design allows an offset compensation of the Operational Amplifier (OPA) by adjusting a potentiometer.

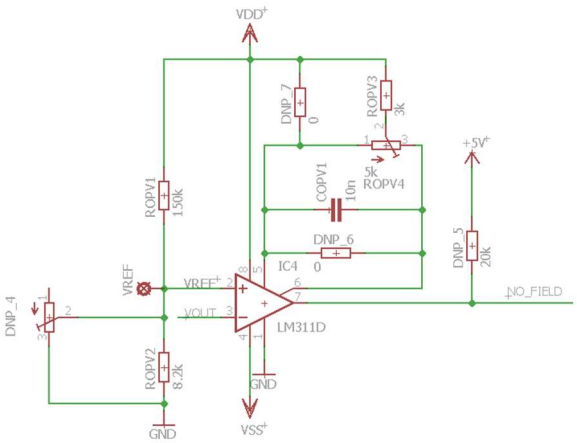

Figure 18: Schematic of the comparator block.

3.3.6 Supply

The board has to be supplied externally with symmetrical +/- 15V and generates internal 5V with a LM7805 voltage regulator to supply the Arduino. Because the reduction from 15V to 5V can cause a lot of waste heat the voltage regulator is chosen as a wired component to allow a better heat transfer from the package as well as the possibility to add an additional heat sink. Each voltage level is buffered by two capacitors, one bipolar Tantalum capacitor with a higher capacitance to compensate for current load changes and a smaller SMD capacitor to filter high frequency disturbances. Because during programming the Arduino is supplied by the computer via USB port a jumper is implemented to disconnect the internal supply on the board to avoid compensation currents between multiple sources.

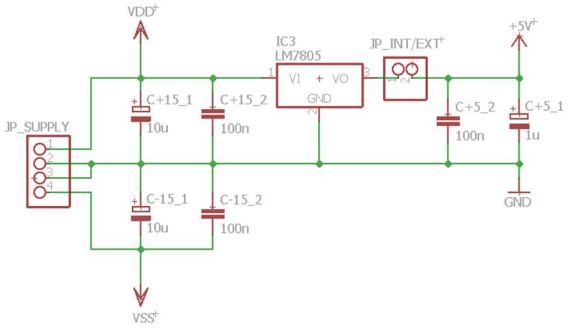

Figure 19: Schematic of the supply block.

3.3.7 Circuit Protection

To protect the switching ICs, on both their supplies capacitors are placed that filter high frequencies and transient voltage spikes. This is implemented with two capacitors per supply pin to realize a symmetric layout. In addition to that the digital input signals of the switches are connected to a transient-voltage-suppression diode array IC, that filters transient voltages above the defined HIGH level of 5V.

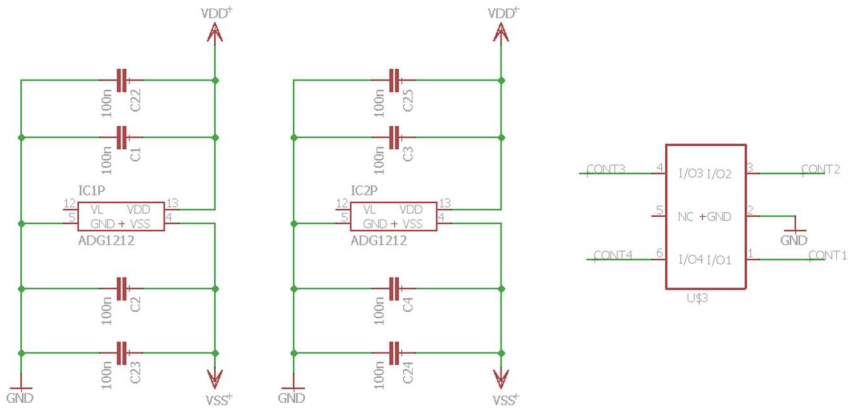

Figure 20: Schematic of the circuit protection block.

3.3.8 Arduino

The purpose of the Arduino microcontroller board is to manage the exact timing of the switches while allowing for a maximal flexibility of switching patterns. The Arduino receives a signal form the PCB when a certain threshold in the antenna voltage is exceeded, which triggers an interrupt and starts the switching routine. While doing so a pulse is send to an output pin, which serves as a trigger signal for the oscilloscope. The Arduino is supplied via the Vin Pin with 5V from the PCB, which allows to operate the whole setup with a single supply. Alternatively, the Arduino can be connected to the USB port of a computer, which allows for fast debugging and additional data to be sent from the Arduino to the computer via serial communication over the USB port. In this case the 5V supply from the PCB should be disabled by opening a jumper on the PCB. The use of the Arduino adds some additional timing constraints. Since the field detection is activated by an interrupt the interrupt response time, which is measured to be between 13µs and 20µs, adds to the total delay of the field detection. Because the whole design is made for a specified LPCD pulse duration of about 200µs, this delay is acceptable.

```
const byte interrupt_pin = 2;
const byte trigger_pin = 11;
volatile byte field_detected = LOW;

void setup(){
  attachInterrupt(digitalPinToInterrupt(interrupt_pin), fieldDetectionISR, FALLING);
  pinMode(interrupt_pin, INPUT_PULLUP);
  pinMode(trigger_pin, OUTPUT);
}
void loop(){
  if(field_detected){
    digitalWrite(trigger_pin, HIGH);
    digitalWrite(trigger_pin, LOW);
    field_detected = LOW;
  }
}
void fieldDetectionISR(){
  if(digitalRead(interrupt_pin)==LOW)
    field_detected = HIGH;
}
```

Figure 21: Example Arduino code for interrupt and trigger test.

Also, the switching time of the Arduino outputs limits the switching speed. By using direct port manipulation of the microcontroller instead of the provided digital functions in the code this time is reduced form 4µs to 1.2µs and also allows to switch multiple output signals at the same time.

```
void setup(){
  byte code = 4;  //code from 0 to 15
  byte port = 0;
  DDRD &= B00001111;  //set Pin 7-4 as Outputs

  //write code on Pin 7-4 in binary
  port = PORTD;
  port &= B00001111;
  port |= code << 4;
  PORTD = port;
}
```

Figure 22: Example Arduino code for port manipulation

3.4 Simulation of the Demonstrator

The design was tested by simulation of the circuit shown in Figure 23, which implements the described design. In this simulation real component models provided by the manufacturers were used for the following components: Analog switches ADG1212, Schottky diodes MMBD301LT1G, Zener diodes BZX84C12L, OPA LM311 and voltage regulator LM7805. Due to the differential design always two capacitors, which are connected in series, are switched at the same time. Meaning that the effectively switched capacitance is half the capacitance of the capacitors. Also, the parasitic capacitance of the switches has an influence on this value.

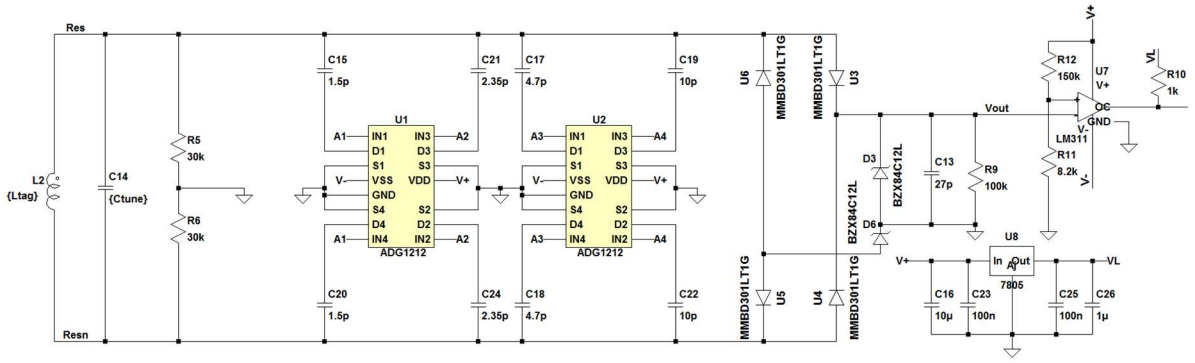

Figure 23: Circuit used for the Demonstrator simulation.

The simulation result in Figure 24 can now be compared with the result of the ideal simulation from Figure 12. Due to the dual implementation and the introduced parasitic capacitances the capacitance values to be switched are changed, however the impact on the reader and transponder voltages is the same.

