HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

DIPLOMARBEIT

Herr Ing.

Hans-Jürgen Pirch

PICC Modulation Analysis

Mittweida, 2014

Information Technology & Electrical Engineering

DIPLOMA THESIS

PICC Modulation Analysis

author:
Mr. Ing. Hans-Jürgen Pirch

course of studies:
Computer Engineering

seminar group:
KT10wWA-F

first examiner:
Prof. Dr-Ing. Volker Delport

second examiner:
Dipl.-Ing. Uwe Schnabel

submission:
Linz, 2.10.2014

defence/ evaluation:
Mittweida, 2014

Fakultät Elektro- und Informationstechnik

DIPLOMARBEIT

Analyse von PICC Modulation

Autor:
Herr Ing. Hans- Jürgen Pirch

Studiengang:
Technische Informatik

Seminargruppe:
KT10wWA-F

Erstprüfer:
Prof. Dr-Ing. Volker Delport

Zweitprüfer:
Dipl.-Ing. Uwe Schnabel

Einreichung:
Linz, 2.10.2014

Verteidigung/Bewertung:
Mittweida, 2014

Bibliographic description / Bibliografische Beschreibung:

Pirch, Hans-Jürgen:

PICC Modulation Analysis - 2014 - 17, 66, 19 S.

Mittweida, Hochschule Mittweida, Fakultät Elektro- und Informationstechnik, Diplomarbeit, 2014

Abstract:

This diploma thesis discusses interoperability problems between certified RFID readers and transponders based on the ISO/IEC14443 standard and the root cause for them. The main goal is the definition of new test methods and parameters that can supplement the existing test regime for such systems and allow the identification of those problems beforehand.

Acknowledgements:

I would like to thank Dipl.-Ing. Uwe Schnabel for guiding and supporting me during the course of this work and for providing me a forum in the RFID community. Furthermore I would like to thank Prof. Dr-Ing. Volker Delport for all the useful comments and taking on this work, although we never met in person. I would also like to thank my company HID Global for financing my studies, as well as my colleagues from the research and development department who cross-read my work and helped me to eliminate various spelling and grammar issues. At the end I would like to express my appreciation to my partner Theresa who supported me the entire time, by keeping me balanced and helping me putting pieces together.

Table of Contents

List of Figures

List of Tables

List of Equations

Terms and Abbreviations

ASK	Amplitude Shift Keying
BSI	Federal Office for Information Security (Germany)
BP	Bandpass Filter
BPSK	Binary Phase Shift Keying
CRC	Cyclic Redundancy Check
EMC	Electromagnetic Compatibility
EMD	Electromagnetic Disturbance
fc	Carrier Frequency (13.56MHz)
fs	Subcarrier Frequency (fs/16 = 847.5kHz)
FFT	Fast Fourier Transform
FSK	Frequency Shift Keying
H	Magnetic Field Strength
IC	Integrated Circuit
ISO	International Organization for Standardization
kbps	Kilobits per Second
LMA	Load Modulation Amplitude
LP	Lowpass Filter
LSB	Lower Sideband
NFC	Near Field Communication
NRZ	None Return To Zero
PCB	Printed Circuit Board
PCD	Proximity Coupling Device

PICC	Proximity Integrated Circuit Card
PSK	Phase Shift Keying
Q	Quality factor
RefPICC	Reference PICC
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Root Mean Square (quadratic mean)
SNR	Signal to Noise Ratio
SPICE	Simulation Program with Integrated Circuit Emphasis
SRF	Self Resonance Frequency
UHF	Ultra High Frequency
USB	Upper Sideband

1 Introduction

In this introductory section the purpose and main objective of this diploma thesis is discussed. It also provides an overview on the organization of the document.

1.1 Purpose

RFID systems based on the ISO/IEC 14443 standard have found widespread application in areas such as physical access, cashless payment and e-government.

The number of applications is still growing and other technologies based on ISO/IEC14443 are emerging (e.g. Near Field Communication NFC).

The International Organization for Standardization (ISO) has developed various test methods ([ISO05] to [ISO07]) to ensure interoperability between transponders (proximity IC cards or PICCs) and readers (proximity coupling devices or PCDs). These test methods are described in the standard ISO/IEC10373-6. National institutions such as the Federal Office for Information Security in Germany (BSI) have created certification processes for PCD and PICC manufacturers based on the applicable test standards, again intended to ensure the interoperability between certified PICC (e.g. Electronic Passport or Citizen Card) and PCD products.

However, numerous cases have been observed in which a certified PCD product fails to read a certified electronic document (PICC) for reasons related to the RF interface. This indicates shortcomings in the current standards and test procedures.

These shortcomings in the specifications may have led to the use of receiver concepts in common RFID reader IC's, that will result in communication failure under certain circumstances. Any remedy could only practically be applied to future PICC's because of the large and widespread use of existing PCD's containing such IC's.

1.2 Objective

Observations from the field have shown that PCD’s and PICC’s can be certified against today’s standards, but still be incompatible with each other. Services that require high reliability, such as cashless payment or e-government, are especially affected by such interoperability issues.

This thesis focuses on the analysis of the PICC modulation with the goal of identifying the root cause of the observed problems. The results of this analysis shall lead to test parameters/procedures that can identify such problematic RF interface behaviours and prevent affected PICCs from being rolled out into the marketplace.

As a follow-on project outside of the scope of this document, the results shall be submitted to the ISO committee for the extension of today's standards.

1.3 Organization of this thesis

This thesis is subdivided into eight chapters.

After the general introduction an overview of the RFID technology with focus on ISO/IEC14443 is provided in **chapter 2**. In this overview the basic modulation schemes of the standard, as well as today's tests for RFID devices, are briefly explained.

Chapter 3 outlines the scope of work for this thesis and introduces the idea of constellation plots for ISO/IEC14443 transponders.

In **chapter 4** the results of a previous investigation on interoperability problems between a certified PCD and a set of certified PICCs are shown. In addition the individual devices (PCD and PICCs) that showed communication errors are described in more detail.

The measurement setup and the analysis procedure used to generate constellation plots for a PICC modulation are described within **chapter 5**, followed by the results for the various test samples in **chapter 6**.

Chapter 7 defines new test parameters and limits for constellation plots and show how these can be applied to a sample PICC.

Finally **chapter 8** provides a conclusion on the results of the previous chapters, as well as an outlook on the next steps such as future improvements to the suggested analysis procedures. In addition an assessment of the work from the authors point of view is provided.

2 Technology Background and Test Methods

This part of the thesis provides an overview on RFID technology. The focus is set on systems based on the ISO/IEC14443 standard, which are the subject in this document. In addition the test methods for these systems are outlined and potential shortcomings of the existing test regime are discussed.

2.1 Overview RFID systems

RFID systems consist of a reader and a population of transponders (i.e. user cards, tags, etc.). The reader communicates with the transponder, retrieves data and sometimes also transmits data back. They can be subdivided into the following hardware criteria:

- Form factor of the transponder
- Functionality / memory size of the transponder
- Frequency / read range / type of coupling used by the system

[FinKl2002] distinguishes between three categories which are shown in the table below.

Table 2-1: Overview RFID systems

	Close Coupling System	**Remote Coupling System**	**Long Range System**
Typ. Read Range	About 1cm	< 1m	> 1m
Frequency	1Hz-30MHz	120kHz – 13.56MHz	• 868MHz / 915MHz • 2.5GHz / 5.8GHz
Coupling	Inductive coupling	Inductive Coupling	Back scatter effect
Typ. Applications	Physical access	• Physical access • Cashless payment • E-Government	• Item level inventory • Road charge • Livestock
Standards	ISO/IEC10536	• ISO/IEC15693 • ISO/IEC14443	• ISO/IEC18000-6 • ISO/IEC18000-4

2.1.1 Close coupling systems

Close coupling systems are designed for very low read ranges up to about 1cm. This allows the specific placement of the transponder's coil within the air gap of a ring core of the reader. This forms a transformer with good coupling that provides a much higher effective power transfer from the reader to the transponder than can be achieved by the remote coupling or long range systems. However, close coupling systems have largely

become displaced due to the fast development in the area of remote coupling systems and are almost irrelevant in today's market.

2.1.2 Remote coupling systems

Systems with a read range of up to about 1m are called remote coupling systems. Almost all of these systems use inductive coupling for communication and power transfer between reader and transponder (see section 2.2). Today over 90% of the RFID systems sold into the market belong to this category. For that reason a large number of different systems for various applications are available. The carrier frequencies are typically 125kHz or 13.56MHz with only a few exceptions for special purposes running at 27.12MHz. Systems based on the ISO/IEC14443 standard are also within this category and the focus of this thesis.

2.1.3 Long range systems

RFID systems with read range much higher than 1m are typically referred to as long range systems. They operate either at the UHF frequencies 868MHZ (Europe) and 915MHz (USA) or in the microwave range at 2.5GHz and 5.8Ghz. Transponders in long range systems communicate with the reader via the reflection of the electromagnetic wave. In order to send data the tag changes its antenna impedance. This leads to a variation of the reflected wave that can be recognized by the reader. For that reason these systems are also often referred to as backscatter systems.

Passive backscatter transponders achieve typical read ranges of up to 7m, whilst active (battery supported) backscatter transponder may even work up to 20m. It should be noted that an active backscatter transponder is not using the energy of the battery for communication, but only for the supply of the internal electronics.

2.2 Inductive coupling

2.2.1 Working principle

An inductively coupled transponder usually consists of a single chip and an attached coil, which is used as an antenna. Most inductively coupled transponders are passive, meaning that power is supplied by the reader. To this end, the reader produces a high frequency electromagnetic field which the transponder uses.

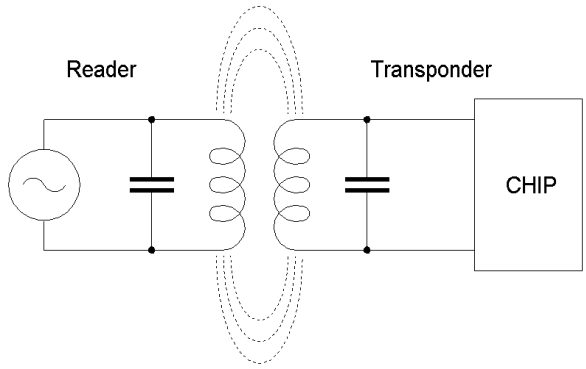


Figure 2-1: Inductively coupled system

Mathematically, the coupling can be treated as a simple alternating magnetic field, as the operating ranges of the system are within the nearfield of the antenna. The nearfield is defined as the area around an antenna where electromagnetic waves have not yet started to develop. This is the case up to a distance of about $\frac{wavelength}{2\pi}$, which equals 3.5m for 13.56MHz systems (for more details see [FinKl2002] section 4.2.1.1).

Both antenna coils (transponder and reader) have a parallel capacitor, creating a parallel resonant circuit. The capacitor is chosen to achieve a resonance frequency near the working/carrier frequency of 13.56MHz.

The arrangement of the two coils can also be interpreted as a loosely-coupled transformer, with a coupling factor which varies with position and geometry.

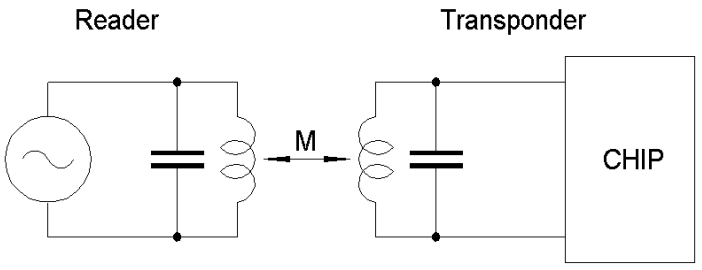


Figure 2-2: Inductively coupled system as transformer with mutual inductance M

2.2.2 Load modulation

As previously mentioned, the inductively coupled system can be interpreted as a transformer. Putting a transponder (with a SRF around 13.56 MHz) into the magnetic field of a reader absorbs energy from the field. This loading of the reader's antenna, caused by the transponder, can be represented as a transformed impedance at the antenna.

To communicate with the reader, the transponder switches an additional load impedance across its own antenna, which results in a further impedance/voltage change at the reader's antenna. Typically ohmic or capacitive load modulation is used.

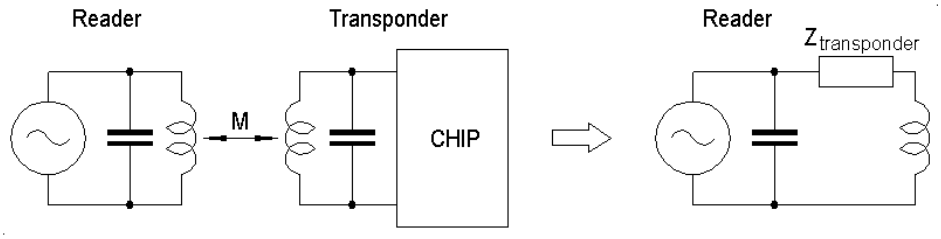


Figure 2-3: Transformed impedance of transponder in reader network

Because of the loose coupling between the reader and the transponder, the voltage change caused by the load modulation is only a few millivolts (about 6 – 45 mV). Considering that the 13.56MHz carrier signal on the reader's antenna may be as high as 100V, the achieved signal to noise ratio is about -80 dB for a transponder signal strength of 10mV, if the carrier voltage is considered as noise.

$$SNR = 20\log(\frac{V_{Transponder}}{V_{Reader}})$$

Equation 2-1: Signal to noise ratio

This small signal is consequently difficult to detect.

For this reason 13.56MHz systems use a subcarrier. Switching the load resistor at a certain frequency *fs* (a sub harmonic of the carrier) results in two sidebands at 13,56MHz +/- *fs*. These two sidebands are more easily detected by the reader. The subcarrier can be ASK, FSK or PSK modulated to carry data.

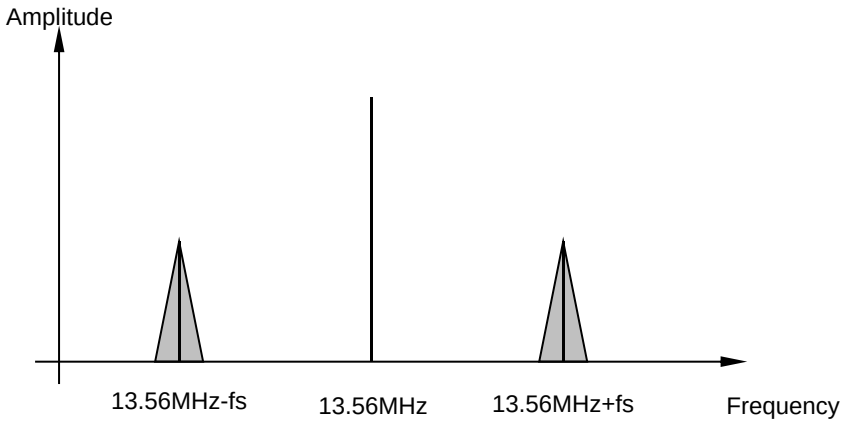


Figure 2-4: Amplitude spectrum caused by load modulation with subcarrier (fs)

2.3 ISO/IEC14443

This section provides a brief overview on the RF interface definitions of the ISO/IEC14443 standard. More detail can be found in the applicable standards ([ISO01] to [ISO04]) as well as in [FinKl2002] section 9.2.2.

ISO/IEC14443 describes the function and operating conditions of proximity IC cards and proximity coupling devices. Systems based on this standard typically show read ranges of 2 to 10cm and have a wide range of applications such as ticketing, cashless payment and physical access. The PICC's usually use a microcontroller for data storage and processing.

The standard consists of four parts:

- Part1: Physical characteristics
- Part2: Radio frequency power and signal interface
- Part3: Initialization and anticollision
- Part4: Transmission protocols

The standard defines two different types of PICCs referred to as type A and type B. The two PICC types differ from each other in their modulation and bit coding (part 2), as well as in their initialization and anticollision (part 3). All work performed within this thesis falls into part 2 of the standard.