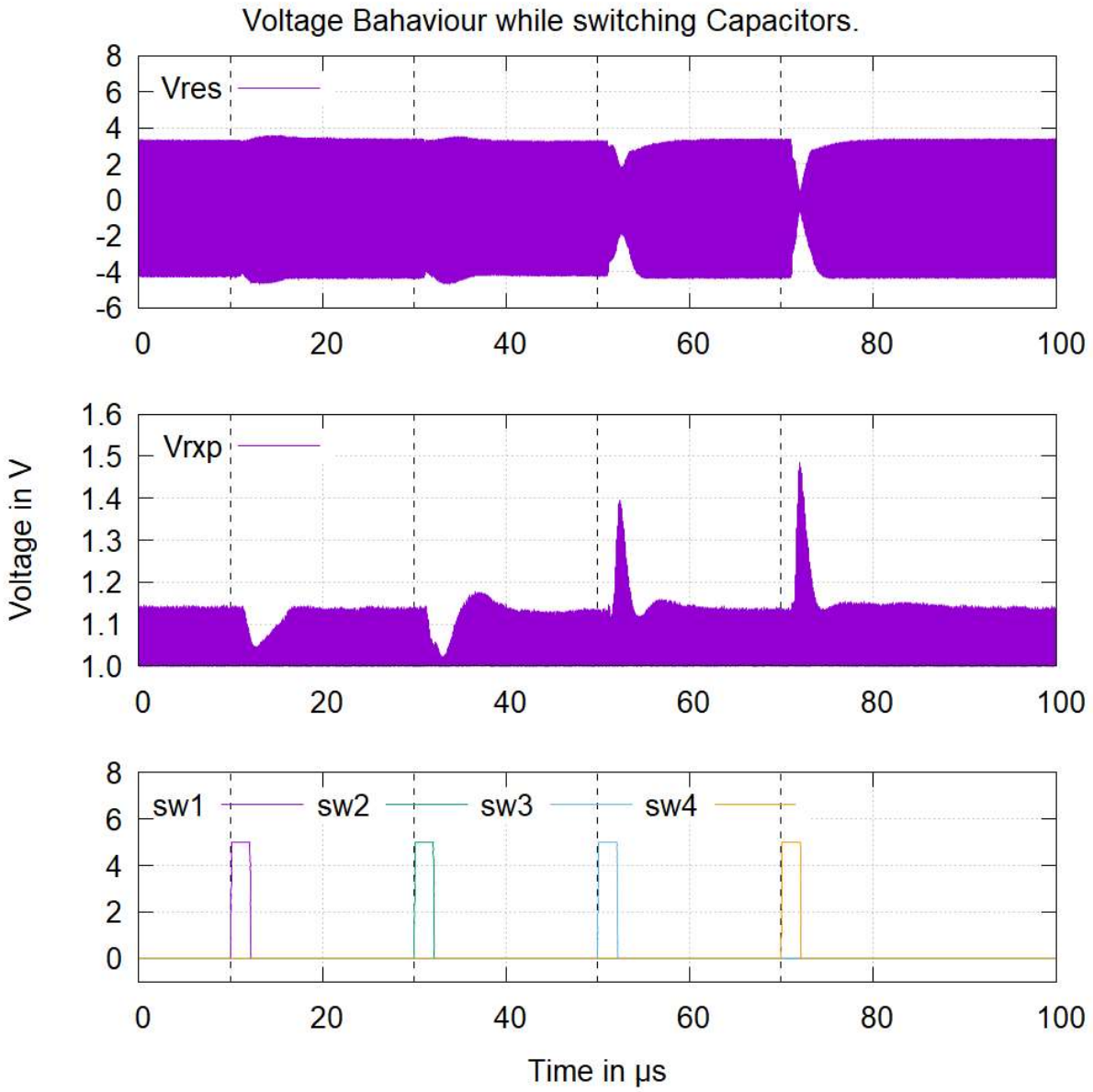

Figure 24: Effect of switching capacitors on the transponder simulated with real models.

3.5 PCB Layout

3.5.1 Electromagnetic Compatibility Aspects

Because the board is supposed to operate in a laboratory environment with a lot of possible noise sources, one being the reader itself, the layout is done with focus on the electromagnetic robustness. This is implemented by the following measures.

Ground Plane:

To shield the circuit from the RF-field generated by the reader the backside of the board is almost completely filled with a copper layer, which is connected to the ground

signal of the circuit. The backside is also used to route signals, but the length of those traces was kept to a minimum, only used to cross traces on the topside in order not to split up the ground plane. In the antenna area no ground plane was implemented so that the field in the antenna stays uninterrupted.

Minimal Loop Area:

It is a known effect, that loops on a PCB can act as antennas for electromagnetic fields and cause disturbances in the circuit. Also, they cause parasitic inductances which are hard to calculate and can cause problems when connected to ICs since these external parasites are usually not considered during circuit design. To reduce the impact of these effects an effort is made to identify crucial loops in the design and minimize their area.

Symmetric Placement:

Instead of having one single loop in the circuit, a differential design can be implemented with two symmetric loops with opposite winding directions. By doing so the distortions in the two loops have opposite signs and can cancel each other out. Also, in terms of parasitic capacitances, resistances and propagation delay a symmetric placement is favourable.

3.5.2 Design Flow

Floorplan:

At first the width of the PCB is set to 54mm which is the width of a standard ID1 card specified in ISO/IEC14443-1 [5]. In this area the most important parts are placed first. The connectors are placed at the border of the board so that they can be easily connected to the external elements. The analogue switches are placed in the center and the tuning capacitors next to the antenna.

Suppressor capacitors:

Next the suppressor capacitors for the analogue switches were placed on the backside of the board in order to place them as close as possible to the ICs. Since the pins next to the supply signals Vcc and Vdd are connected to ground, two capacitors are placed in a symmetric way for each supply pin. This way the loops are opposed and have a minimal area.

AC Signals:

The next loop that is considered is the antenna signal. Because the suppressor capacitors are placed on the backside the capacitors that will be switched can be placed directly next to the pins of the analogue switches and the antenna signals routed around very close to the package of the IC to minimize the loop area. In order to avoid mismatch between the signal paths the layout is done symmetrically.

Block assembly, Signal routing:

After all these important components are taken care of, the remaining parts are sorted in their corresponding blocks, arranged to minimize the used board area and routed. Then, the so designed blocks are placed on the board so that the signals connecting the different blocks can be easily routed.

Afterwards the remaining signals are routed, so that the important signals are not interrupted by vias.

Supply lines:

In the end the supplies are routed using a star supply system, where every block gets their own trace to the supply pin on the board.

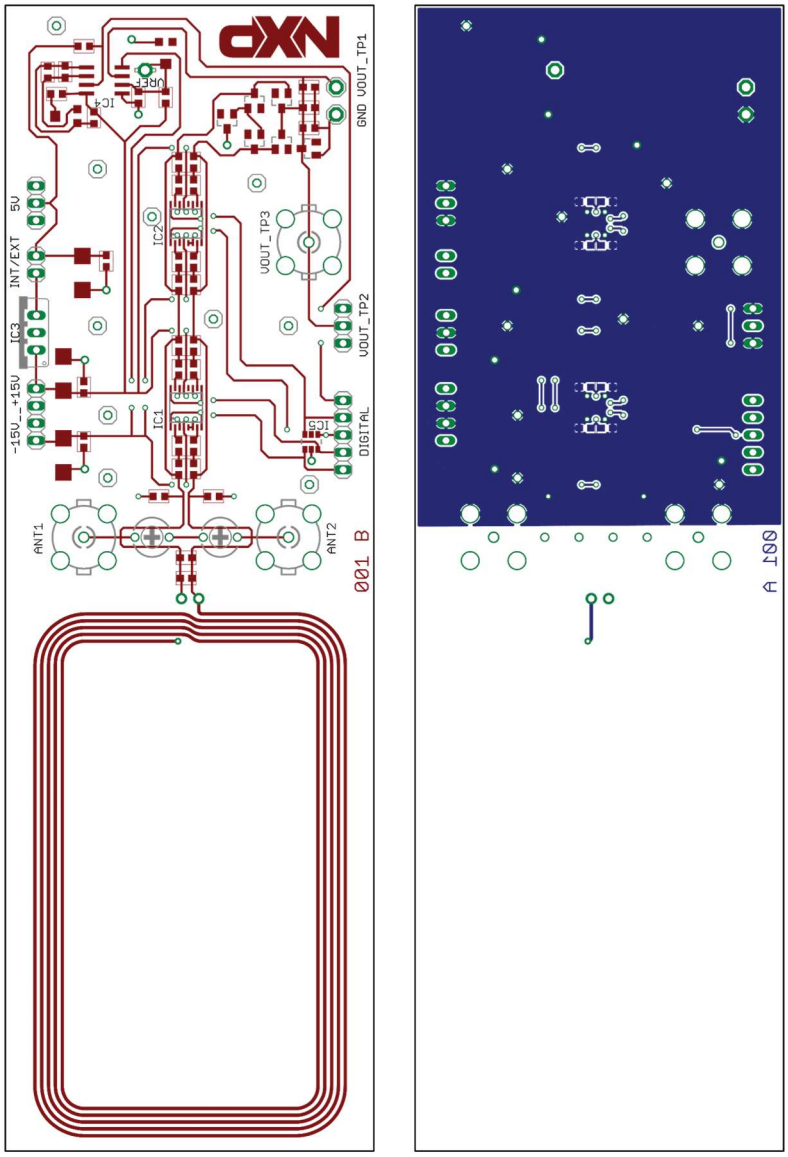

Figure 25: PCB Layout.