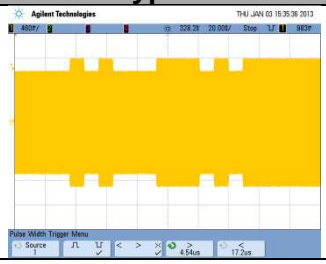
General operation conditions are:

- Field strength: 1.5 - 7.5 A/m
- Read range: typically up to 10cm
- Frequency: 13.56 MHz +/- 7 kHz

2.3.1 PCD communication interface

The following table provides an overview of the communication interface for both PICC types.

Table 2-2: Data transfer reader (PCD) to transponder (PICC)

PCD → PICC	Type A	Type B
Modulation @ 106kbps		
Modulation:	ASK 100%	ASK 10%
Bit coding:	Modified Miller-code	NRZ-code
Baud rate:	106, 212, 424, 848kbps (fc/128 – fc/16)	106, 212, 424, 848kbps (fc/128 – fc/16)

The PCD communicates with the PICC by modulating the carrier either 100% ASK for type A or 10% ASK for type B. As the 100% ASK modulation means that during the modulation the type A PICC is not supplied by any reader field, a modified Miller-code is used. For type B PICCs a simple NRZ bit coding is used.

The following figure illustrates the concepts of both modulation schemes.

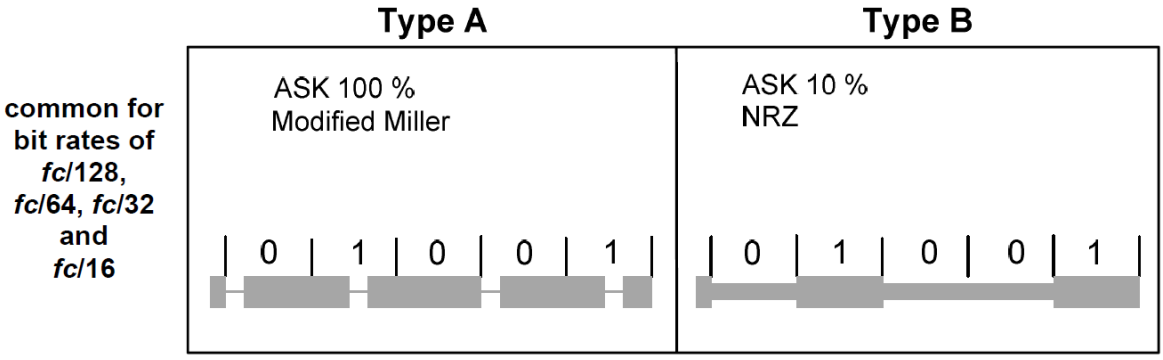


Figure 2-5: Example PCD to PICC communication signals (source: [ISO01])

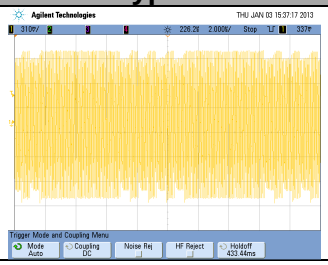
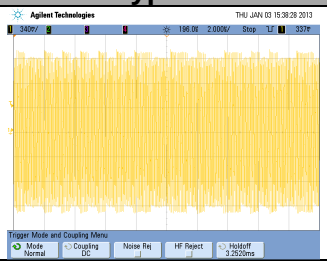
In the modified Miller-code a short modulation pause is either applied in the first half (logical zero) or in the second half (logical 1) of the bit duration. If a one is followed by a zero the modulation pause is omitted to maintain the power supply to the PICC.

In the type B communication scheme a logical one is simply represented by unmodulated field and a logical zero is represented by the modulated (10% lower) field.

2.3.2 PICC communication interface

The PICCs use load modulation to send data back to the PCD. This load modulation is applied with a subcarrier of 847.5kHz (fc/16). The following table provides an overview of the different modulation schemes for type A and B PICCs.

Table 2-3: Data transfer transponder (PICC) to reader (PCD)

PICC → PCD	Type A	Type B
Modulation @ 106kbps		
Modulation:	Load modulation with subcarrier 848kHz (fc/16), ASK / BPSK modulated	Load modulation with subcarrier 848kHz (fc/16), ASK / BPSK modulated
Bit coding:	Manchester code / NRZ-code	NRZ-code
Baud rate:	106, 212, 424, 848kbps (fc/128 – fc/16)	106, 212, 424, 848kbps (fc/128 – fc/16)

Type A cards use a Manchester encoded subcarrier at the lowest communication speed of 106kbps (fc/128). At higher communication speeds the modulation scheme changes to binary phase shift keying as used for type B PICCs.

Figure 2-6 illustrates sample PICC communication signals for all airspeeds.

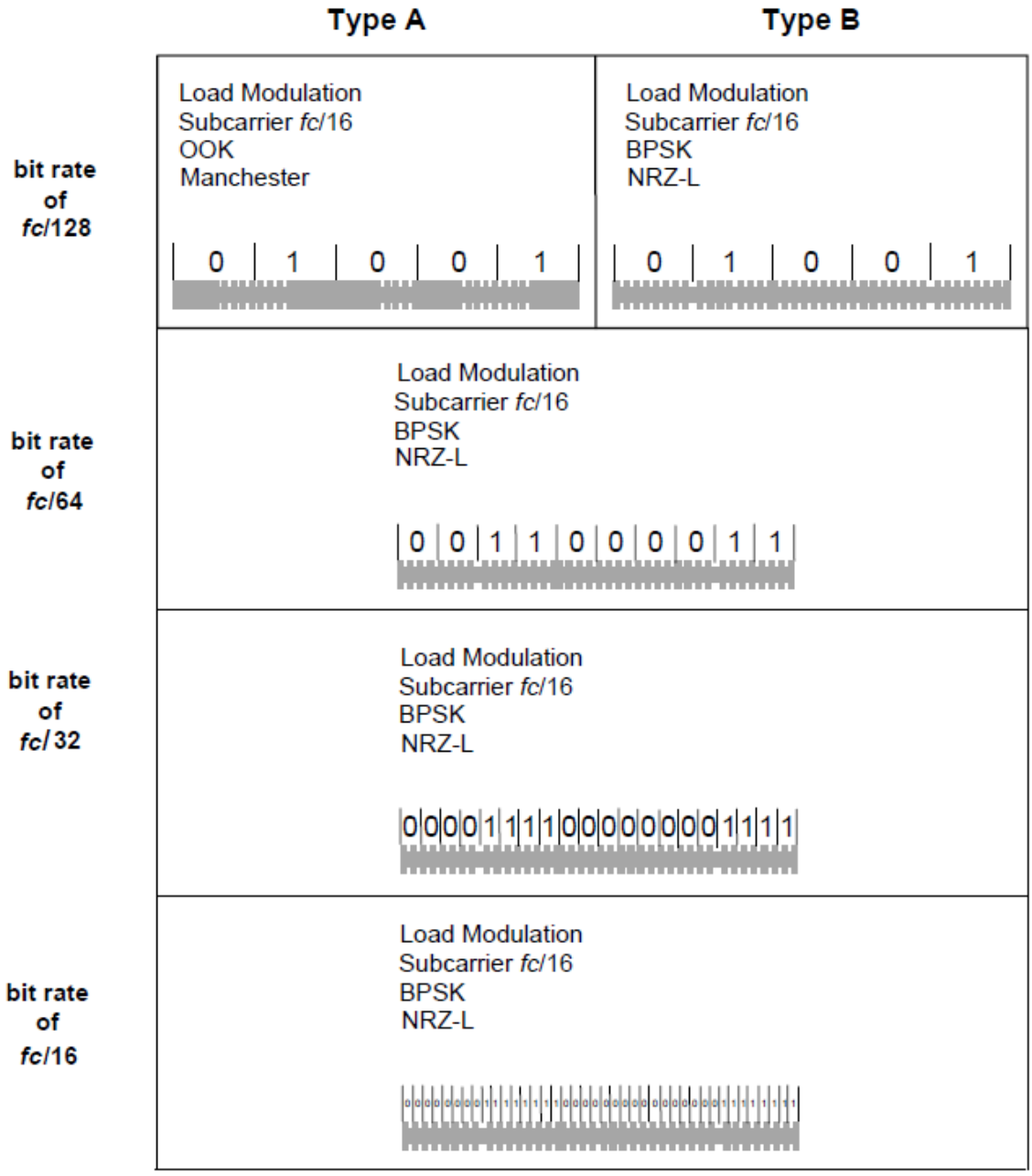


Figure 2-6: Example PICC to PCD communication signals (source: [ISO01])

2.4 Current test methods for proximity RFID systems

The ISO/IEC 10373 was created to define test methods for cards without an IC. These tests focus on general quality requirements such as bending stiffness, resistance to chemicals, flammability, et cetera.

For common data exchange technologies additional test methods were developed and added to the standard in parts. In the case of proximity RFID systems based on ISO/IEC 14443 these test methods are defined in part 6 of the ISO/IEC 10373 ([ISO05] to [ISO07]).

Table 2-4: ISO/IEC10373 identification cards - test methods

Part -1	General
Part -2	Magnetic Stripe Technologies
Part -3	Integrated Circuit Cards (contact cards)
Part -4	Contactless Integrated Circuit Cards (close coupling ISO/IEC 10536)
Part -5	Optical Memory Cards
Part -6	Proximity Cards (according to ISO/IEC 14443)
Part -7	Vicinity Cards (according to ISO/IEC 15693)

The name of the standard is somewhat misleading as it not only defines test methods for the card (PICC), but also for the reader (PCD).

2.4.1 ISO/IEC10373-6 test methods for proximity cards

The ISO/IEC 10373-6 defines tests for each part of the ISO/IEC14443 standard. This means tests for the RF interface defined in [ISO01] to [ISO04] and protocol tests to verify the requirements of the standard.

As the observed communication problems between certified PCDs and PICCs were related to the RF interface, the protocol tests are not further discussed in this section.

The following table provides an overview of the basic RF Interface tests specified for PCDs. Certain tests, for example EMD (Electro Magnetic Disturbance), are left out intentionally as these are concerned with side effects rather than basic RF properties.

Table 2-5: Overview basic PCD RF interface tests

Test Name	Purpose	Comment
PCD field strength	Checks that the field strength of the PCD in the operating volume is within the specified limits	H_{MIN} = 1.5A/m H_{MAX} = 7.5A/m
Modulation index and waveform	Checks that the modulation waveforms of the PCD meet the requirements of ISO/IEC 14443 (e.g. rise/fall time, overshoot, etc.)	Guidance on required signal processing (filtering of measured waveform) is provided by the standard
Load modulation reception	Checks that the PCD is able to decode a certain minimum modulation amplitude produced by a PICC	Test is performed using the Reference PICC which is a model that represents a worst case PICC

The following table shows the corresponding PICC tests. Again, side effect tests such as maximum loading and EMD have been left out.

Table 2-6: Overview basic PICC RF interface tests

Test Name	Purpose	Comment
PICC transmission	Checks that the load modulation amplitude of a PICC is above the minimum limit within the operating field range (1.5A/m to 7.5A/m). At the same time this test verifies that a PICC is working over the complete field strength range	An FFT is calculated over 6 subcarrier cycles to determine the amplitude of the upper and lower sideband in [mV]. The phase of the spectrum is not evaluated
PICC reception	Checks that the PICC is able to receive/decode the PCD modulation	The PCD modulation waveform parameters are varied within the limits to ensure the PICC is able to decode correctly

2.4.2 Potential shortcomings of current test methods

On closer examination, it becomes obvious that the current test procedures fall short of being able to verify the dynamics of a PICC's load modulation signal. Today only the amplitude of the spectrum is evaluated.

For PCD’s there are tests on the modulation depth, which could be viewed as the amplitude of the modulation. In addition the dynamics of the PCD modulation are specified by means of rise and fall times as well as overshoots as shown below.

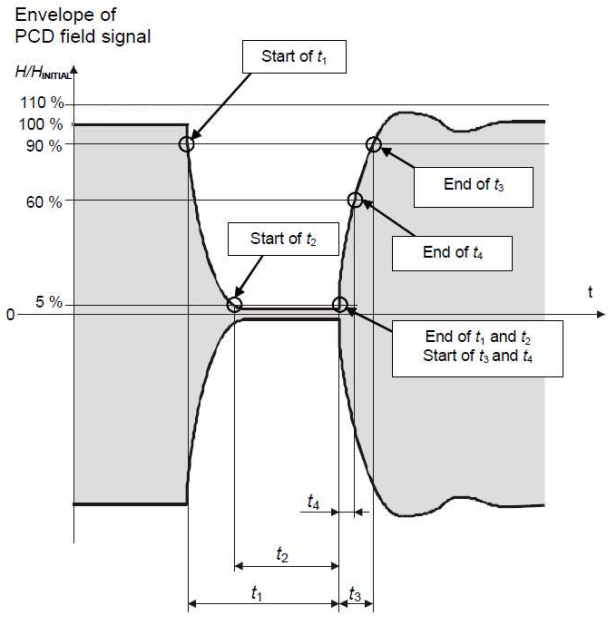


Figure 2-7: ISO/IEC14443 type A modulation pause at 106kbps (source: [ISO01])

To illustrate the shortcomings of current test procedures two PICC load modulation signals were simulated and analysed as required by [ISO05].

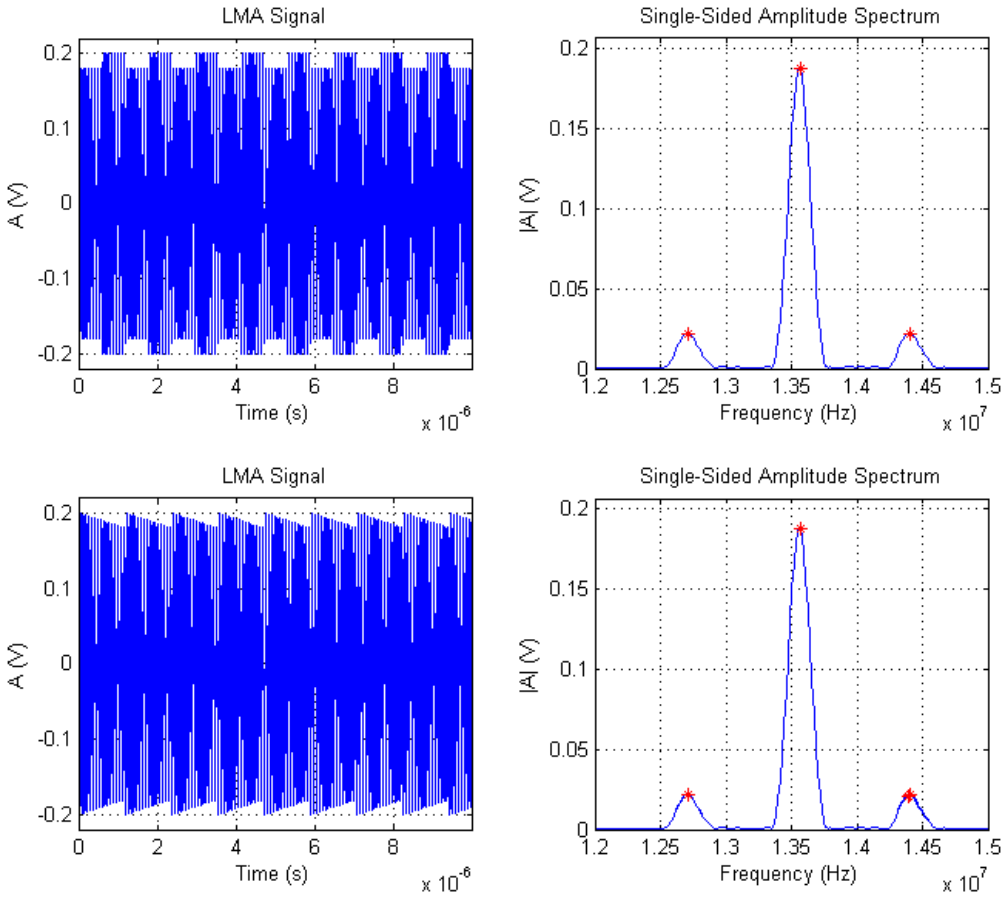


Figure 2-8: Amplitude spectrum for different load modulation waveforms

As shown in Figure 2-8 both load modulation signals result in the same sideband amplitudes in the single sided amplitude spectrum, even though one uses a perfect square modulation whilst the other signal is of a saw tooth shape. Both signals would have the exact same result in a certification process as only the sideband amplitudes need verification, even though it is obvious that the signals are different.