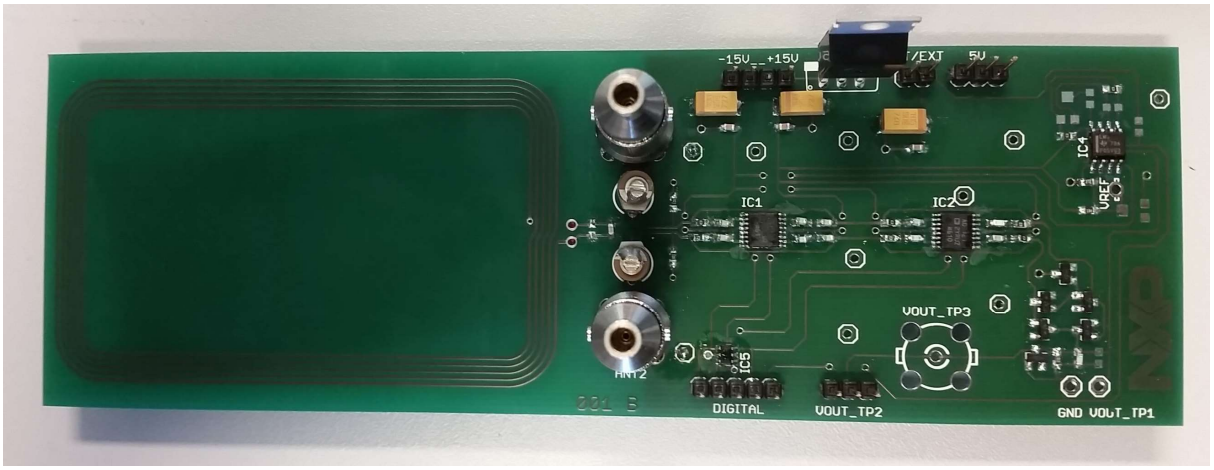

Figure 26: Assembled Demonstrator Board.

4 Evaluation

4.1 Test Setup

To evaluate the PCB a test setup is installed where the PCB was placed in a ID1 card holder. A smartphone is placed under the holder and the distance between smartphone and card can be adjusted by turning a knob on the side. For the external ±15V supply a common laboratory Power Supply Unit (PSU) is used while the Arduino is supplied by a laptop so that debugging of the code is possible. The supply jumper is removed for this setup. The measurement of the antenna voltage is done by connecting an oscilloscope to the two connectors as well as a pin on the Arduino which provides a trigger signal. By doing so a detailed view of the effects of the switching process is possible. The remaining channel of the oscilloscope can be used for measuring different signals on the PCB or the Arduino.

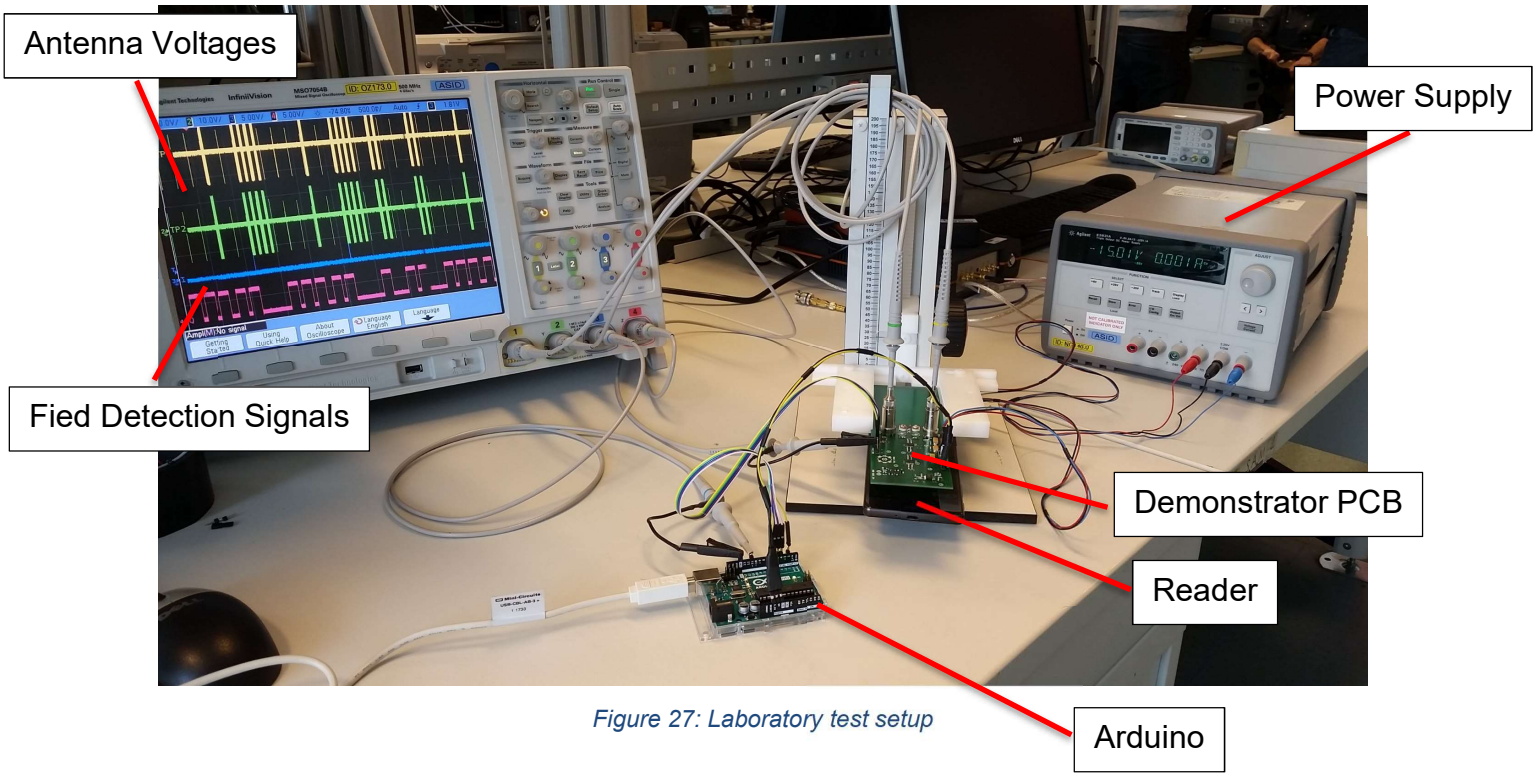

Figure 27: Laboratory test setup

4.2 Field Detection

The timing of the field Detection can be seen in Figure 28. The top signal is the field detection signal. This is the output of the comparator and switches and changes to LOW after the threshold of 0.78V on the rectifier is exceeded. The middle signal shows the trigger signal generated after the Arduino interrupt, which can be seen to occur 19.65µs after the field is turned on. The bottom signal shows the voltage on the capacitor of the rectifier. The major contribution to the response time delay is coming from the interrupt of the Arduino as expected.