This example shows that the actual load modulation waveform of the signal is not considered at all in today's test regime. Due to this, any distortions in the load modulation would be ignored. It should be noted that the saw tooth waveform was chosen as a purely theoretical example and may not necessarily lead to a communication problem in a real life scenario.

3 Scope of Work

This part elaborates on the objectives of the thesis and outlines the scope of work. To achieve this, a closer look at the dynamics of PICC load modulation is taken as a theoretical basis for the task definition.

3.1 Dynamics of PICC load modulation

Load modulation is generated through an impedance change within the PICC. This impedance change results in phase and amplitude variation in the magnetic field contribution of the PICC.

A current flowing through a coil produces a magnetic flux Φ proportional to that current. Conversely, voltage is induced in a coil that is exposed to a changing magnetic field, according to Faraday's law of induction.

$$\vec{V}in = -N \cdot \frac{d\phi}{dt}$$

$$\vec{\phi} = \vec{B} \cdot A$$

$\vec{B}$ flux density

$\vec{\phi}$ magnetic flux

A area

N number of windings

Equation 3-1: Induced voltage according to Faraday's Law

If this relationship is applied to an inductively coupled RFID system the following vector diagram can be drawn:

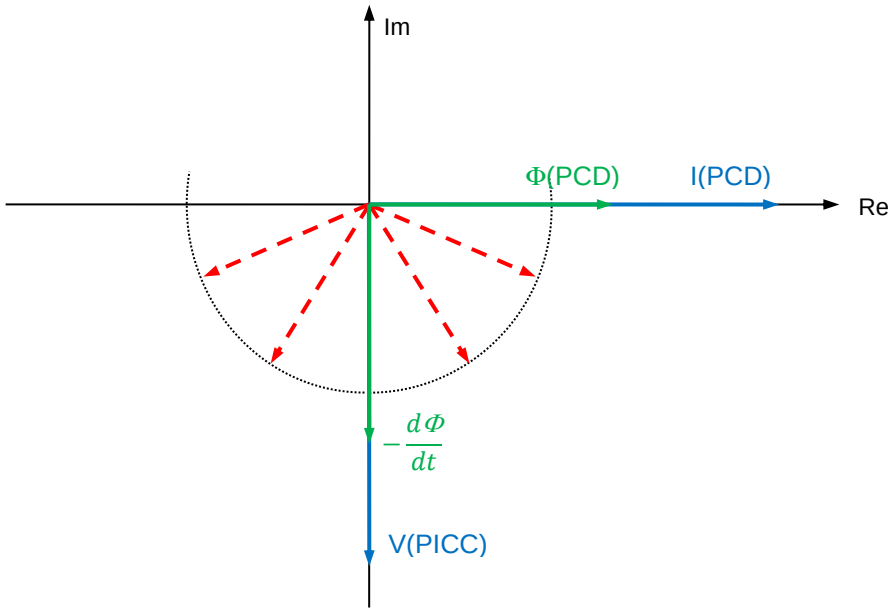


Figure 3-1: Vector diagram of PCD and PICC current relationship

As the magnetic flux Φ(PCD) produced by the PCD current I(PCD) is a sine function with a frequency of 13.56MHz, the induced voltage V(PICC) must be a negative cosine function according by Equation 3-1($\frac{d\Phi}{dt}$). This means that the induced voltage in the PICC's antenna will have a phase shift of -90°. Based on the PICC's IC impedance the phase of the current through the PICC's antenna may vary between ±90° relative to the PICC's voltage V(PICC). In other words, the phase difference between PCD and PICC antenna currents can vary between -180° and 0°. This can also be verified by a SPICE simulation as shown in Appendix A.

As the impedance of the PICC determines the phase shift between the PICC's field and the PCD's field, load modulation will not only cause a change in the amplitude of the field, but will also cause a change in the phase shift.

Because of this effect a constellation plot can be generated that shows the two stages of the PICC:

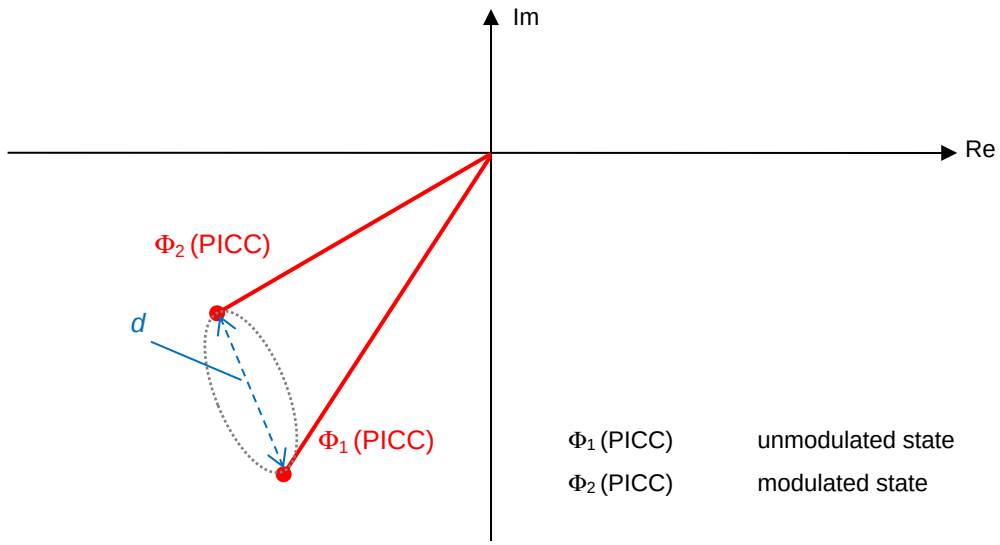


Figure 3-2: Constellation plot of PICC field

Figure 3-2 shows a constellation plot example with the two endpoints Φ_1(PICC) and Φ_2(PICC). The distance *d* essentially represents the load modulation amplitude that is evaluated in today's test methods. However the dynamic change between these two points, indicated by the ellipse, is ignored.

3.2 Analysis of PICC modulation

As mentioned in section 1.2 the main task of this thesis is to analyse the modulation of PICCs to identify the root cause for the observed communication problems. This analysis shall take use of constellation plots as shown in Figure 3-2.

In order to create such a plot, a suitable measurement setup and procedure needs to be developed.

An important consideration for this new test procedure is that no additional measurement equipment above today's requirements from the standards shall be necessary. This allows an easier implementation within companies and certification laboratories, if this test procedure should get adopted within ISO.

For the analysis two different PICC types shall be used, which have both shown interoperability on a certified PCD in the past (see 4 Initial Investigation). The results of these can be compared to functioning PICCs as well as the Reference PICC, which is defined within [ISO05].

3.3 Limits for new test parameters/methods

In addition to the analysis itself, test limits for this new method shall be defined that determine whether a PICC will show any communication problems on its RF interface.

Under the assumption that the root cause for the problem can be found within a constellation plot, the limits may be defined around the modulation endpoints Φ1(PICC) and Φ2(PICC) and regulate the dynamic change between them.

4 Initial Investigation

This section provides a summary of the initial investigation conducted in 2010 by engineers of HID Global and the PICC manufacturer, when communication problems between a certified PCD and certified PICCs where first observed. In addition an overview of the affected devices is provided.

4.1 Devices under test

4.1.1 PICCs – citizen ID sample cards

The PICCs that showed the communication problems were initial samples for the German electronic ID card project. The cards are based on the ISO/IEC14443 standard and are certified through a third party laboratory to meet the requirements of the standards and national technical reports [BSI2010].

Figure 4-1: German electronic ID card

Two different types of sample PICCs from different RFID IC manufacturers showed problems in the communication - details of which are withheld in this document for confidentiality reasons. In this document the PICC types are distinguished by a type number and a running sample number as shown in the table below:

Table 4-1: Overview PICC samples

Type	Sample Number	Reference	Comment
1	1	**T1S1**	PICC that showed communication problems. Only a single sample was available.
2	1	**T2S1**	PICC that showed communication problems.
	2	**T2S2**	
	3	**T2S3**	

4.1.2 PCD terminal

The PCD terminal had also been certified to meet the requirements of the ISO/IEC14443 standard plus additional requirements set by the BSI in Germany [BSI2010].

Figure 4-2: PCD terminal

For the RF interface of a PCD the core component is the RFID reader IC, which implements ISO/IEC14443 and other RFID standards, plus basic framing and error detection (parity and CRC). The typical tuning/matching circuit for such an IC is shown in Appendix B.

This particular terminal uses a very common reader IC that has a quadrature (or IQ) demodulator as its analog front end. The reason for using IQ demodulation is that for inductive coupling systems the phase of the PICC's load modulation can vary due to many parameters:

- Coupling (e.g. distance of the PICC; antenna design; …)
- Quality factor of PICC antenna
- Resonant frequencies of PCD/PICC
- Matching/Tuning circuit used by the PCD
- …

The quadrature demodulator ensures that the PICC load modulation signal is detected independently of the phase. At the same time this demodulation scheme has advantages in the achieved sensitivity of the receiver over other demodulators such as envelope detectors.

The following block diagram provides an overview of the IC's receiver architecture including some of the available debugging signals.

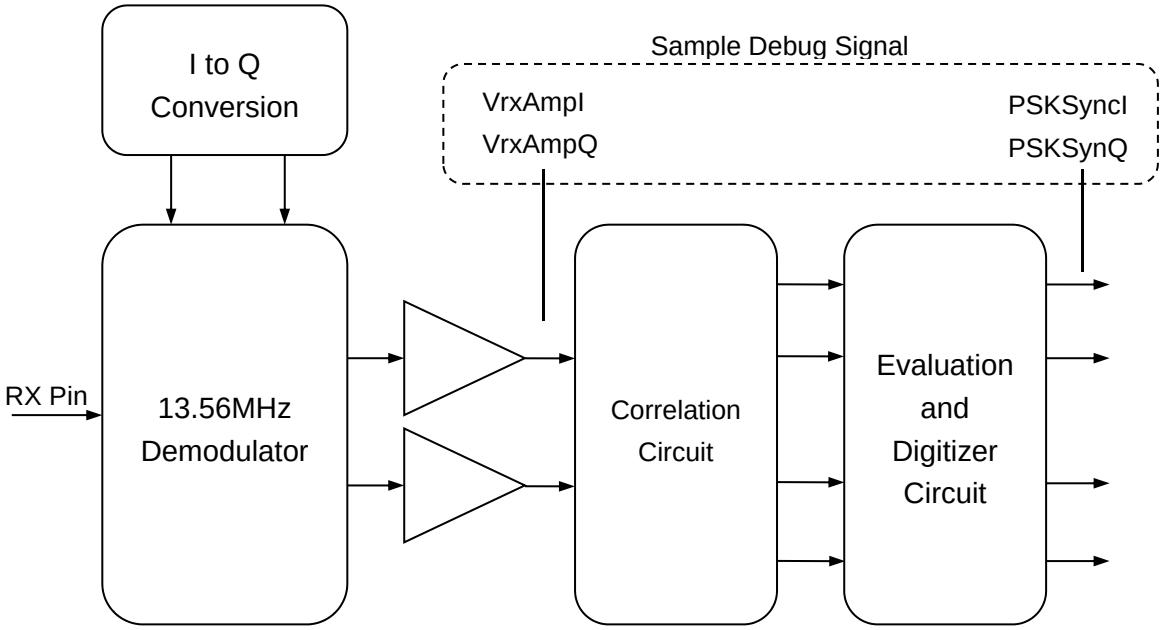


Figure 4-3: Block diagram reader IC quadrature demodulator

4.2 Initial results

The reading problems with type 1 and 2 PICCs were encountered with the PICCs placed directly on the surface of the PCD's housing (antennas concentric). This position results in strong coupling between the antennas. Positions with lower coupling did not show communication problems. By monitoring the magnetic field, using an oscilloscope and simple wire loop, it was discovered that the ID card answered the PCD commands even in the cases of communication failure. This indicated that something related to the load modulation of the card must be the cause of the PCD's receiver to fail.

Based on these findings, debug signals of the PCD's reader IC (see Figure 4-3) were used to further quantify the problem.

The following oscilloscope screenshot shows traces recorded during a successful read at higher distance and the error case directly on the PCD. The two sets are shown superimposed on one another (green = successful and red = error).

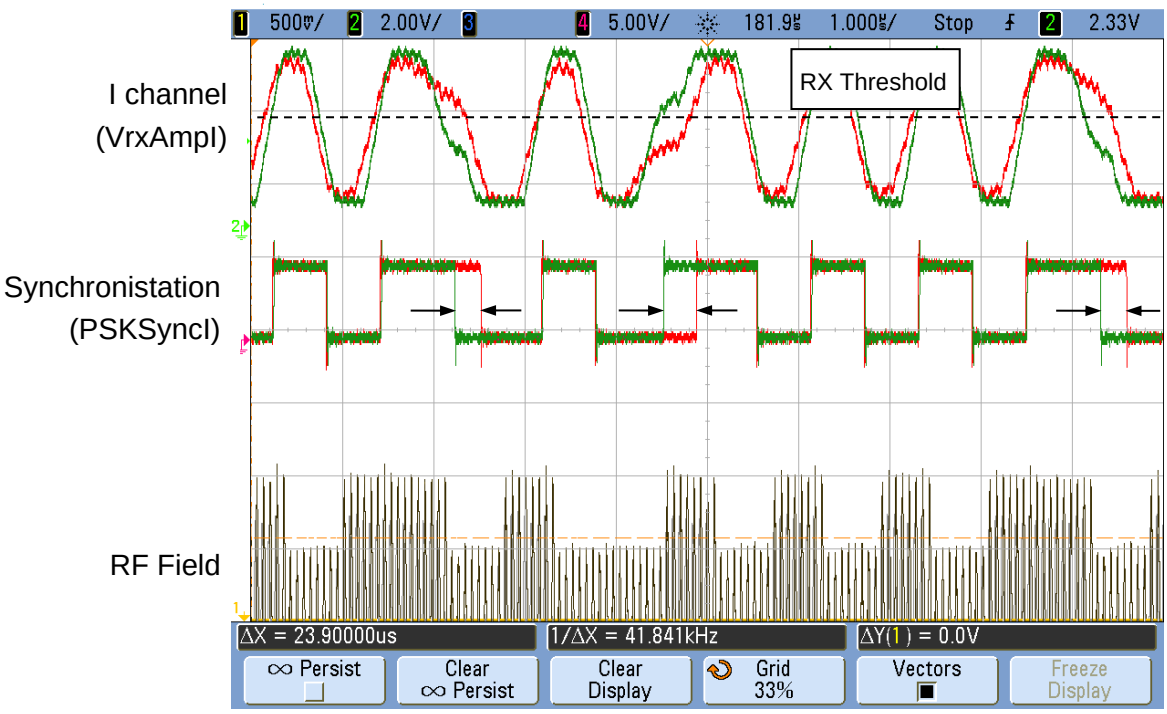


Figure 4-4: Comparison of successful read operation and error case

The VrxAmpI signal shows a distortion in the form of a bump and/or a dip. This bump is dependent on the coupling between the PCD and the PICC, which if too high causes the digitizer to produce a wrong synchronization signal, resulting in the receiver terminating prematurely, due to CRC or parity errors.

The HID Global engineers also confirmed that the distortion is not caused by the amplifier of the demodulator by remeasuring the internal signals with a lower amplification setting. This indicates that something related to the load modulation of this particular PICC causes the distortion, rather than any of the reader IC receiver stages. The observed error was the same for type 1 and type 2 citizen ID card samples.

4.3 Replication of initial results

The initial investigation was repeated by myself, but with different commands needing to be used. This is because the initial tests relied on temporary security certificates which were no longer available. The repeated tests relied on the error condition occurring with standard ISO/IEC14443 commands (e.g. anticollision sequence).

The problem was successfully replicated using standard ISO/IEC14443 commands. As the amount of data exchanged with such commands is much less than reading identification information, multiple tries were necessary to trigger the error condition. Nevertheless, this indicates that the underlying problem is not related to specific crypto-operations of the PICC.

In addition, various tests with other Reference PICCs (see Appendix C) were performed. During these tests, parameters such as load (shunt regulator emulation), load modulation amplitude and resonance frequency were varied but despite this, the error condition could not be replicated (no distortions on VrxAmpI/Q signal).

During the certification process of the PCD, which makes use of the Reference PICC specified in [ISO05], no problems were encountered either.

This indicates that the current equivalent circuit models of the PICC are not able to invoke the error conditions, which were shown by the Type1 and 2 PICCs and are unsuitable for this investigation.

5 Analysis Setup and Procedure

The following describes the setup and the procedure that was used to analyse the PICC modulation and create the intended constellation plots. The required signal processing was implemented in MATLAB®, which is a high level language and environment for numerical computing and has been used for ISO contributions in the past.

5.1 Analysis setup

To allow the generation of a constellation plot, both the phase and amplitude of a PICC's field need to be measured accurately. Measuring the current through a PICC antenna is not straight forward, as typically there is no access to the antenna itself.

In order to get a representative measurement without access to the PICC's antenna, a measurement coil can be placed around the antenna. The voltage induced in this measurement coil is proportional to the change in the magnetic flux (see Equation 3-1: Induced voltage according to Faraday's Law) which, in turn, is proportional to the current through the PICC's antenna as shown below.

$$\vec{B} = \mu \cdot \overrightarrow{H} = \mu \cdot N \cdot \frac{\vec{I}}{l}$$

$\vec{B}$ flux density

$\overrightarrow{H}.$ magnetic fieldstrength

μ magnetic permability

N number of windings

$\vec{I}$ current through inductor

l length of coil

Equation 5-1: Magnetic flux density created by a coil

As the current through the PICC's antenna is bound to be a sine wave with a frequency of 13.56MHz, the voltage measured on the measurement coil will have a phase of -90° compared to the current.

If the current through the PCD's antenna is measured by similar means, the phase of the signal on the second measurement coil is also -90° and due to this the individual phases in this measurement arrangement compensate for each other.

Such a measurement is unable to determine absolute values of current or field contribution, but in most cases a relative measure is sufficient.

Another problem is that a PICC is a passive device and needs to be powered by a PCD's magnetic field. For this reason simple measurement coils are not sufficient to measure the currents, as the induced voltage would comprise both the PCD's field and the PICC's field contributions. To overcome this problem, the Test PCD Assembly described in [ISO05], may be used. This apparatus consists of four coils in a Helmholtz arrangement with the PCD's antenna in the centre (actively driven antenna) and two 'sense coils' equally spaced on either side. Against one of these sense coils the calibration coil is placed.

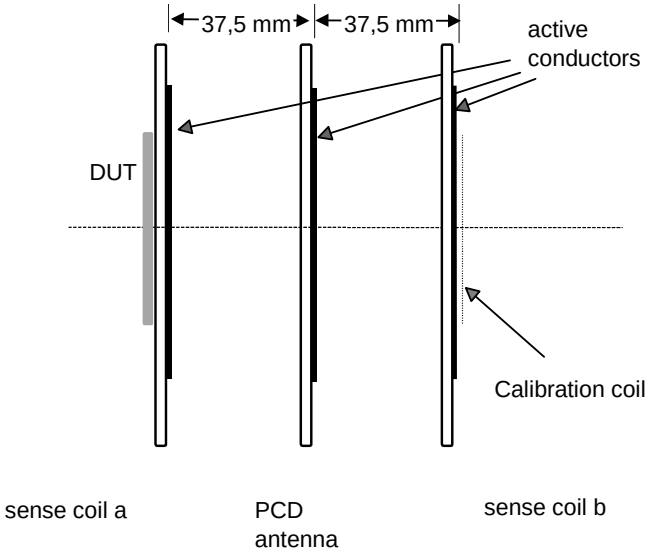


Figure 5-1: Test PCD assembly (source: [ISO05])

The voltage induced in the calibration coil is proportional to the PCD's magnetic field (or antenna current). The PICC under test is placed in the position marked DUT and as such is 75mm away from the calibration coil. Due to this the field contribution of the PICC measured by the calibration coil is negligible.

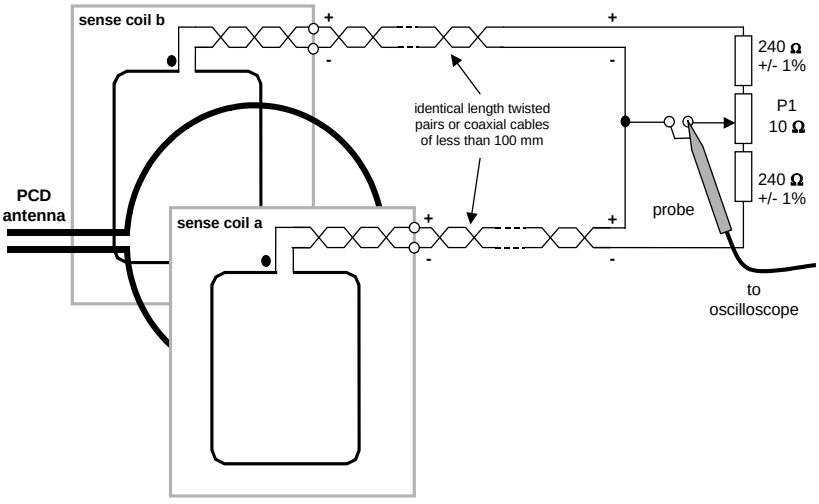


Figure 5-2: Test apparatus principle (source: [ISO05])

The two sense coils (sense coil a and b) are connected in opposite polarity to a central point (via the so called load modulation test circuit show in Figure 5-2). Because of this polarity arrangement, the voltage induced in each sense coil by the magnetic field of the PCD cancels the other at the connection point of the oscilloscope probe. Typically a PCD field rejection ratio of 30-40dB is achieved.

With the PICC under test being placed against one of the sense coils, the magnetic field contribution of the PICC is not compensated and can be measured at the central connection point.

Figure 5-3: Test PCD assembly with calibration coil

This Test PCD assembly allows simultaneous measurement of the sense coil voltage, which is representative of the current through the PICC's antenna and the voltage on the calibration coil, which is representative of the current through the PCD antenna.

The following oscilloscope screenshot shows such a measurement:

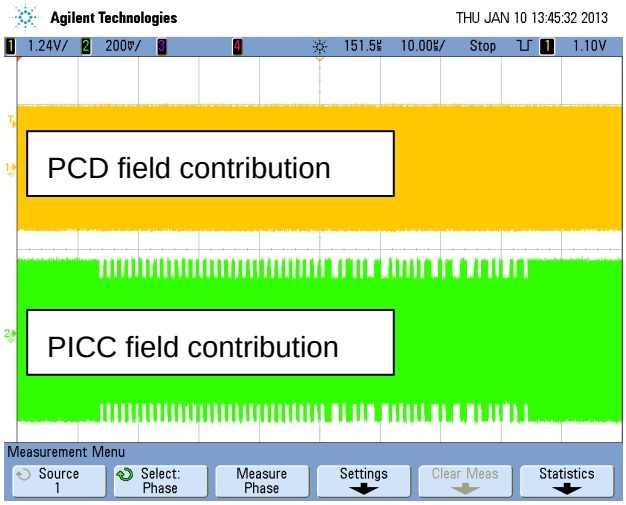


Figure 5-4: PCD and PICC field contribution

Today this setup is used to determine the spectral amplitude of the load modulation of a PICC. To ensure that it is also fit for purpose to determine the phase of the PICC's field, simulations were conducted.

To do this the inductances and the individual mutual inductances of the Test PCD Assembly were calculated. To achieve this, a finite element analysis based on the double integral Neumann formula was used:

$$L = \left(\frac{\mu_0}{4\pi}\int\int\frac{1}{|r_{ij}|}ds_i ds_j\right) + \frac{\mu_0}{4\pi}\cdot y$$

L inductance

μ_0 magnetic constant

r_{ij} distance between two points

y constant that depends on distribution of current in the wire

Equation 5-2: Neumann formula

The calculation of inductance by this method has proven to be very accurate (±5% accuracy) compared to other formulas, which only achieve accuracies in the 20% range. More details on the implementation of the Neumann Formula can be found in Appendix D.

With the results for mutual inductances a SPICE model for the setup could be established.

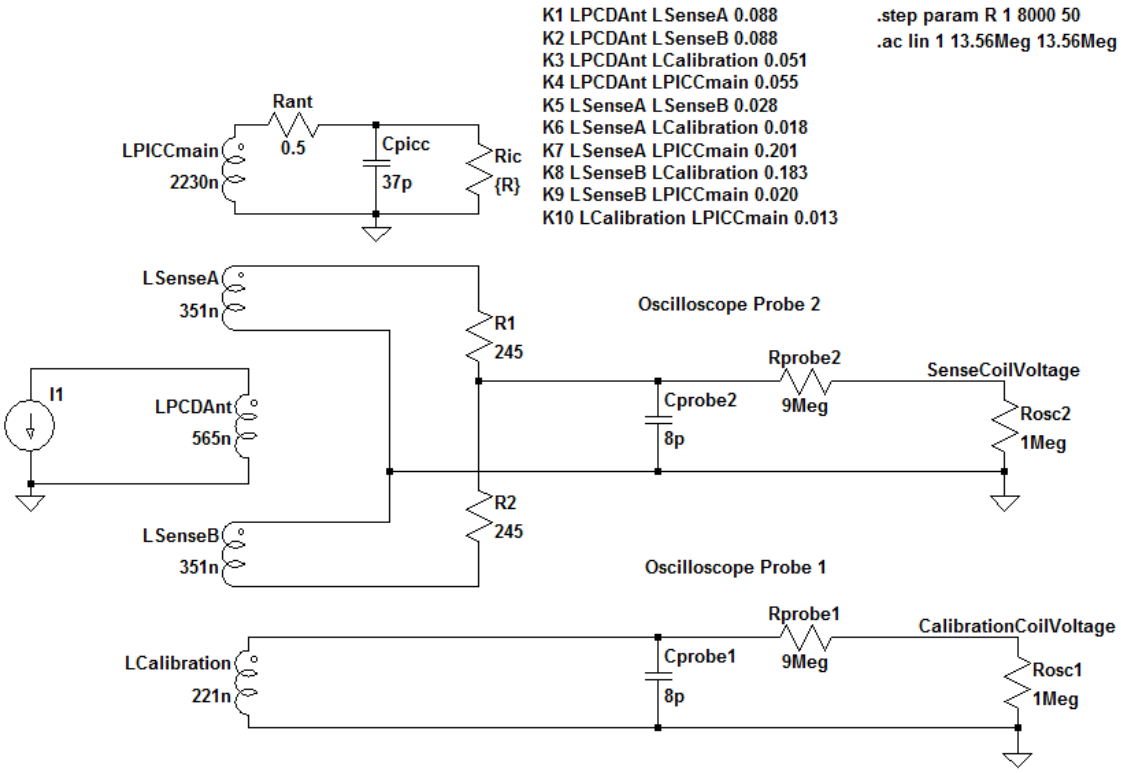


Figure 5-5: Spice model for Test PCD Assembly with PICC in DUT position

For the PICC a simplified model was used with the main coil of the Reference PICC as antenna (see Appendix C). The impedance of the oscilloscope probes at the calibration and the sense coils was also taken into account.

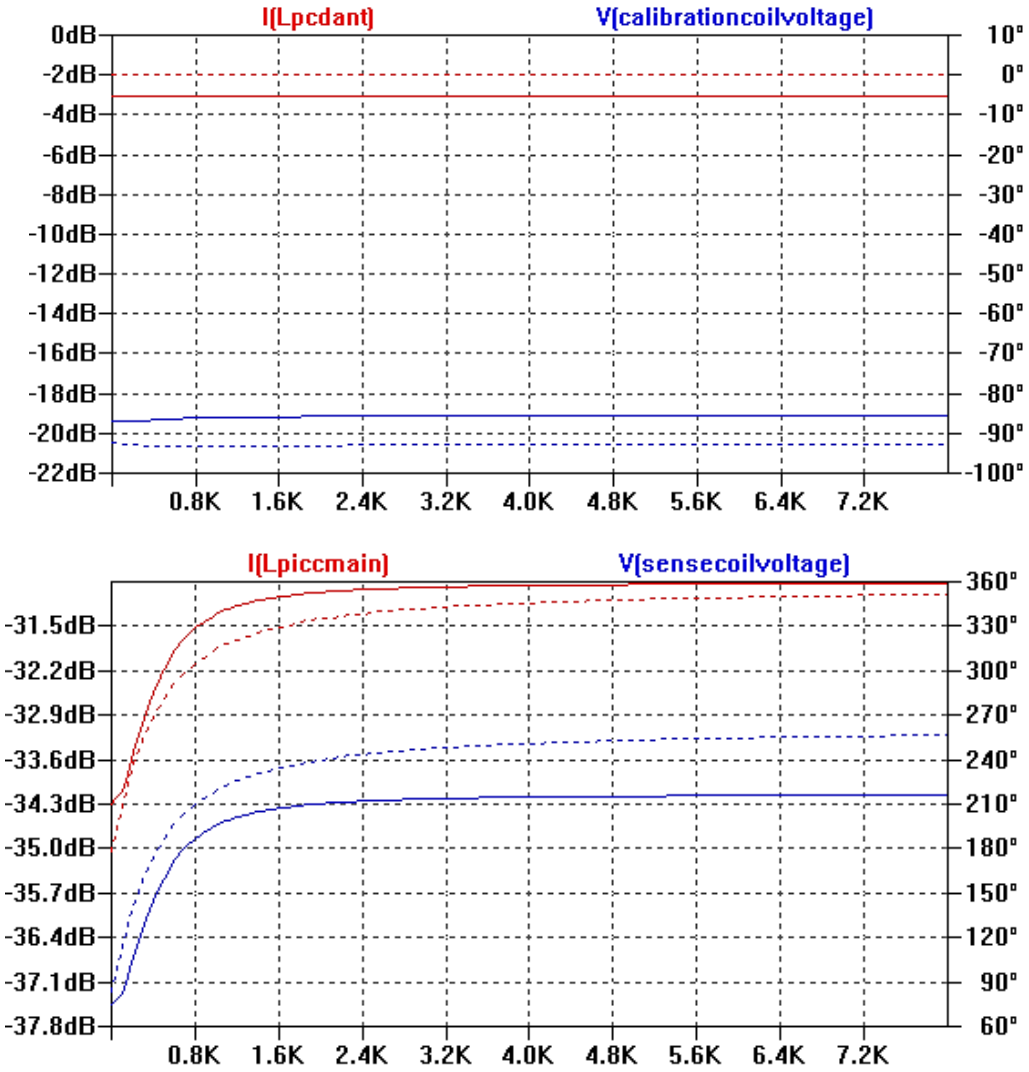


Figure 5-6: Test PCD Assembly simulation results

The results confirm that the calibration coil voltage is representative of the current through the PCD's antenna, whilst the sense coil voltage represents the current through the PICC's. As such these two voltages are also representative of the individual field contributions.