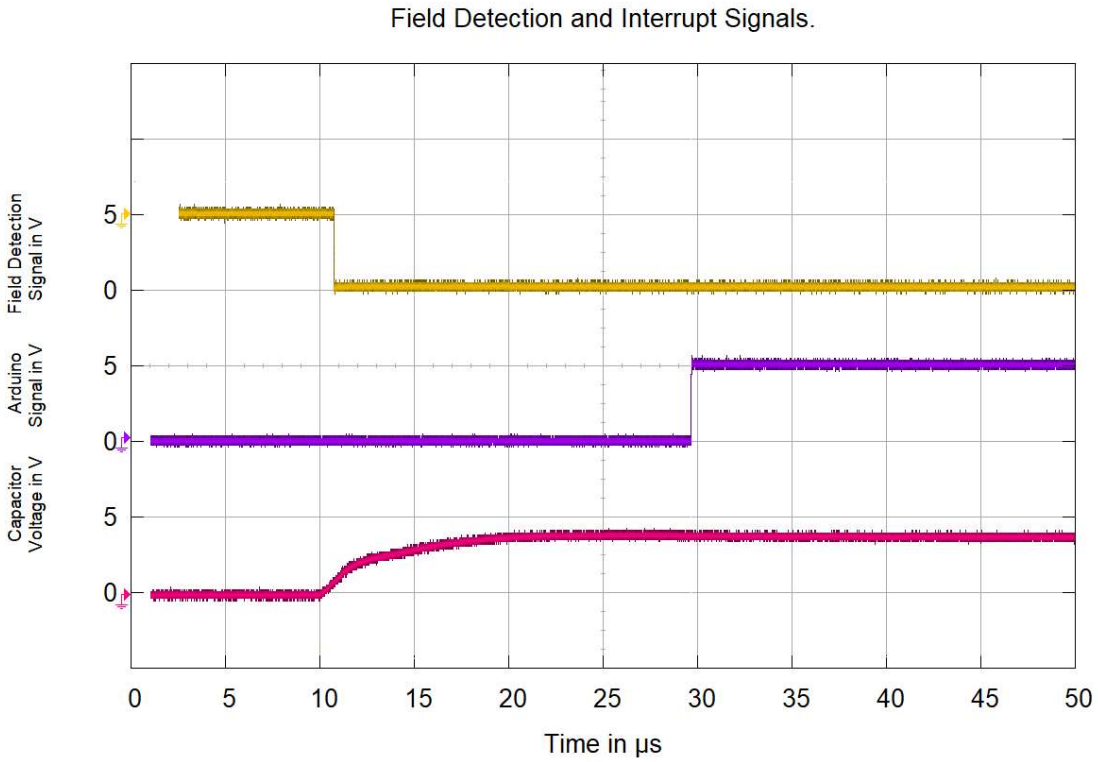

Figure 28: Field detection signals oscilloscope screenshot.

4.3 LPCD

In comparison Figure 29 shows the LPCD in a normal state without switching on the board. In this case a card is detected once, which can be seen by the additional polling pulse performed by the reader when the transponder is detected.

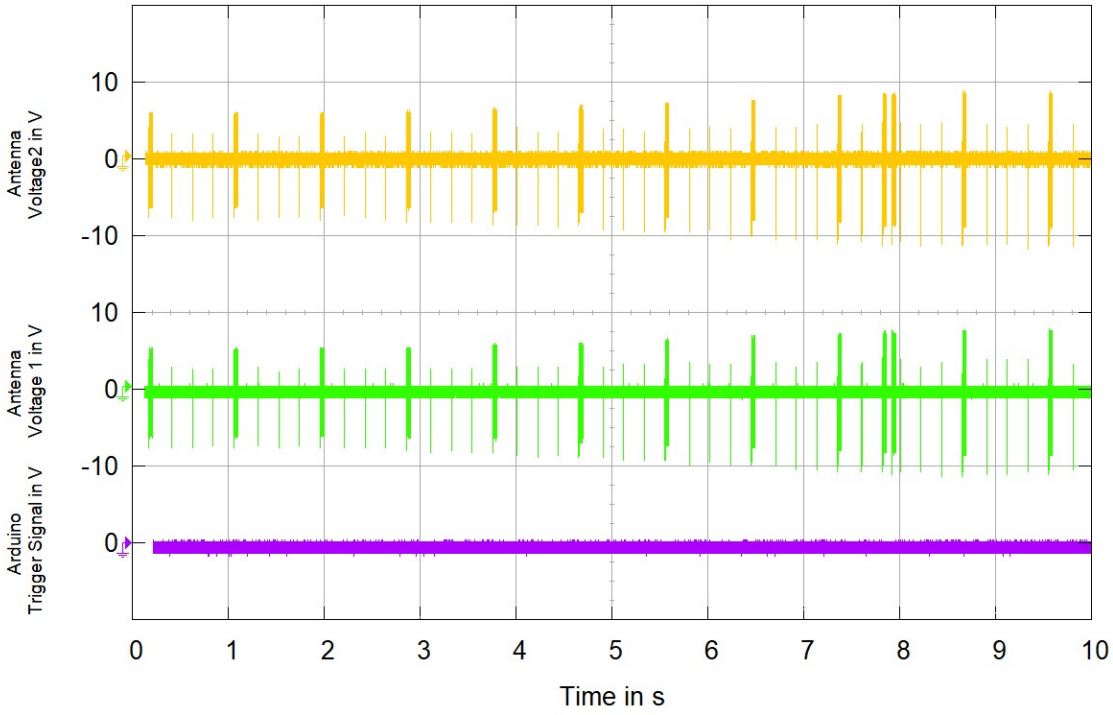

Figure 29: Card detection with normal transponder behaviour.

Figure 30 shows a test of a switching pattern, where the green and yellow signals show the two antenna voltages and the red one the field detection signal. The violet signal is the trigger signal generated by the Arduino and shows the duration of the switching. In this example the Arduino is programmed to start a switching sequence at every 11th detected pulse. Since the board does not have a chip, which can communicate with the reader, the smartphone is not able complete detecting a card. Instead the triggering of the LPCD causes repeated card polling out of the normal sequence. In Figure 30 it can be seen, that four consecutive card polls are conducted by the reader after a switching sequence which confirms that the transponder is detected by the reader.

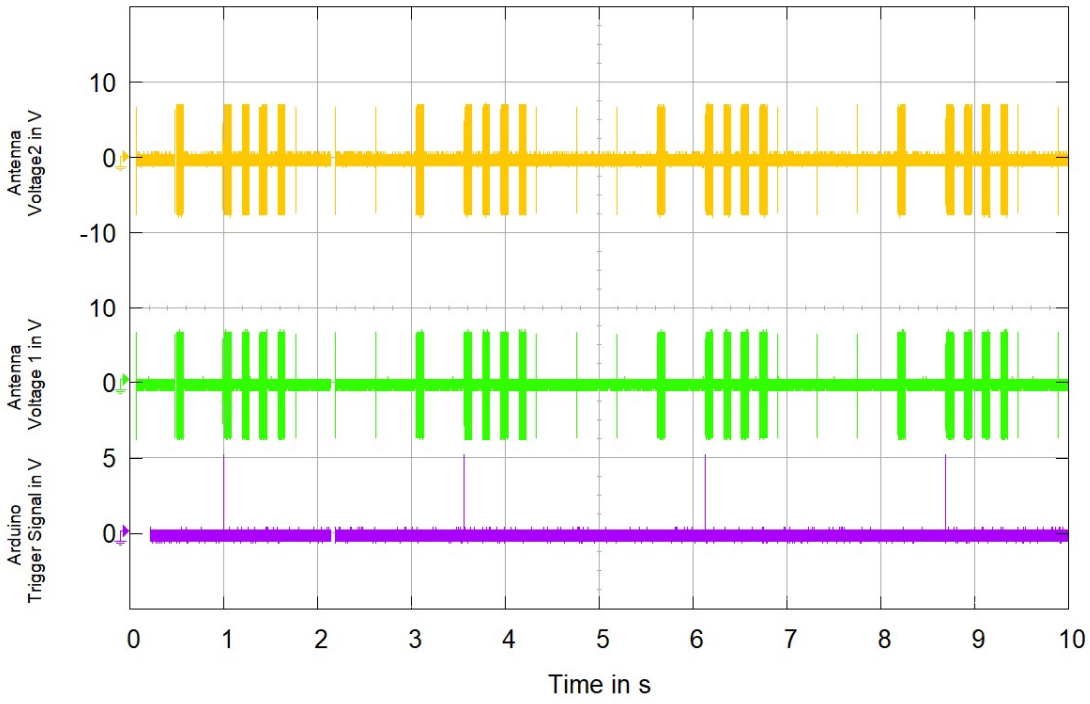

Figure 30: Card detection with modified transponder.

4.4 Detuning

To verify the effective detuning of the circuit, caused by the analogue switches, the resonant frequency is measured for different conditions. The impact of adding a capacitance to the resonant circuit is dependent on the absolute properties of the circuit, which mostly consists of parasitic elements. So first the antenna is observed alone to determine the actual inductance L as well as the parallel capacitance of the antenna Cp.