5.2 Analysis procedure

5.2.1 Constellation plot

To draw a constellation plot of the PICC field contribution two components of the field are required:

- The relative amplitude change of the PICC field contribution during load modulation (envelope).
- The phase shift between the PCD and PICC field contribution (or respectively the currents through their antennas).

To extract this information from the recorded data, the following signal analysis procedure was programmed in MATLAB®:

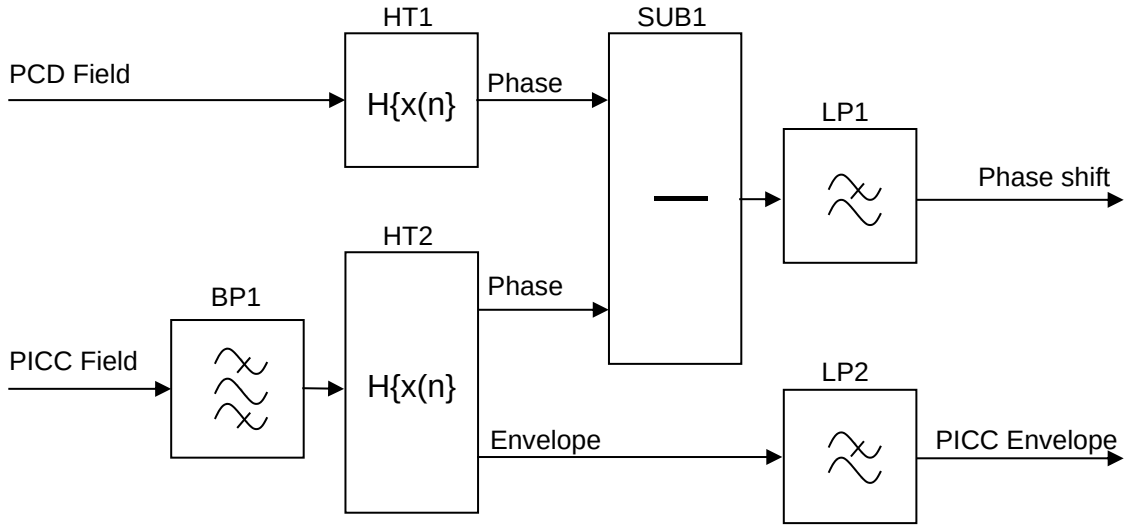


Figure 5-7: Signal analysis procedure for constellation plot

The Hilbert transform was used to calculate the envelope and the phase of the individual fields (HT1 and HT2). It is often used in the area of Fourier analysis and can be viewed as a filter that performs a phase shift of all frequency components. The Hilbert transform of a function f(x) is defined as follows:

$$H\{f(x)\} = \frac{1}{\pi} PV \int_{-\infty}^{\infty} \frac{f(x)dx}{x - y}$$

PV notation for Cauchy principal value

Equation 5-3: Hilbert transform

The transform can also be interpreted as a convolution.

$$H\{f(x)\} = \frac{1}{\pi x} * f(x)$$

Equation 5-4: Hilbert transform written as convolution

To extract the envelope and phase information from the measurement data, the Hilbert transform alone is not sufficient, and the so called discrete-time analytical signal is needed.

$$x_a(t) = x(t) + jH\{x(t)\}$$
$$x_a(t) \quad \text{analytical signal}$$
$$x(t) \quad \text{input signal}$$
$$H\{x(t)\} \quad \text{hilbert transform of input signal}$$

Equation 5-5: Discrete-time analytical signal

According to [Marple1999] the discrete-time analytical signal can be calculated with the following algorithm:

1) Calculate the FFT X(f) of the input signal
2) Create a second vector H(i) with the following elements
    a. 1 for i = 1,(n/2)+1
    b. 2 for i = 2,3,…,(n/2)
    c. 0 for i = (n/2) +2,…,n
3) Calculate the element wise product of H(i) and X(f)
4) Calculate the inverse FFT of the result from step 3 (first n elements are the result)

This algorithm is also used by MATLAB's command "hilbert()".

From the discrete-time analytical signal, the envelope and phase of the original signal x(t) can be calculated (also performed by HT1 and HT2).

$$A(t) = \sqrt{x(t)^2 + H\{x(t)\}^2}$$
$$\varphi(t) = \arg\{x(t), H\{x(t)\}\}$$
$$A(t) \quad \text{envelope}$$
$$\varphi(t) \quad \text{phase}$$

Equation 5-6: Calculation of envelope and phase from discrete-time analytical signal

For the constellation plot the phase shift $\Delta\varphi$ between PCD and PICC field is needed. For this, the phase of the PCD is subtracted from the PICC phase (SUB1).

$$\Delta\varphi(t) = \varphi_{PICC}(t) - \varphi_{PCD}(t)$$
$$\varphi_{PCD}(t) \quad \text{PCD phase}$$
$$\varphi_{PICC}(t) \quad \text{PICC phase}$$

Equation 5-7: Phase shift between PCD and PICC field contribution

The bandpass filter BP1 was introduced to remove any noise that would not be captured by a standard PCD antenna. In practice the SRF of a PCD antenna may very between different designs. Typically it will remain between 13.12MHz and 14MHz. The quality factor of the antenna needs to be between 18 and 34 to achieve the required modulation waveform (for more details on the quality factor range refer to Appendix E)

With this data at hand, the passband for a filter can be calculated that considers all frequencies that may be relevant to a PCD.

$$B = \frac{SRF}{Q} \qquad f_U = SRF + \frac{B}{2} \qquad f_L = SRF - \frac{B}{2}$$
$$B \quad \text{3dB Bandwidth}$$
$$f_U \quad \text{upper cut - off frequency}$$
$$f_L \quad \text{lower cut - off frequency}$$
$$SRF \quad \text{Self resonance frequency of PCD Antenna}$$

Equation 5-8: Bandwidth and cut-off frequency calculation

Table 5-1: Upper and lower cut-off frequencies of PCD antennas

SRF [MHz]	B [kHz]	fL [MHz]	fU [MHz]
13.12	729	12.391	13.849
14.00	778	13.222	14.778

This suggests that PCD antennas may pick up signal between 12.391MHz and 14.778MHz depending on the resonant frequency and quality factor.

The standards already describe a test concerning electromagnetic disturbance produced by a PICC (for more details refer to EMD tests defined in [ISO02]). This test focuses on the signal levels in the upper and lower sidebands. The defined filters for this test have a bandwidth of 1MHz with the centre frequency being either the upper or the lower sideband frequency.

Table 5-2: Upper and lower cut-off frequencies of EMD test filters according to [ISO02]

Sideband Frequency [MHz]	B [kHz]	fL [MHz]	fU [MHz]
12.7125 (LSB)	1000	12.2125	13.2125
14.4075 (USB)		13.9075	14.9075

The maximum and minimum frequency in the EMD test is very close to the calculated edge frequencies for PCD antennas. As the EMD test is supposed to look at any frequencies that may be interpreted by a PCD, this makes the limits also applicable for this investigation. The only difference is that for the EMD test the carrier frequency needs to be filtered whilst for the analysis of the PICC modulation it needs to be present.

Based on this the filter for the PICC field contribution is designed with a passband from 12.2125MHz to 14.9075MHz.

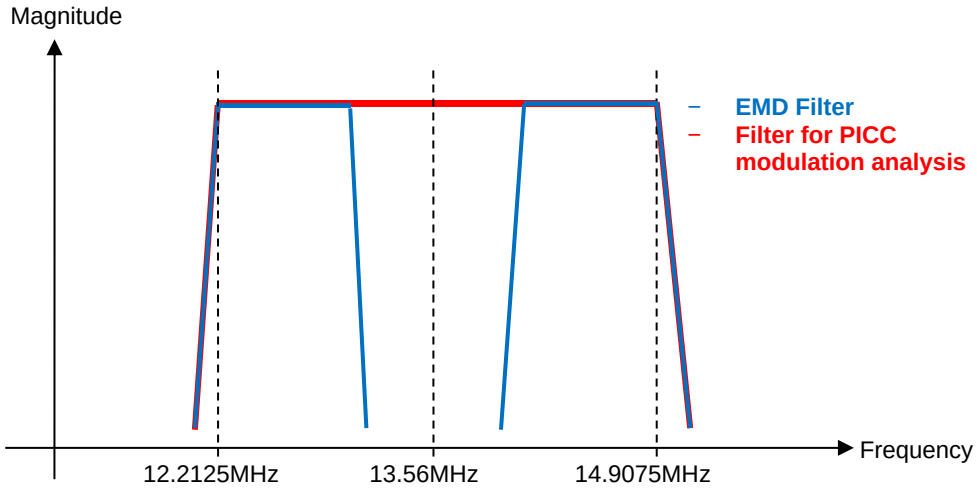


Figure 5-8: Comparison EMD filter vs. filter for PICC modulation analysis

To reject the carrier frequency as well as possible the filters for the EMD test have a very high roll-off and order. In the case of a real PCD antenna the filter characteristics are not as strict. A second order elliptic filter was designed that has a very low ripple (0.2dB) in the passband and a roll-off comparable to that of a PCD antenna.

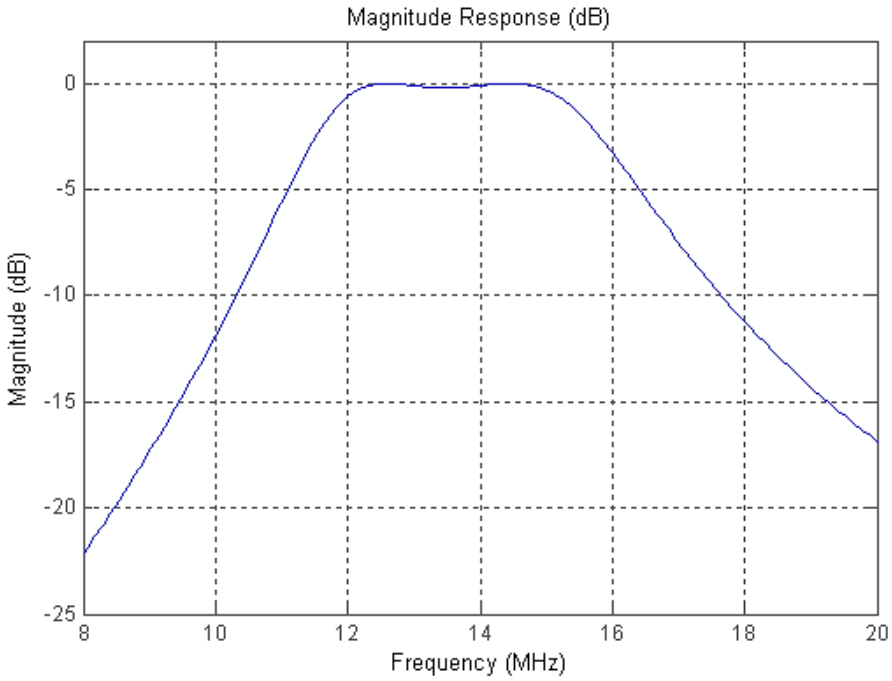


Figure 5-9: Magnitude response of bandpass filter BP1

The problem with elliptic filters is the high variation in the group delay. As the phase component of the PICC's field is essential, zero phase filtering is required to avoid any distortions introduced by the filter. This means that the data is filtered twice, once in the forward and once in the reverse direction. Due to this the phase distortions of the filter are compensated. However, the effective transfer function of the filter is the square of the transfer function of the base filter (effective order is doubled). This was already considered in Figure 5-9.

The two lowpass filters LP1 and LP2 were implemented as first order Butterworth filters with a cut-off frequency of 2.5GHz. The cut-off frequency was derived from the internal filter of the RFID reader IC in the PCD terminal described in section 4.1.2. Again zero-phase filtering was applied.

5.2.2 Simulation of PCD receiver

To be able to reproduce the error condition as shown in Figure 4-4, in parallel to the signal processing described in the previous section, a model for the PCD‘s IQ demodulator was implemented.

In general quadrature modulation is a technique which uses the carrier two times with a 90° phase shift. On each of the carriers a baseband signal can be modulated. Afterwards the signals are added together. The two components are referred to as I for the in-phase and Q for the quadrature component. For this reason this modulation scheme is also called IQ modulation.

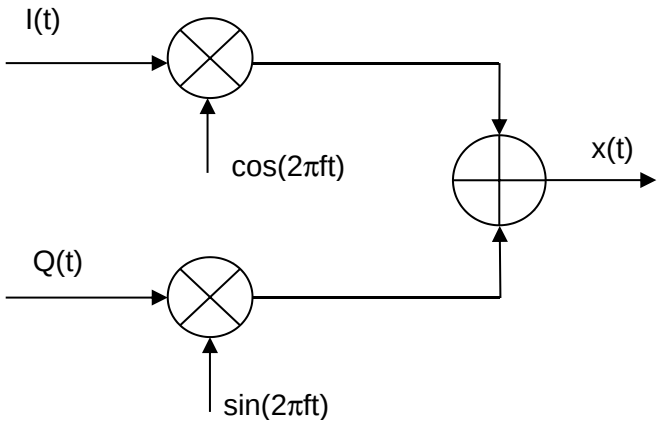


Figure 5-10: IQ Modulation principle

The demodulator needs to have both same frequency and phase as the modulator to ensure functionality. The mechanism is the converse of the modulator.

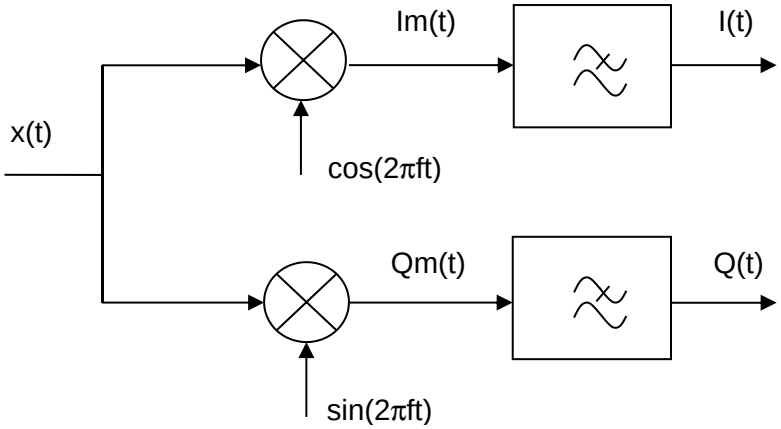


Figure 5-11: IQ demodulation principle

Due to the multiplication of x(t) with cos(2πft) or sin(2πft) the signals Im(t) and Qm(t) not only consist of the representative baseband signals. In addition there are frequency conversion products of two times the carrier frequency. These are filtered with a low pass filter leading to the baseband signal.

In case of the RF interface IC used by the PCD terminal, quadrature demodulation is used because the phase of the PICC reply can vary as shown in section 3.1. If the PCD were to use a simple mixer, load modulation signals with a phase shift of 90° could not be decoded. The quadrature demodulation architecture ensures that regardless of the phase shift at least one of the two channels (I or Q) should carry the load modulation information.

To simulate the demodulation of the recorded measurement data, the PICC field contribution (sense coil voltage) was multiplied with the sine and cosine of the angular carrier frequency.

$$I_m(t) = V_{sense}(t) \cdot \cos(2\pi \cdot 13.56 \cdot 10^6 \cdot t + \varphi_{PCD}(0) + \varphi_{rec})$$
$$Q_m(t) = V_{sense}(t) \cdot \sin(2\pi \cdot 13.56 \cdot 10^6 \cdot t + \varphi_{PCD}(0) + \varphi_{rec})$$
$V_{sense}(t)$ Sense coil volatge
$\varphi_{PCD}(0)$ PCD phase at t = 0

Figure 5-12: IQ demodulation of PICC field contribution

In the case that the demodulation frequency has the same phase as the PCD field, the resulting I and Q channel would be very similar to the amplitude and the phase of the PICC field. However, in a real PCD terminal there is an additional phase shift φ_{rec} introduced by the receiver network. For the PCD terminal from section 4.1.2 this was measured as about 80°.

With this IQ demodulation added, the complete signal processing procedure looks as follows:

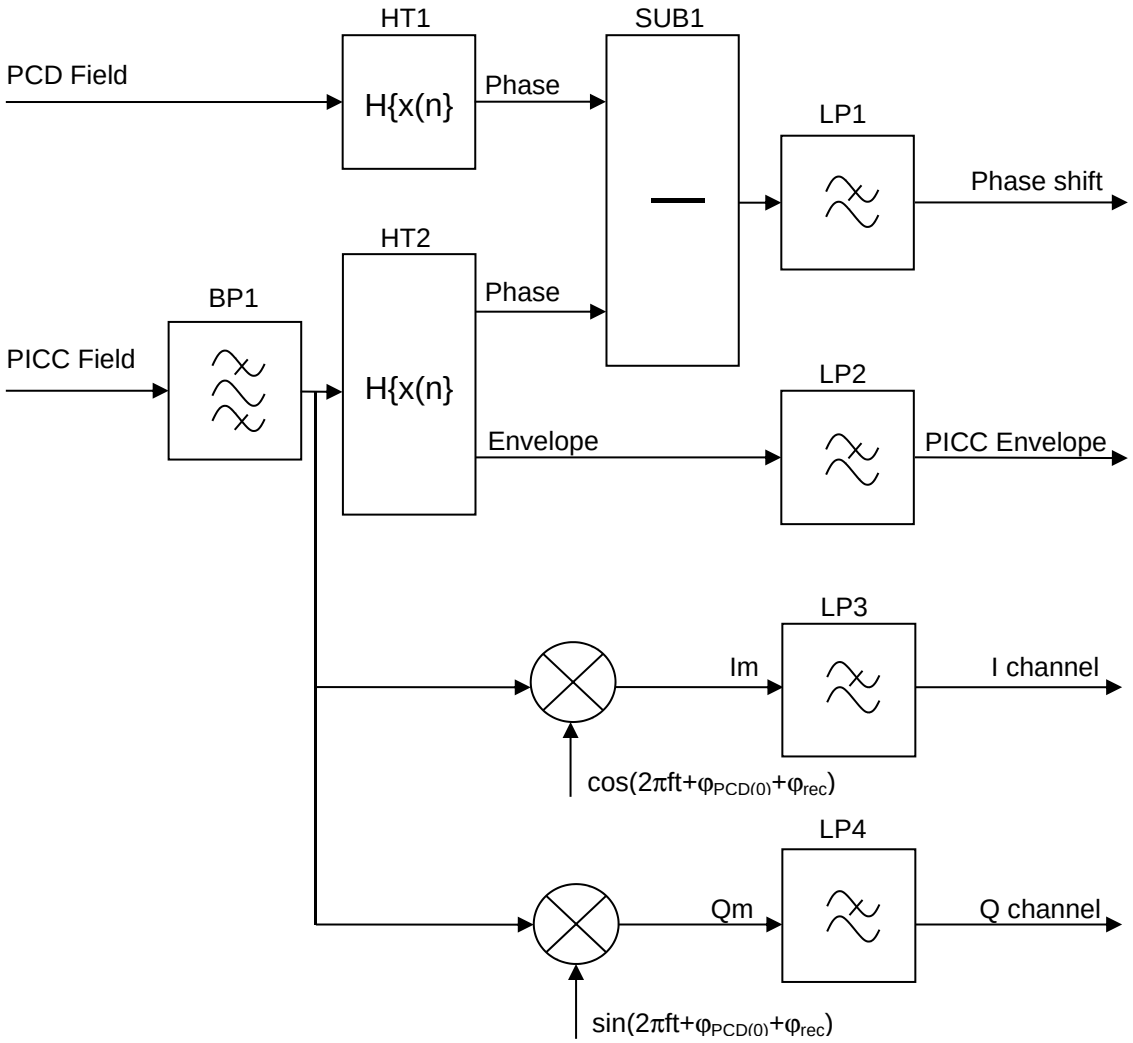


Figure 5-13: Signal analysis procedure including IQ demodulator

For the filter LP3 and LP4 the same Butterworth lowpass characteristics were used as for LP1 and LP2 before.

6 PICC Analysis Results

This chapter documents the results of the measurements performed on various PICCs including the Reference PICC (described in [ISO05]), working PICCs and citizen ID card samples, which show the communication problem. The measurements were performed according to the analysis procedure described in section 5.

In addition a conclusion is drawn on the root cause of the communication problems observed with the type 1 and type 2 samples.

6.1 Overview

Each tested PICC was analysed at multiple field strength points within the standard defined range from 1.5A/m to 7.5A/m. Special attention was paid to the higher 5A/m range, as the PCD terminal on which the problems were observed produces a field strength of about 5-5.5A/m at the critical positions on its surface.

The measurements were conducted with an Agilent MSO6104A oscilloscope at a sampling rate of 2GSa/s for each channel. The probes that were used with the oscilloscope have in input capacitance of 8pF and meet the requirements for any measurement defined within the test standards [ISO05] to [ISO07].

The Test PCD Assembly antenna was driven from an Agilent 33521A arbitrary waveform generator via a 10Watts amplifier from Amplifier Research to generate the required modulation and trigger a PICC response.

6.2 Results for Reference PICC and working PICC samples

To create a baseline dataset, the Reference PICC of [ISO05] together with unproblematic PICC samples were analysed first.

The Reference PICC was tuned to a resonance frequency of 16.5MHz, which is considered an average value for ISO/IEC14443 PICCs. For each field strength the load resistor (emulation of shunt regulator) was set to give a VDC of 3V (for more details see Appendix C).

The following figure shows the constellation plot for the Reference PICC at 5.5A/m with the two modulation points Φ_1(PICC) and Φ_2(PICC). Instead of an angular diagram the envelope of the PICC field contribution was simply plotted against the phase shift, which leads to a similar result.

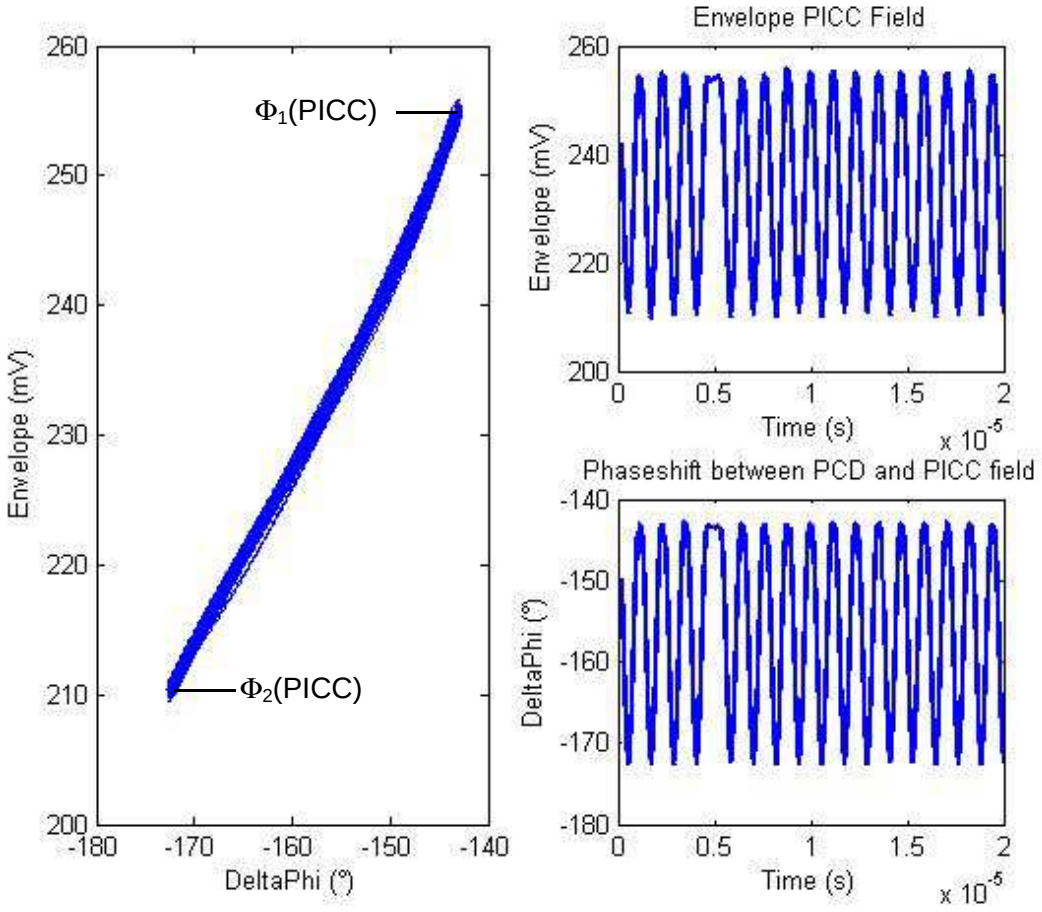


Figure 6-1: Reference PICC constellation plot at 5.5A/m

On the right hand side of Figure 6-2, parts of the envelope and phase shift of the PICC field contribution are shown. As suggested, the load modulation not only changes the amplitude of the field, but also leads to phase jumps at the subcarrier frequency.

The dynamic change between the two endpoints of the constellation plot at such a high field strength results in an almost straight line. At lower field strengths the dynamic change in the constellation plot for the reference PICC differs as shown below.

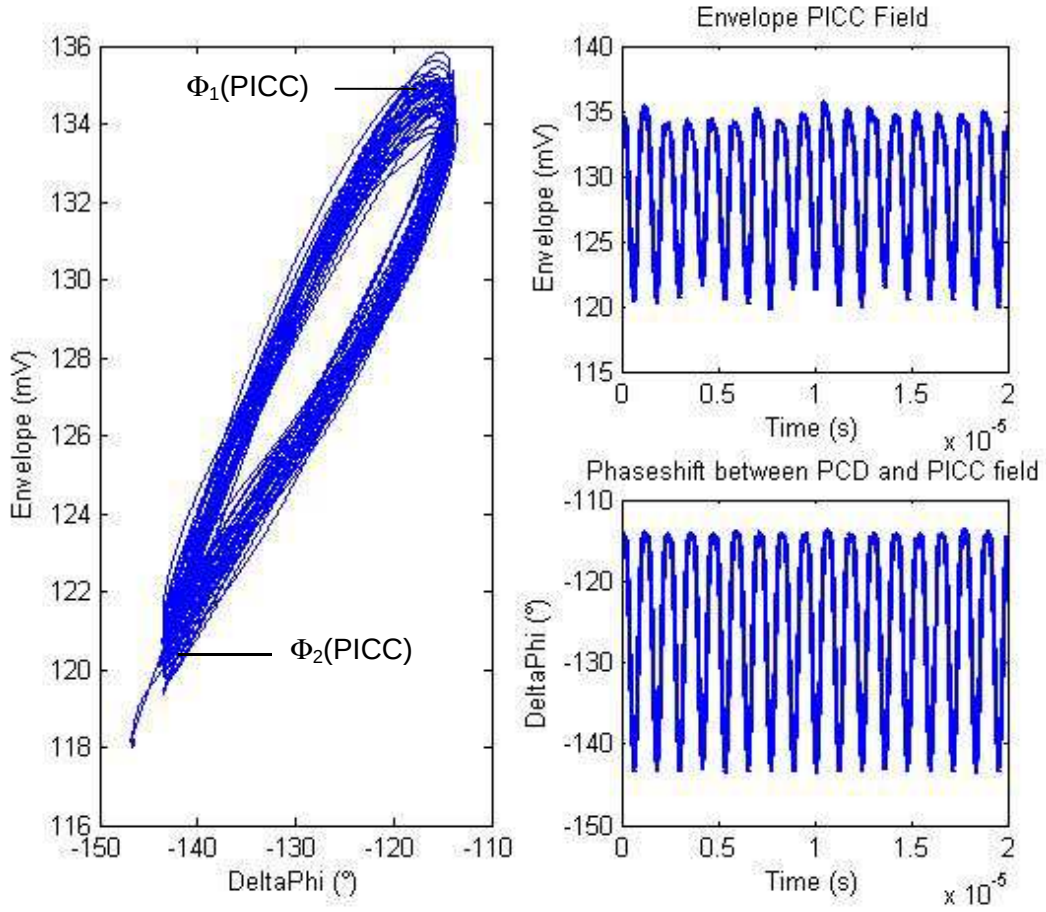


Figure 6-2: Reference PICC constellation plot at 1.5A/m

At 1.5A/m the dynamic change between the endpoints of the constellation plot appears as an ellipse. The reason for this is the higher quality factor of the Reference PICC at low field strengths, due to the higher load resistance of the shunt regulator (see Appendix C).

The start of the load modulation results in a rapid change of energy. Naturally, the antenna circuit of the Reference PICC tries to oscillate at its resonance frequency of 16.5MHz. Because of the higher quality factor, this leads to small overshoots in the envelope of the PICC field contribution, which in turn lead to a widening of the dynamic change.

Note that the load modulation itself is also slightly misshapen at 1.5A/m. This again is due to the high Q factor and the change applied to it during load modulation. However, the general shape is not contributing to the widening of the dynamic change as long as it is the same for envelope and phase shift.

The following figure shows the constellation plots for the Reference PICC at multiple field strength points.

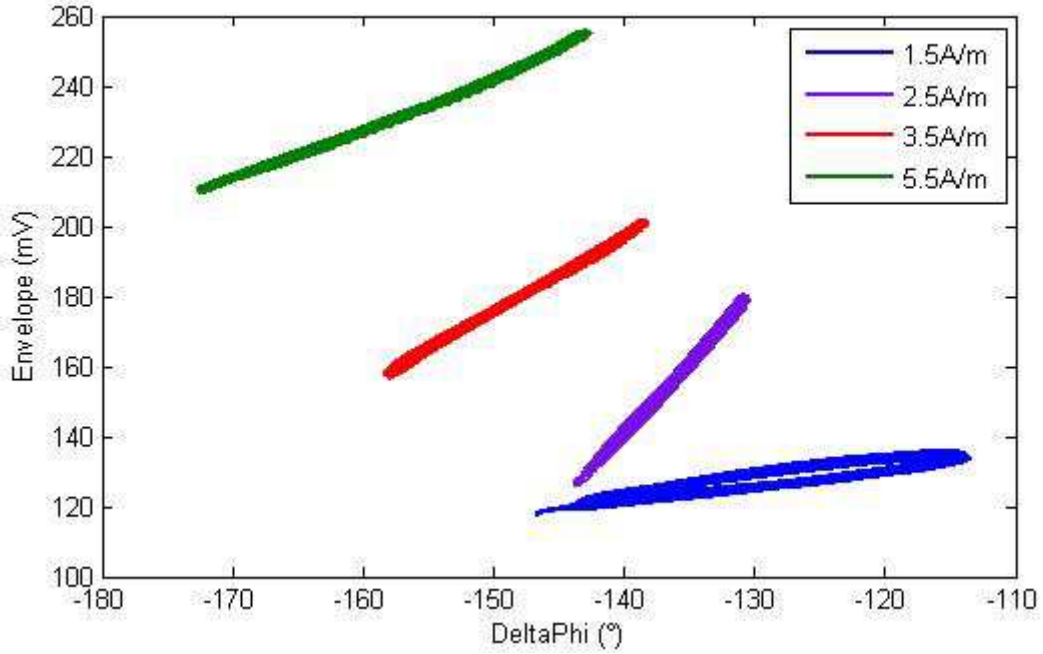


Figure 6-3: Reference PICC constellation plots at various field strengths

The plot shows that already at 2.5A/m the dynamic change becomes almost a line. So the Reference PICC only causes a minimal overshoot during load modulation at the minimum field strength defined by the standard. The distance of the two modulation endpoints depends on the setting for the load modulation resistor. For this particular test it was simply varied to provide a reasonable size of the constellation plot.