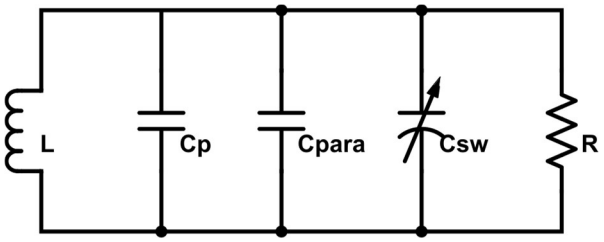

Figure 31: Equivalent circuit of the Demonstrator board.

To do this the antenna is detached from the board and the resonant frequency is measured with a network analyser with a variety of different capacitors (C_1 … C_i) soldered parallel to the antenna. Using Formula 4 the following equations can be derived.

$$f_1 = \frac{1}{2\pi\sqrt{L(C_p + C_1)}} \tag{7}$$

$$f_i = \frac{1}{2\pi\sqrt{L(C_p + C_i)}} \tag{8}$$

With the measured resonant frequencies, the antenna properties can be calculated.

$$C_p = \frac{C_1 - C_2 * \left(\frac{f_i}{f_1}\right)^2}{\left(\frac{f_i}{f_1}\right)^2 - 1} \tag{9}$$

$$L = \frac{1}{(2\pi f_1)^2 (C_p + C_1)} \tag{10}$$

Next, the parasitic capacitance of the board Cpara is determined. This time the same measurement as before is done with the whole board. The switches stay idle and again different capacitors are soldered on the board and the resonant frequencies measured. The difference in the calculated parallel capacitances is the parasitic capacitance of

the board Cpara. By doing so the parameters are determined to be: L=3.53µH, Cp=4.19pF, Cpara=13.82pF. In Figure 32 the two measurements are plotted. The difference of the curves shows the difference in the detuning sensitivity caused by the parasitic capacitances of the board.

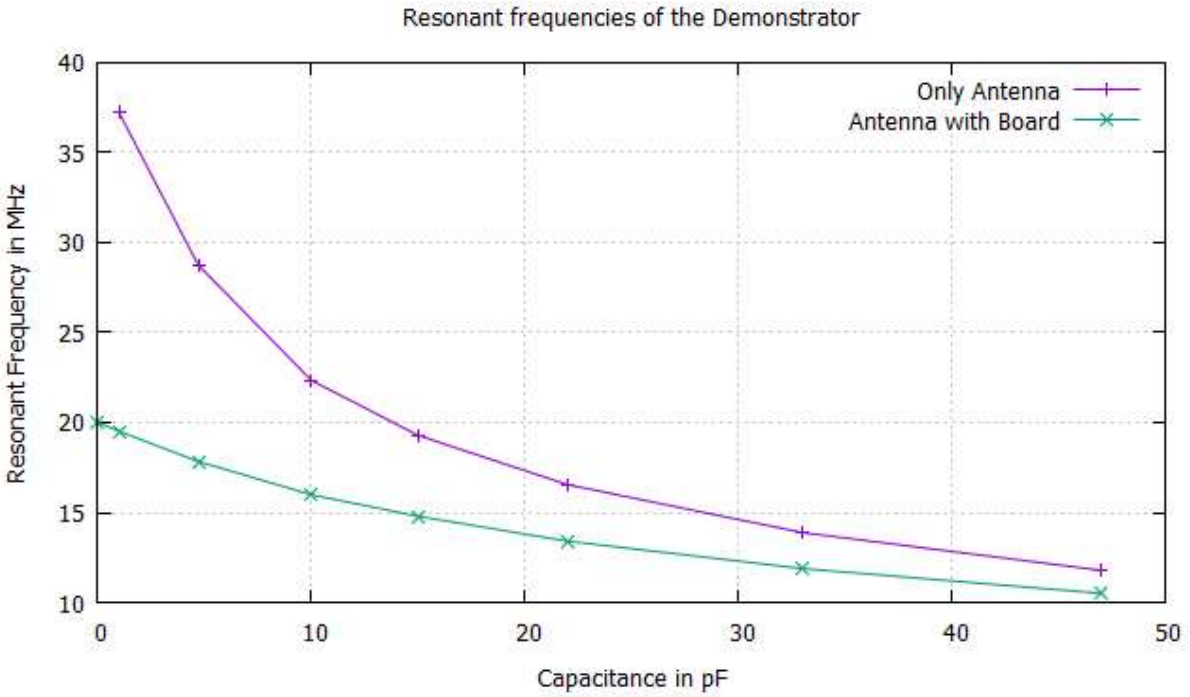

Figure 32: Plot of Demonstrator board resonant frequencies.

4.5 Evaluation Board

For a more detailed analysis the PN5180 Evaluation board [12] is used as reader device. This allows to operate the LPCD manually as well as to access the registers of the reader. The board is connected to a laptop by USB and controlled with the NFC Cockpitv.4.7.0. The main objective of this is to read out the AGC value of the reader repetitively to show the impact of the transponder in detail.

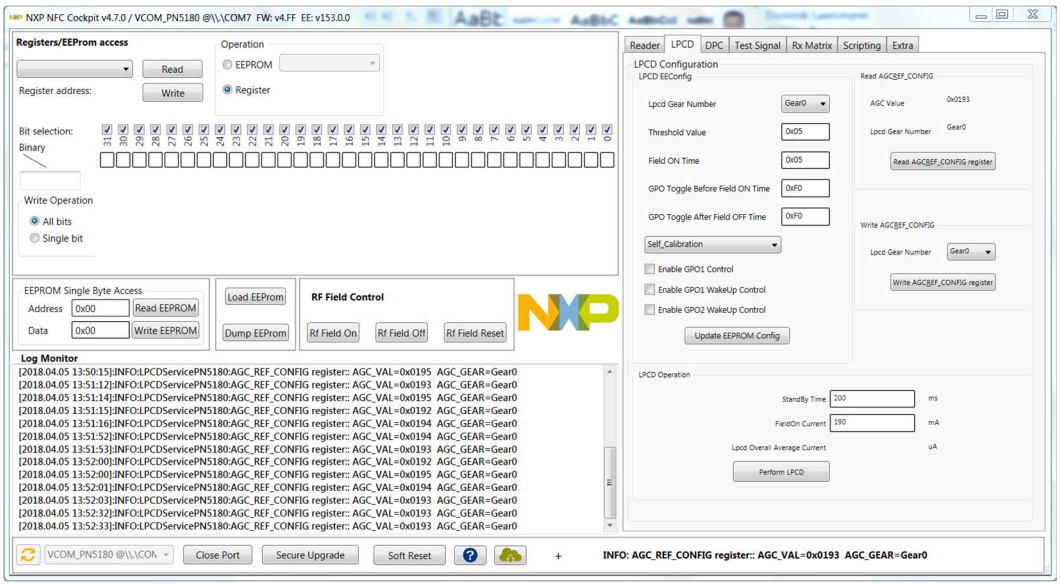

Figure 33: NFC Cockpit LPCD GUI.

The AGC value register is now read out, while the capacitance of the board is switched through every possible value and the distance to the reader remains unchanged at 80mm. Because the range of the capacitor bank is only 9.3pF, 3 measurement series are acquired with different trim capacitor positions and the results averaged. The resulting AGC values are shown in Figure 34 and confirm the simulation results (see Figure 10). At the resonant tuning the feedback on the reader becomes a maximum.