Another thing that can be observed is the shift of the initial phase from -113° at 1.5A/m to -148° at 5.5A/m. This change is also caused by the change of quality factor due to the voltage (shunt) regulator of the PICC.

Real PICC samples that were tested exhibit the same behaviour. For all successfully reading PICCs the constellation plot showed two defined modulation endpoints Φ1(PICC) and Φ2(PICC). The dynamic change between those endpoints appears as only a narrow ellipse or almost a line. A wider dynamic change could only be observed at very low field strengths, where the PICCs have a significant high quality factor. For some samples this was below the ISO defined range of 1.5-7.5A/m.

The following shows a constellation plot for an NXP SmartMX PICC sample at 5.5A/m.

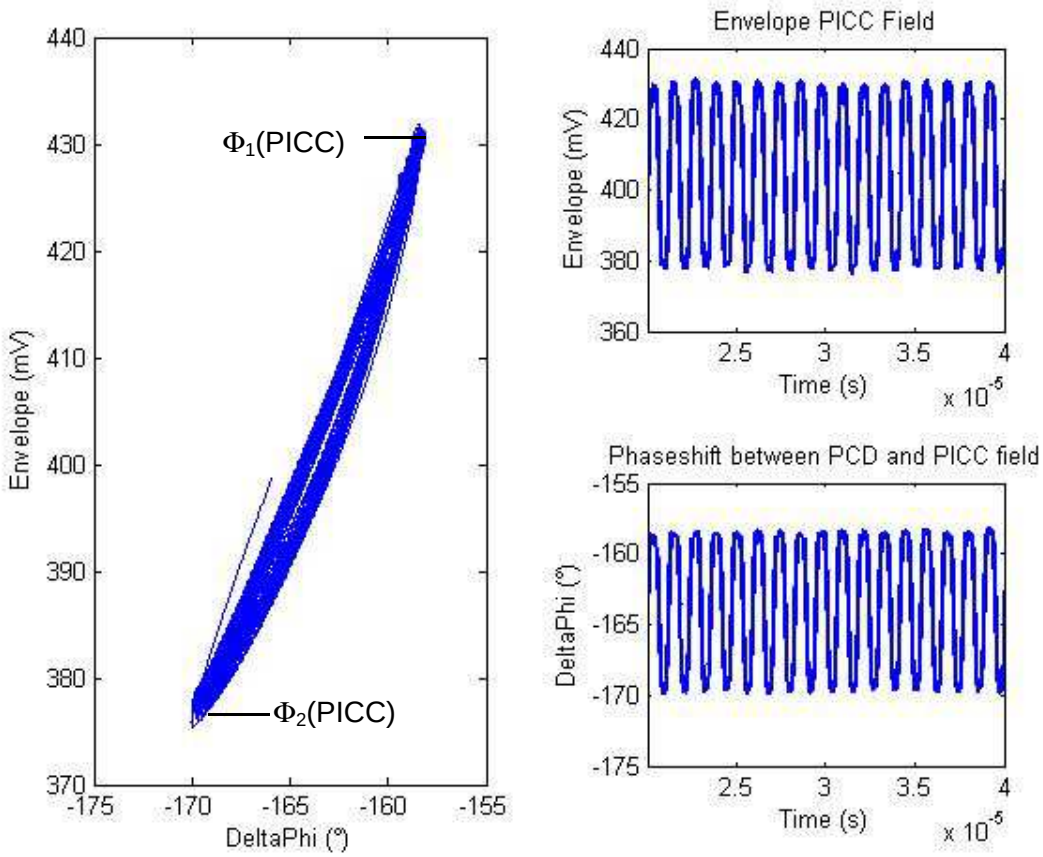


Figure 6-4: NXP SmartMX PICC at 5.5A/m

6.3 Results for Citizen ID card samples type 1

Citizen ID sample cards of Type1 have shown the communication issue described in chapter 4. Unfortunately only a single sample PICC was available for investigation referred to as T1S1.

During the analysis this card showed a very high load modulation amplitude, but also significant overshoot that was clearly visible in the oscilloscope plot. These overshoots persisted even at higher field strengths.

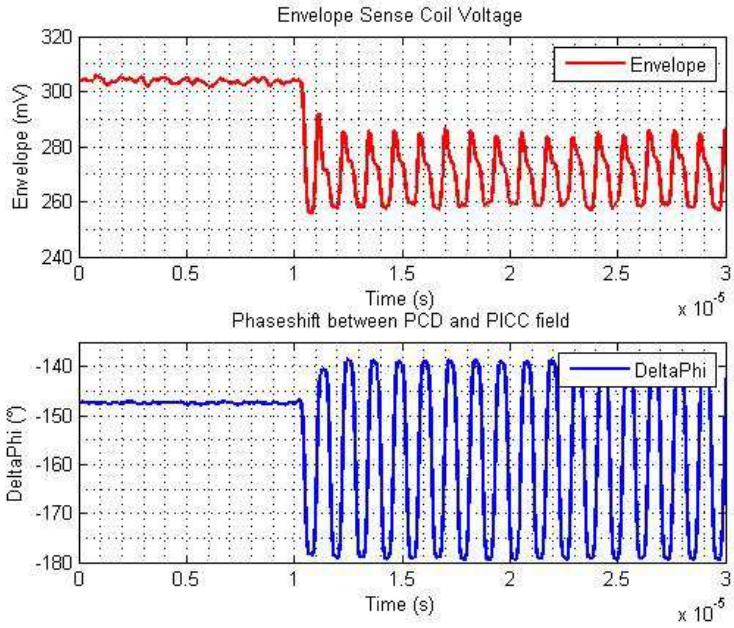


Figure 6-5: T1S1 envelope and phase shift at 3.5A/m

Another difference in this PICC is that it does not reach its initial point of operation again during load modulation as shown in Figure 6-5. This indicates a very high quality factor of the antenna which again conveys overshoots in the modulation.

Even at 5.5A/m the overshoots are large enough to cause a significantly wide dynamic change in the constellation plot as shown in Figure 6-6. This is roughly the field strength at the point of the PCD terminal on which errors were observed.

Also the additional operation point of the PICC can be seen in the constellation plot marked as “OP”.

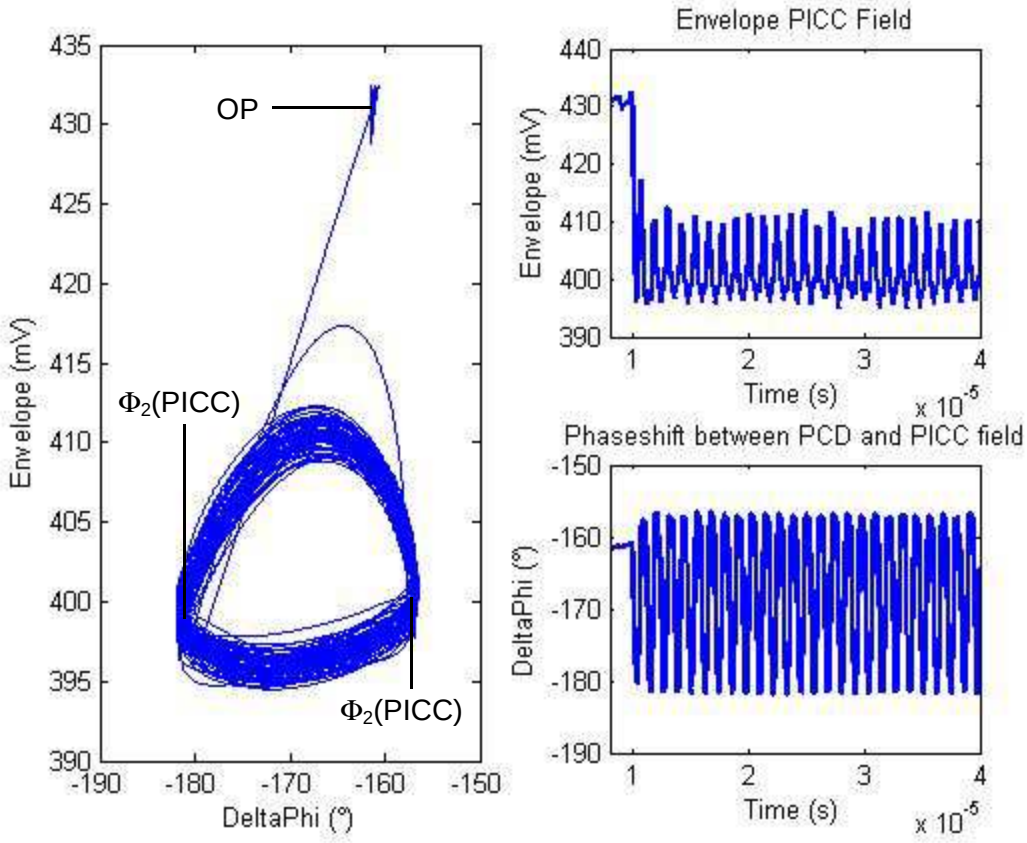


Figure 6-6: T1S1 constellation plot at 5.5A/m

At the IQ demodulation the significant overshoots lead to the same distortions as recorded on the debug pins of the RFID reader IC (see Figure 4-4).

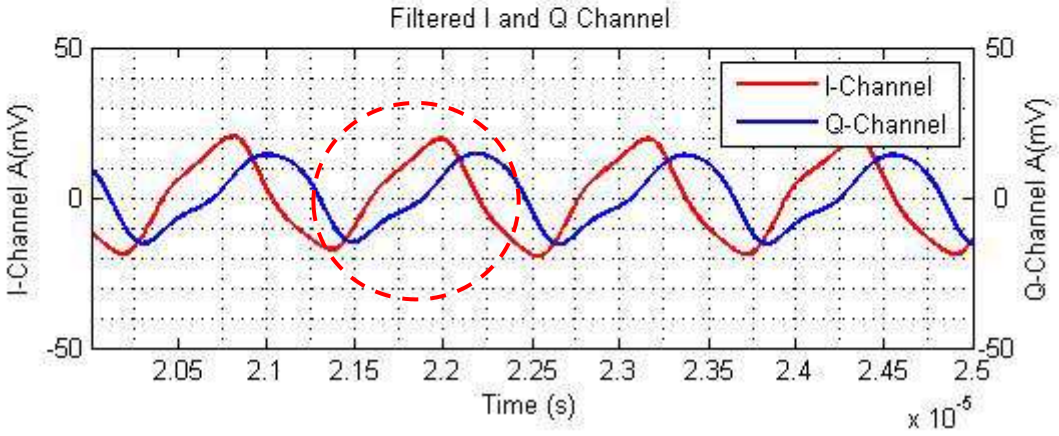


Figure 6-7: T1S1 IQ demodulation at 5.5A/m

6.4 Results for citizen ID card samples type 2

For Type2 PICC samples other effects were observed. Most noticeable was that the phase-jumps during load modulation were not constant, but showed jitter as illustrated in the figure below.

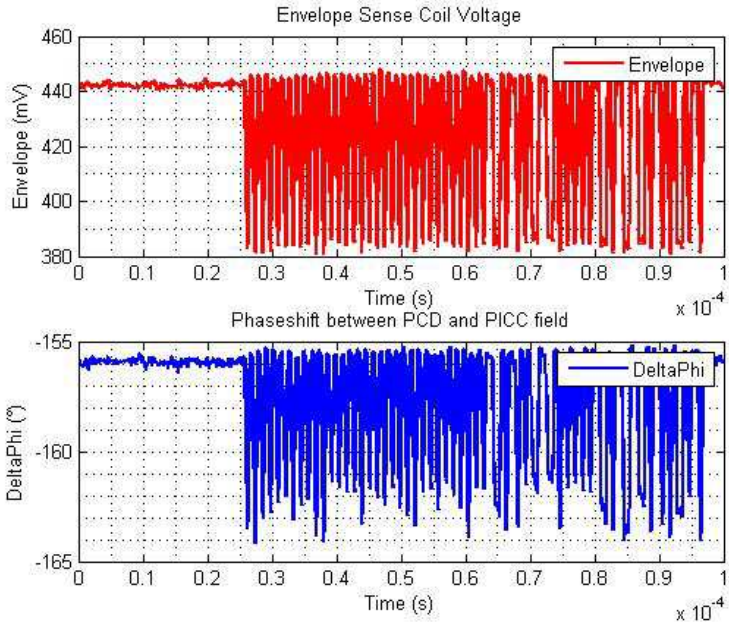


Figure 6-8: T2S1 envelope and phase shift at 5.5A/m

This jitter seems to increase with the field strength the PICC is exposed to. Up to 3.5A/m it is hardly noticeable.

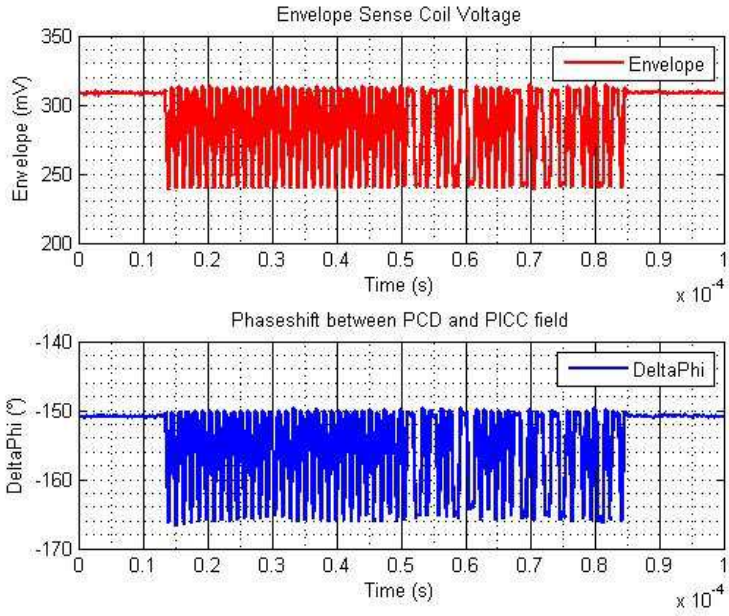


Figure 6-9: T2S1 envelope and phase shift at 3.5A/m

This indicates a problem with the design of the PICC RF interface. One of the most difficult tasks in PICC semiconductor design is to create the RF front end. This needs to be able to work with the high variation of voltages induced over the defined field strength range. Additionally such projects tend to have strict size and cost constraints. The main issues are parasitic structures in the rectifier and load modulation circuit acting as NPN or PNP transistors. At higher voltages the effects of these structures can become significant and lead to behaviors such as the observed phase jitter. However, as the design of Type2 PICCs is not available for review, the detailed root cause can not be determined.

In the constellation plot the observed phase jitter leads to a non-constant Φ2(PICC) endpoint.