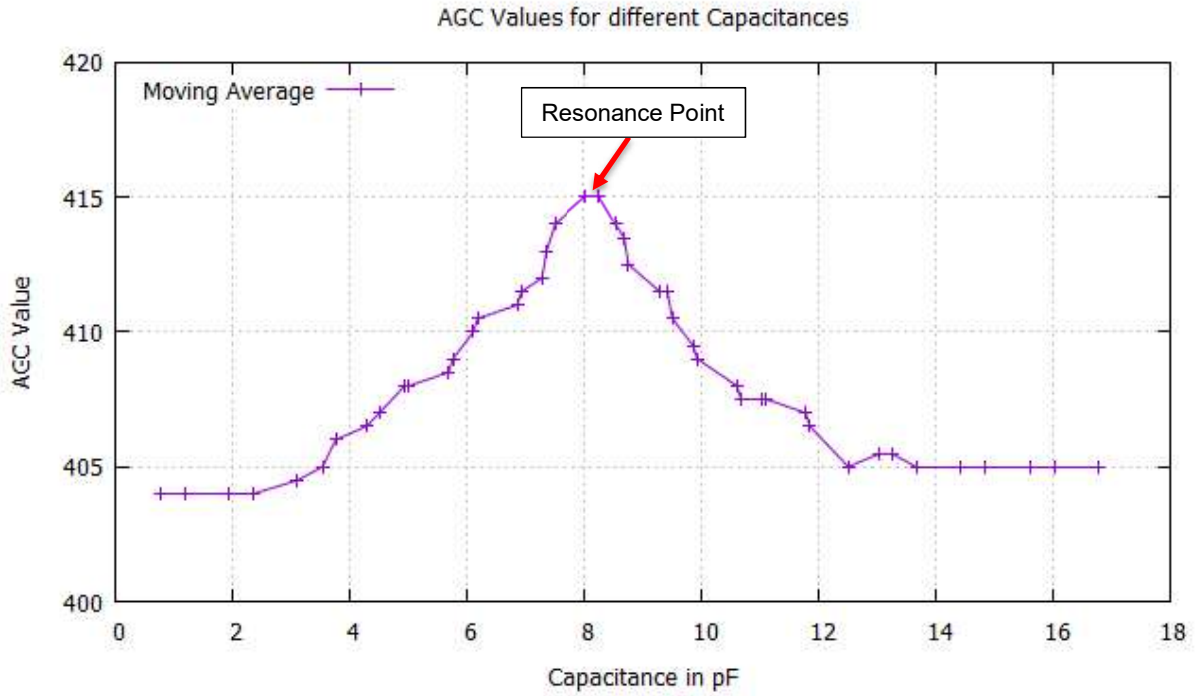

Figure 34: Plot of AGC value over capacitance.

Next the AGC values of the idle and tuned board are compared to the values of a reference tag with an ID1 antenna and a chip. It can be seen in Figure 35 that the behaviour of the board differs significantly from the reference tag. It is also observed that the LPCD detection range of the board, which is measured to be 105mm exceeds any standard tags by far. This results from the high antenna voltage of the board, which is limited by only 12V Zener diodes meant to protect the analogue switches. This causes a higher quality factor than in a normal application. So, in order to get relevant measurement data these diodes are replaced by 3.6V Zener diodes and so the voltage is limited to a more realistic value. The resulting AGC values are shown in Figure 35.

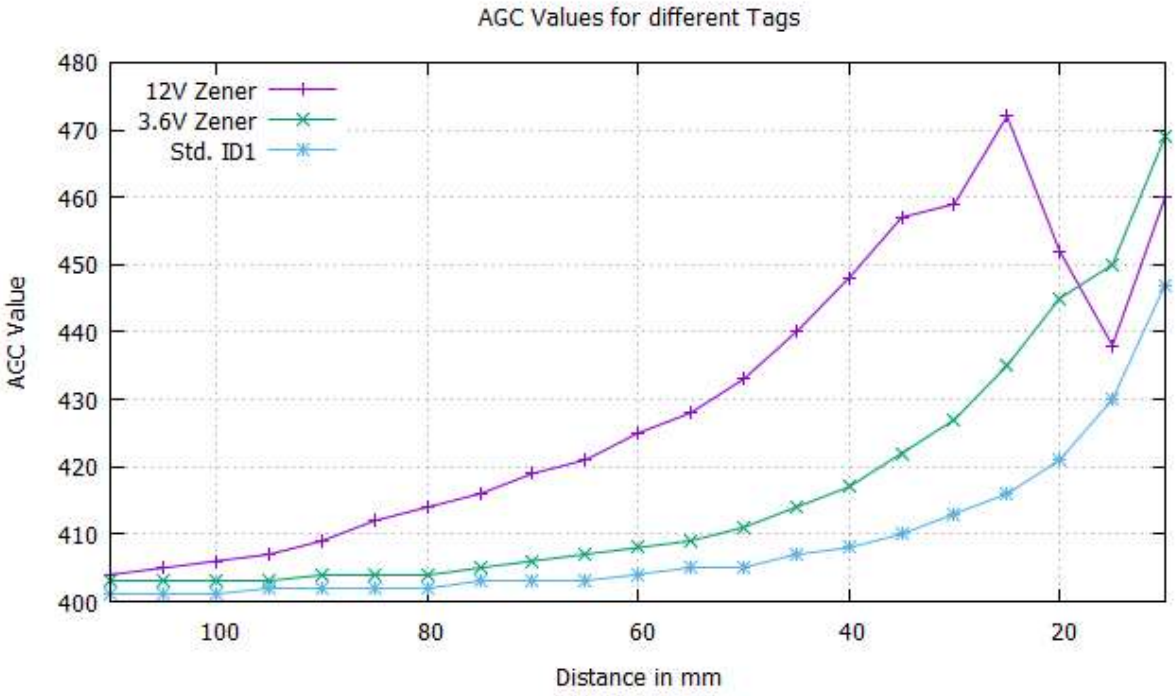

Figure 35: Plot of AGC values for different tags.

It can also be seen in the Figure 35, that the measurement becomes inconsistent if the AGC value gets too high. This is due to the Dynamic Power Control (DPC) feature of the PN5180 [16] which reduces the current of the reader when the detuning becomes too strong in order to keep the antenna voltage in a desired range.

To evaluate the changes caused by the switching of the different capacitances the AGC values are measured with a board tuned slightly above 13.56Mhz. The resonant frequency is measured to be 14.26MHz so it is about 5% higher than 13.56MHz which is a typical detuning for most applications. Figure 36 shows that for this case the AGC values are slightly improved by switching a capacitance. By adding 5pF to the board capacitance an improvement of up to 3 AGC values is observed. Also, the reader appears to be most sensitive to this at medium to long distances, which is beneficial to increasing the detection range.

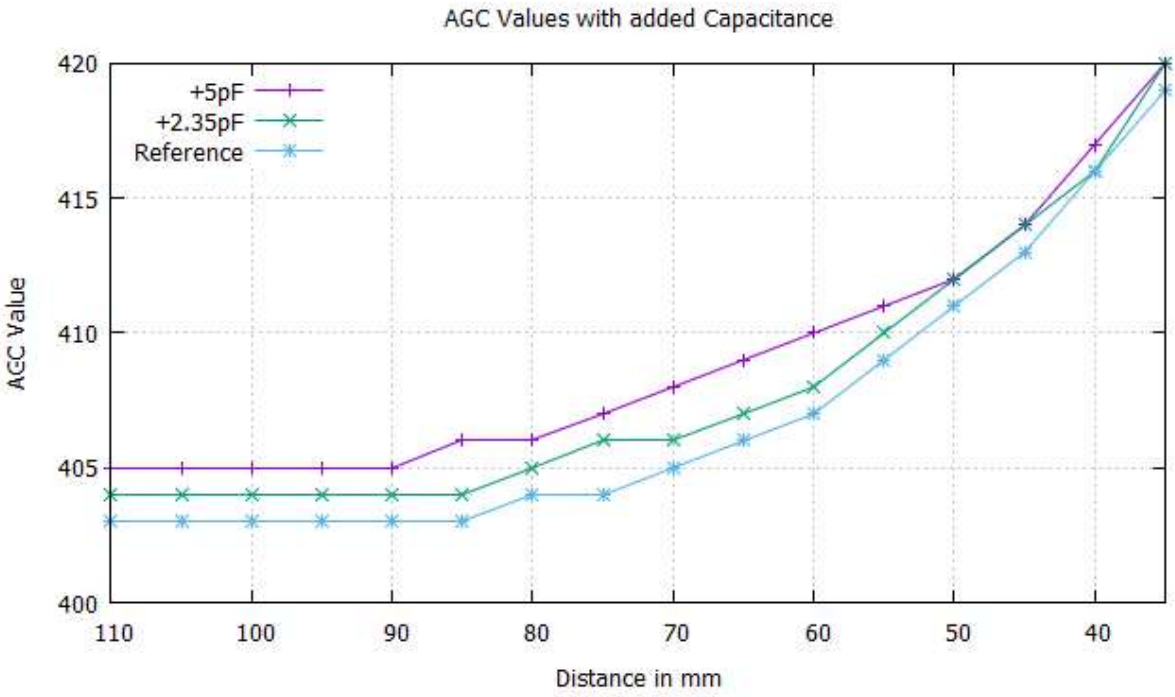

Figure 36: Plot of AGC value improvement.

4.6 Card Detection Range of a Smartphone

The previous test is now repeated with smartphones as reader to determine the change of the detection range. It can be seen from the results in Figure 37 that while not all smartphones are impaired by the detuning in the same way the range can be improved.

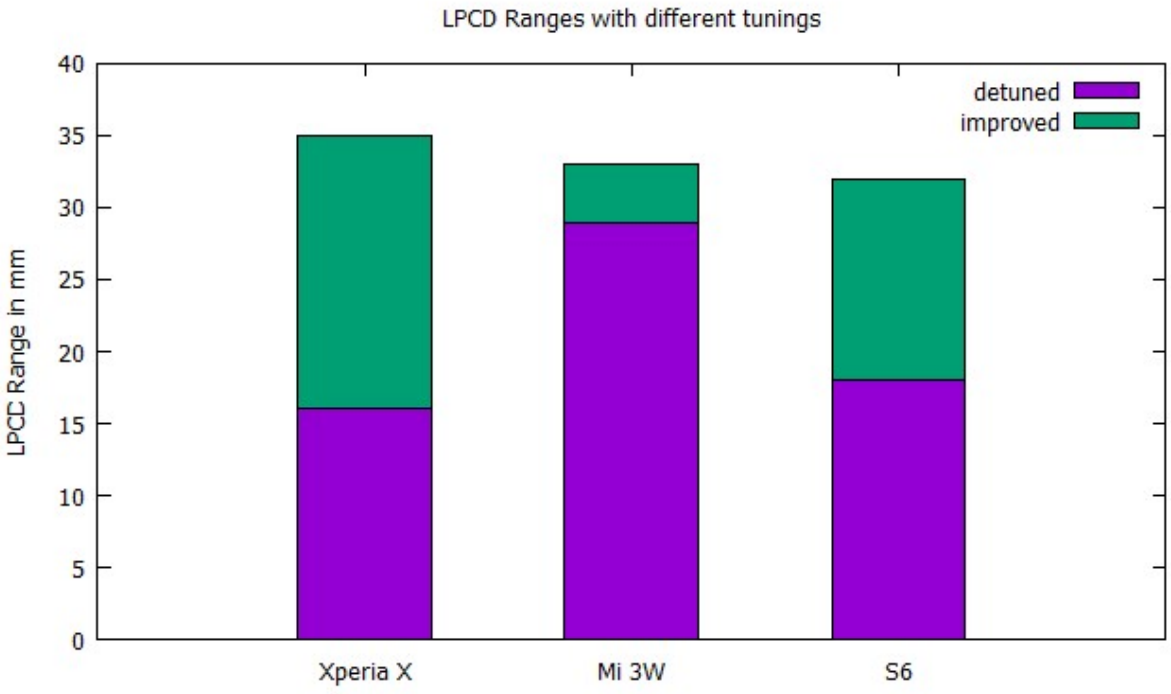

Figure 37: Plot of LPCD range improvement.

5 Discussion

In this thesis several state of the art as well as experimental methods to detect transponders in RFID systems are examined. One of the major use cases are electronic article surveillance systems, which use frequency wobbling to detect simple transponders. These systems profit from the large size of the reader antennas as well as the stationary type of application which comes with generous power supply options. These boundary conditions allow a high detection range and cheap labels and therefore these systems are widely used. While the power consumption for passive transponders has always been a constraint in recent times smartphones and other mobile RFID and NFC solutions became increasingly popular creating the need for power consumption optimization on the reader side. This is achieved by so called Low Power Card Detection methods, which are the main focus of this thesis. Possible implementations are the observation of the oscillation behaviour while turning the field on or off, or measuring the decay time of the field. There are also systems which use a variation of frequency wobbling. But most implementations use a measurement of the reader antenna properties to detect a change in the transponder feedback effectively described by the transimpedanz.

One essential factor looked at is the resonance frequency of the transponder. It is well known that in order to supply the transponder a good tuning is beneficial, because of the higher gain in the resonant circuit. The antenna voltage of the reader is also influenced by this. When the transponder is tuned exactly, the transimpedanz only has a real part and is a maximum. This causes the strongest feedback and the smallest antenna voltage. The exact behaviour between transponder tuning and reader antenna voltage is quantified for an example system. It is shown that this voltage also follows a curve similar to a resonant curve. Most transponders are not tuned exactly, the effect of compensating this tuning was shown with the demonstrator board in combination with different smartphones. It is seen that compensating this detuning can increase the range of the smartphones LPCD.

Another factor shown to be crucial is the quality factor of the transponder. It is seen that, by increasing the limiting voltage threshold of the transponder, which translates to a different quality factor, the range of the LPCD can be increased significantly and also the impact of the tuning is increased. In a normal application the quality factor is determined by the power consumption of the chip as well as the needed bandwidth for the communication that considers the sub carrier signals. In general transponder designers are challenged with a trade-off between data rate and range. Since for card detection no communication is needed, a higher quality factor during card detection can be a promising option. Another limiting factor is the voltage limiter implemented in transponder ICs. This is done to protect the IC from too high voltages on the pins connected to the antenna, that might damage the chip. Usually this limiter already limits the voltage to the highest possible value that the technology of the chip allows, but still this effectively causes a reduction of the quality factor of the system. Overcoming this problem would be a good way to increase the range of the LPCD.

In order to integrate this methods in a chip, certain adaptions have to be made. In this thesis a changing topology of the transponder is implemented by a PCB with analogue switches. These switches require a supply voltage greater than the switched signal, which is a problem when generating the supply from said signal. This problem was avoided using an external supply, but when implementing this on chip level monolithic transistors can be used to switch these signals eliminating this problem. Also, to tune the transponder automatically additional circuit blocks are needed to measure the transponder voltage.

Bibliography

[1] A. Marinčić, Z. Civrić, B. Milovanović, “Nikola Tesla’s Contributions to Radio Developments”, Serbian Journal of Electrical Engineering, vol. 3, no. 2, pp.131–148, November 2006.

[2] H. Stockman, “Communication by Means of Reflected Power”, Proceedings of the IRE, pp. 1196–1204, 1948.

[3] J. Dethloff, "Identifizierungsschalter" DE000001945777C3 issued September 10, 1969.

[4] ISO/IEC 10536:2008, “Identification cards — Contactless integrated circuit(s) cards — Close-coupled cards”, ISO, Geneva, Switzerland, 2008.

[5] ISO/IEC 14443:2008, “Identification cards — Contactless integrated circuit cards — Proximity cards”, ISO, Geneva, Switzerland, 2008.

[6] ISO/IEC 15693:2008, “Identification cards — Contactless integrated circuit(s) cards — Vicinity Integrated Circuit(s) Card”, ISO, Geneva, Switzerland, 2008.

[7] Company Public Application Note, “CLRC663, MFRC631, MFRC 630, SLRC610 Low Power Card Detection”, Appl. Note AN11145, NXP Semiconductors, May 2015.

[8] P. H. Thevenon, O. Savry, S. Tedjini, “Minimization of energy consumption in passive HF contactless and RFID systems”, SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks, September 2011, Split, Croatia.

[9] A. Kozitsky et al., “NFC and RFID Reader Ultra-Low-Power Card Presence Detection Using MSP430 and TRF79xxA”, Application Report SLOA184, pp. 6-13, Texas Instruments, March 2013.

[10] Company Public Product Data Sheet, “PN5180A0xx/C1/C2 High-performance multi-protocol full NFC Forum-compliant frontend” Product data sheet 240933, NXP Semiconductors, July 2015 [Revised July 2017].

[11] K. Finkenzeller. “RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication”, Carl Hanser Verlag München, 7th Edition, 2015.

[12] Company Public Application Note, “PN5180 Evaluation board quick start guide”, Appl. Note AN11744, NXP Semiconductors, April 2016.

[13] Data Sheet, “Low Capacitance, Low Charge Injection, ±15 V/+12 V iCMOS Quad SPST Switches” ADG1212 data sheet, Analog Devices, July 2005 [Revised Feb. 2009].

[14] Theresa Corrigan, “Operating the ADG12xx Series of Parts with ±5 V Supplies and the Impact on Performance”, Appl. Note AN-874, Analog Devices, 2008.

[15] ISO/IEC 10373-7:2008, “Identification cards — Test methods — Part 7: Vicinity cards”, ISO, Geneva, Switzerland, 2008.

[16] Company Public Application Note, “Dynamic Power Control” Appl. Note AN11742, NXP Semiconductors, December 2016.

[P1] Charles, Alexandre, "Detection of the presence of a contactless communication element within the range of a terminal." European Patent Office, Patent Number EP2148289 B1, issued July 21, 2009.

[P2] Jonely, Michael B.,"Rfid detection system." United States Patent and Trademark Office, Patent Number US9411993 B2, issued March 14, 2013.

[P3] Karandikar, Niranjan, "Highly selective low-power card detector for near field communications (nfc)" United States Patent and Trademark Office, Patent Number US9819401 B2, issued September 24, 2015.

[P4] Kormann, Leonhard, "Nfc or rfid device rf detuning detection and driver output power regulation." European Patent Office, Patent Number EP3156935 A1, issued September 26, 2016.

[P6] Lee, Kevin Douglas, "Systems and methods for detecting and identifying a wireless power device." United States Patent and Trademark Office, Patent Number US9252846 B2, issued May 04, 2012.

[P7] Karandikar, Niranjan, "Card detect architecture for near field communications."

United States Patent and Trademark Office, Patent Number US9438317 B2, issued December 19, 2014.

[P8] Kim, Jun Ho, "Nfc card reader, system including nfc card reader, and a method of operating the same." United States Patent and Trademark Office, Patent Number US20160105220 A1, issued October 13, 2015.

Program Code

Capacitance Test Program

```
//pin 0 and 1 reserved for serial communication

//DO NOT CHANGE
const byte cont_1 = 7;
const byte cont_2 = 6;
const byte cont_3 = 5;
const byte cont_4 = 4;

void setup() {
  pinMode(cont_1, OUTPUT);
  pinMode(cont_2, OUTPUT);
  pinMode(cont_3, OUTPUT);
  pinMode(cont_4, OUTPUT);

  Serial.begin(9600);
  while(!Serial);
  Serial.println("Serial started");
}

void loop() {
  char buffer[80];
  byte code;
  byte port;

  Serial.println("Sweep started");
  for(code=0;code<=15;code++){
    port = PORTD;
    port &= B00001111;
    port |= 0 << 4;
    PORTD = port;
    sprintf(buffer, "Code: %2d", code);
    Serial.println(buffer);
    delay(15000);
  }
}
```

Demonstrator Board Program

```
//pin 0 and 1 reserved for serial communication

const byte interrupt_pin = 2;
const byte trigger_pin = 11;

//DO NOT CHANGE
const byte cont_1 = 7;
const byte cont_2 = 6;
const byte cont_3 = 5;
const byte cont_4 = 4;

//Change C Values (0-15)
const byte code_on = 12;
const byte code_off = 0;

//Do Switching Sequence at every xth detected Pulse, 1 for AGC measurements
const byte switching_rate = 1;

volatile byte field_detected = LOW;

//Debug Info
volatile byte pulse_count = 0;
volatile unsigned long last = 0;
volatile unsigned long time_u = 0;

void setup(){

  int port = 0;

  attachInterrupt(digitalPinToInterrupt(interrupt_pin), fieldDetectionISR,
FALLING);

  //Init Pins
  pinMode(interrupt_pin, INPUT_PULLUP);
  pinMode(trigger_pin, OUTPUT);
  pinMode(cont_1, OUTPUT);
  pinMode(cont_2, OUTPUT);
  pinMode(cont_3, OUTPUT);
  pinMode(cont_4, OUTPUT);

  //Init Switches
  port = PORTD;
  port &= B00001111;
  port |= code_off << 4;
  PORTD = port;

  //Configure Serial Communication
  Serial.begin(9600);
  while(!Serial);
  Serial.println("Serial started");
}
```

```
void loop() {

  char buffer[80];

  if(field_detected)
  {
    detachInterrupt(interrupt_pin);

    //Switch in every xth pulse
    if(pulse_count % switching_rate == 0){
      digitalWrite(trigger_pin, HIGH);
      doSwitching();
      //doSweep();
      digitalWrite(trigger_pin, LOW);
    }
    pulse_count++;

    //Send Debug Information to Host
    time_u = micros();
    sprintf(buffer, "Pulse %04d %6luus %6luus", pulse_count, time_u,
time_u-last);
    last = time_u;
    Serial.println(buffer);

    delay(1);//because of comparator glitching
    //delay(50);//because of card polling, remove for AGC measurements
    attachInterrupt(digitalPinToInterrupt(interrupt_pin),
fieldDetectionISR, FALLING);
    field_detected = LOW;
  }
}

void fieldDetectionISR(){
  if(digitalRead(interrupt_pin)==LOW)
    field_detected = HIGH;
}

//Switch C on and off
void doSwitching(){

  int i;
  byte port = 0;

  delayMicroseconds(20);
  for(i=0; i<1; i++){
    port = PORTD;
    port &= B00001111;
    port |= code_on << 4;
    PORTD = port;
    delayMicroseconds(520);

    port = PORTD;
    port &= B00001111;
    port |= code_off << 4;
    PORTD = port;
    delayMicroseconds(5);
  }
}
```

```
//Sweep C over whole range
void doSweep(){

  int code;
  byte port = 0;

  delayMicroseconds(20);
  for(code=0; code<16; code++){
    port = PORTD;
    port &= B00001111;
    port |= code << 4;
    PORTD = port;
    delayMicroseconds(20);
  }
    port = PORTD;
    port &= B00001111;
    port |= code_off << 4;
    PORTD = port;
    delayMicroseconds(5);
}
```

Part List

Device	Name	Package
Schottky Diode	MMBD301LT1	SOT23
Zener Diode	BZX84C12L	SOT23
Zener Diode	BZX84C3V6	SOT23
TSV Diode Array	DT2042-04T	TSOT-26-6
Analog Switch	ADG1212	TSSOP16
Voltage Controller	LM7805	TO220
Operational Amplifier	LM311	SO08
Microcontroller Board	Arduino Uno Rev 3	PCB

Table 2: Special devices used for the Demonstrator Board.

Measurement Data

	Antenna			Board	
Ci	fi	Cp	L	fi	Cp + Cpara
pF	MHz	pF	uH	MHz	pF
0	-	-	-	20.00	-
1	37.20	-	-	19.50	19.25
4.7	28.75	4.49	3.34	17.83	18.15
10	22.34	4.07	3.61	15.98	17.62
15	19.28	4.14	3.56	14.78	18.02
22	16.54	4.17	3.54	13.40	17.92
33	13.88	4.17	3.54	11.88	17.97
47	11.78	4.12	3.57	10.50	17.88

Table 3: Resonant frequency measurement data.

Series1		Series2		Series3	
C	AGC	C	AGC	C	AGC
pF	DEC	pF	DEC	pF	DEC
0.0	404	3.8	407	7.5	415
0.8	404	4.5	408	8.3	415
1.2	404	4.9	408	8.7	414
1.9	404	5.7	409	9.4	411
2.4	404	6.1	411	9.9	409
3.1	405	6.9	412	10.6	407
3.5	405	7.3	413	11.0	407
4.3	406	8.0	415	11.8	406
5.0	408	8.8	411	12.5	405
5.8	409	9.5	410	13.3	405
6.2	410	9.9	409	13.7	405
6.9	411	10.7	408	14.4	405
7.4	413	11.1	408	14.9	405
8.1	413	11.9	407	15.6	405
8.5	413	12.3	407	16.0	405
9.3	412	13.0	406	16.8	405

Table 4: Capacitance vs AGC value measurement data.

Distance	12V Zener	3.6V Zener	ID1
mm	DEC	DEC	DEC
110	404	403	401
105	405	403	401
100	406	403	401
95	407	403	402
90	409	404	402
85	412	404	402
80	414	404	402
75	416	405	403
70	419	406	403
65	421	407	403
60	425	408	404
55	428	409	405
50	433	411	405
45	440	414	407
40	448	417	408
35	457	422	410
30	459	427	413
25	472	435	416
20	452	445	421
15	438	450	430
10	460	469	447
5	382	453	461

Table 5: Distance vs AGC value for different tags measurement data.

Distance	Reference	+2.35p	+5p
mm	DEC	DEC	DEC
110	403	404	405
105	403	404	405
100	403	404	405
95	403	404	405
90	403	404	405
85	403	404	406
80	404	405	406
75	404	406	407
70	405	406	408
65	406	407	409
60	407	408	410
55	409	410	411
50	411	412	412
45	413	414	414
40	416	416	417
35	419	420	420
30	424	424	425
25	429	430	431
20	438	438	439
15	449	448	450
10	452	451	454
5	471	472	473

Table 6: Distance vs AGC value for different tunings measurement data

	detuned	+5p
	mm	Mm
Xperia X	16	35
Mi 3W	29	33
S6	18	32

Table 7: Detection ranges measurement data.