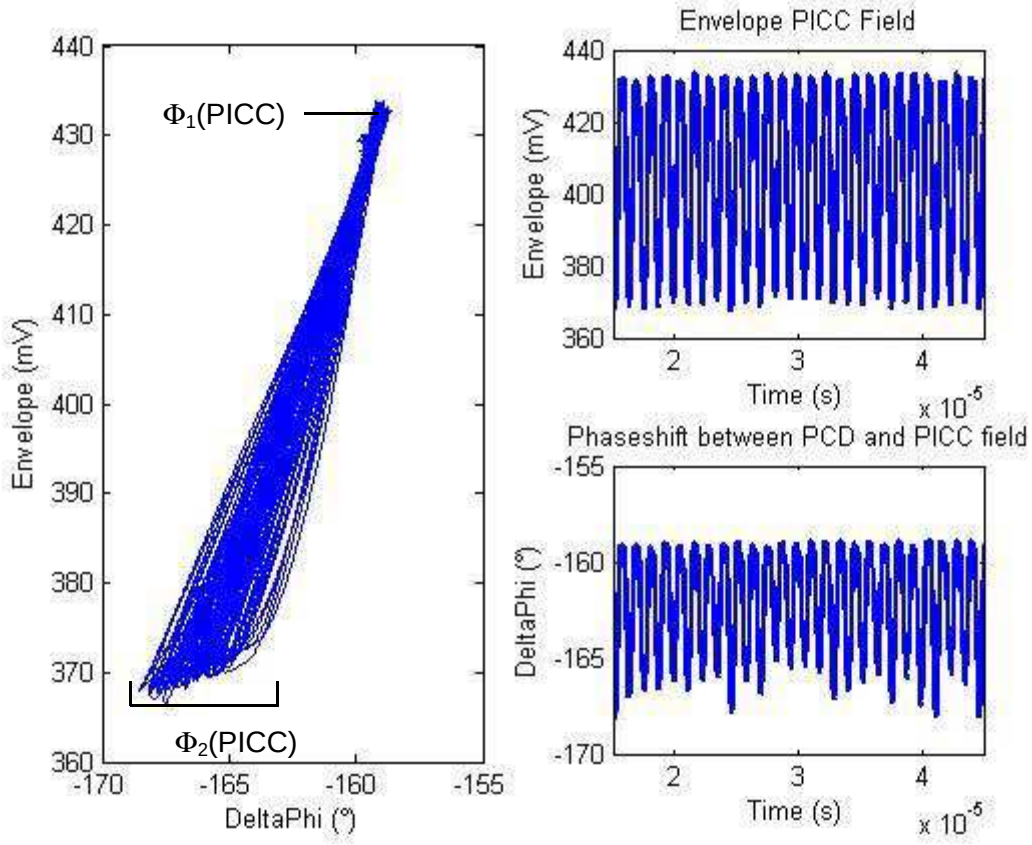


Figure 6-10: T2S1 constellation plot at 5.5A/m

All three samples of this PICC type exhibited the same behaviour.

The observed phase jitter does not lead to distortions of the kind shown in Figure 4-4, but to a variation of the I- and Q-channel signal strength distribution. This may lead to demodulation issues, if the RFID reader IC were to lock onto the channel with the initially stronger signal, instead of dynamically selecting the better signal throughout the reply.

However, another effect was observed with the Type2 PICC. This is a slower edge of the phase compared to the envelope jumps. This may be related to the phase jitter. As a result of this behaviour, the I- and/or Q-channel again suffers from distortions that can cause false decoding.

Figure 6-11 illustrates such a case and includes the envelope and the phase curve responsible.

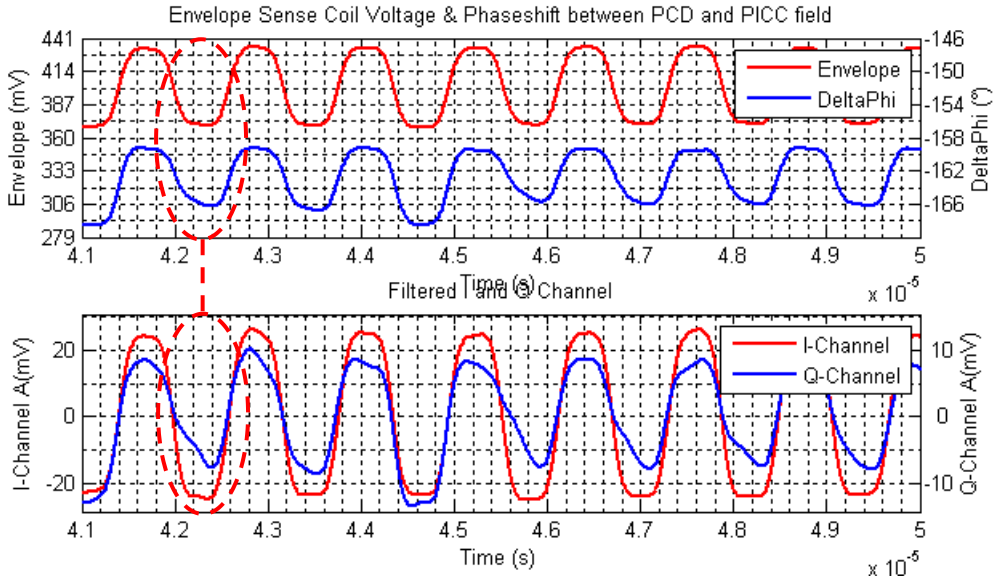


Figure 6-11: T2S1 IQ demodulation at 5.5A/m

During the distorted subcarrier cycle the constellation plot again shows a wider dynamic change.

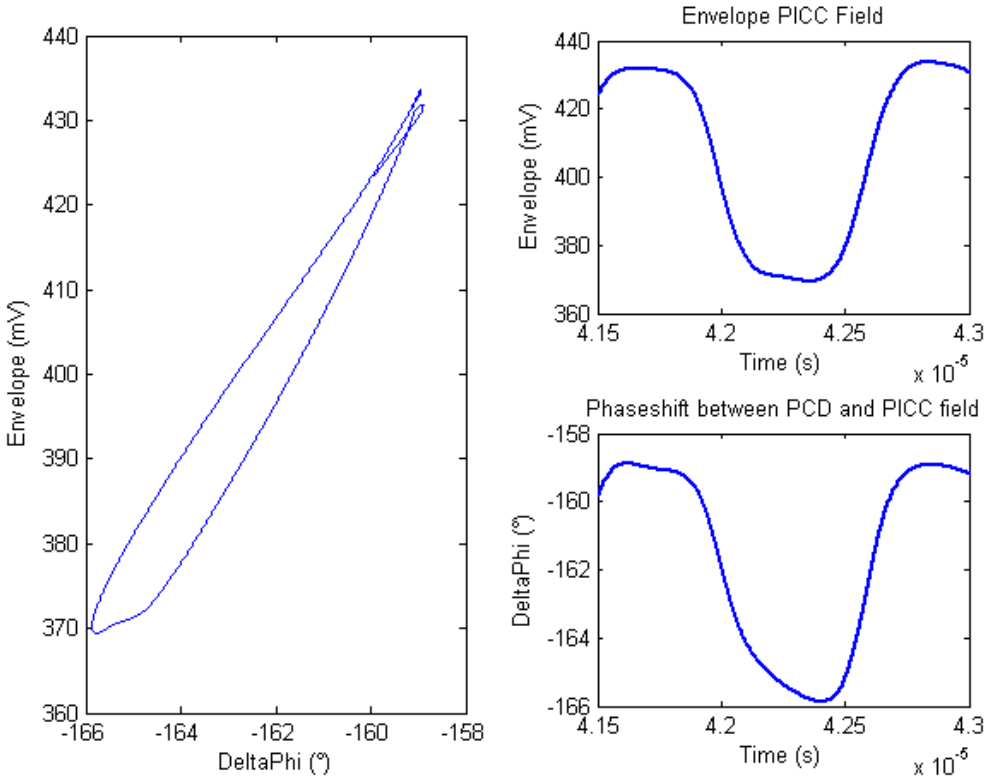


Figure 6-12: T2S1 constellation plot at 5.5A/m error case

6.5 Impact of PCD receiver

All of the preceding constellation plots were created with a fairly large bandwidth of bandpass filter BP1. This large bandwidth of 1.695MHz is appropriate, if a large population of PCDs with different resonance frequencies is considered.

However, the receive bandwidth of an individual PCD antenna is in the range of about 700kHz as already shown in Table 5-1. In addition to the smaller bandwidth of the antenna, the PCD may even use additional filtering in the receiver network.

In this section the impact of a smaller bandwidth on the constellation plot shall be evaluated. For this purpose the 3dB bandwidth of the PCD terminal under test (see 4.1.2) was measured and filter BP1 was adjusted to those values.

Table 6-1: Bandwidth of PCD terminal under test

Lower cut-off frequency fL [MHz]	13.4733
Upper cut-off frequency fU [MHz]	14.2267
Bandwidth B [kHz]	753.4

Additional filtering in the receiver network was not considered for simplicity sake.

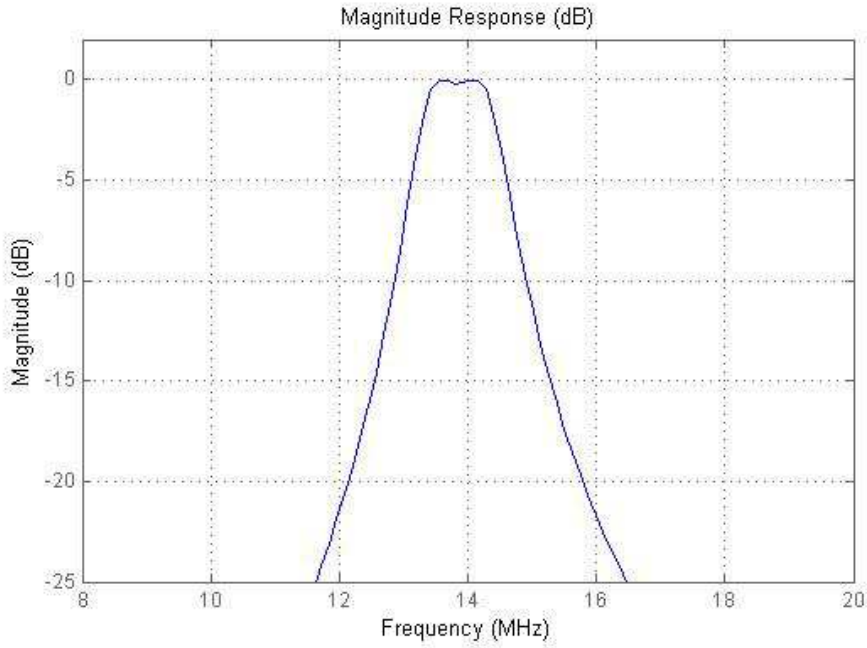


Figure 6-13: Magnitude response of BP1 with reduced bandwidth

Again zero-phase filtering was used to avoid any unintended phase distortions.

These tests showed that in the case of overshoots, as they were observed with the citizen ID card sample of type 1, the reduced bandwidth may lead to an increase of the distortions in the IQ demodulator.

The following figure shows the comparison between the constellation plots with the original higher bandwidth filter (2695kHz) and the adjusted filter parameters to replicate the PCD terminal's antenna characteristic (753.4kHz).

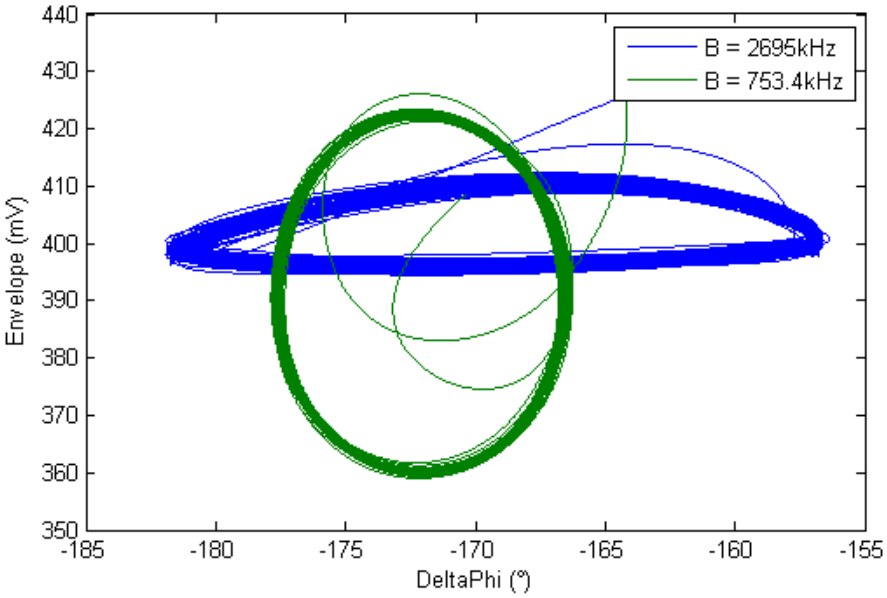


Figure 6-14: Comparison T1S1 constellation plot with different filter bandwidth

In the case of type2 PICC samples the observed phase jitter was actually improved by the lower bandwidth of filter BP1.

Also at samples that did not show any issue the impact of the filter was largely negligible and only affected the amplitude of phase and envelope jumps during modulation.

6.6 Summary

The analysis has shown that a good correspondence between the phase shift and the amplitude (envelope) of the PICC's field contribution is essential for successful reading. A lack of correspondence is seen as a wider ellipse in the constellation plot and evidently leads to distortions in the IQ demodulation. The orientation of the ellipse in the plot has no significance. A lack of correspondence can be caused by distortions such as the observed phase jitter and/or overshoots in the envelope. Such behaviours are not flagged by existing tests in the standards.

A potential improvement to the tests would be the method of creating a constellation plot, which not only shows the modulation endpoints, but also plots the dynamic change between them.

Further it was shown that the more limited bandwidth of a real PCD receive characteristic may increase distortions such as overshoots. This needs to be considered in the definition of limits for such a test.

7 New Parameter and Test Limits

This chapter covers the definition of limits for a PICC's constellation plot to ensure that no communication problems can occur due to distortions in the load modulation. For such limits new formal parameters in the constellation plot are defined as a measure for the quality of the load modulation. The implementation of the new test limits is explained upon the measurements conducted with the citizen ID card sample T1S1. Afterwards a short proposal for the extension of the standards is provided.

7.1 Parameter definitions

For the definition of test parameters it shall be assumed that the dynamic change of the constellation plot forms an ellipse, as this shape is closest to the observed results from section 6. This shape would represent a non-ideal constellation plot with a certain degree of distortions.

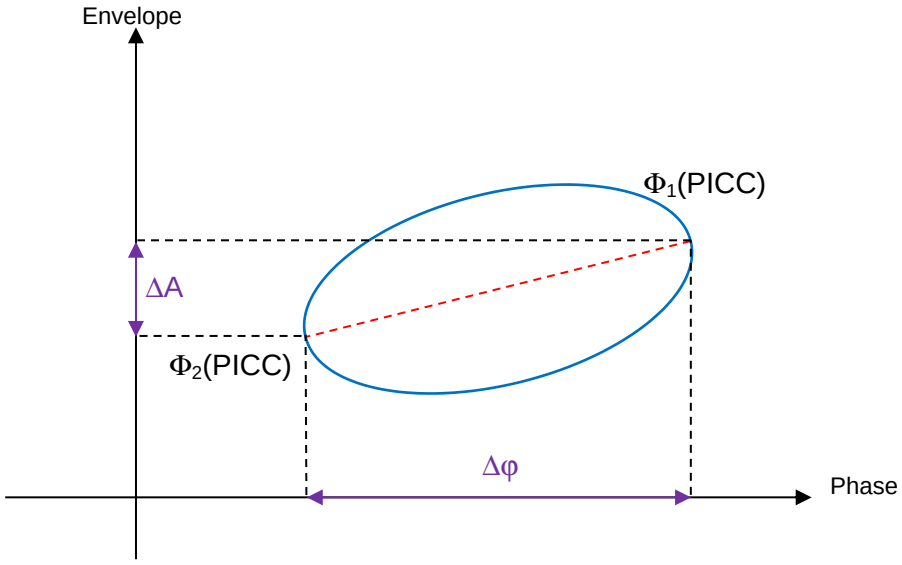


Figure 7-1: Generic constellation plot

The modulation endpoints Φ_1(PICC) and Φ_2(PICC) are located on the major axis (red dotted line). The major axis represents the perfect dynamic change (no distortions) in the form of a straight line between Φ_1(PICC) and Φ_2(PICC).

The load modulation amplitude of the PICC is determined through the change of the envelope ΔA and phase $\Delta\varphi$.

The size of the minor axis of the ellipse is proportional to the lack of correspondence of envelope and phase in the load modulation waveform of the PICC, as shown in chapter 6.

Based on this, two additional points Φ_{n1}(PICC) and Φ_{n2}(PICC) are defined. The two points are chosen, such that the line joining them is perpendicular to the „major axis“ of the constellation plot and the distance between them is maximised.

In the case of a perfectly elliptical dynamic change the points would be on the ellipse‘s minor axis.

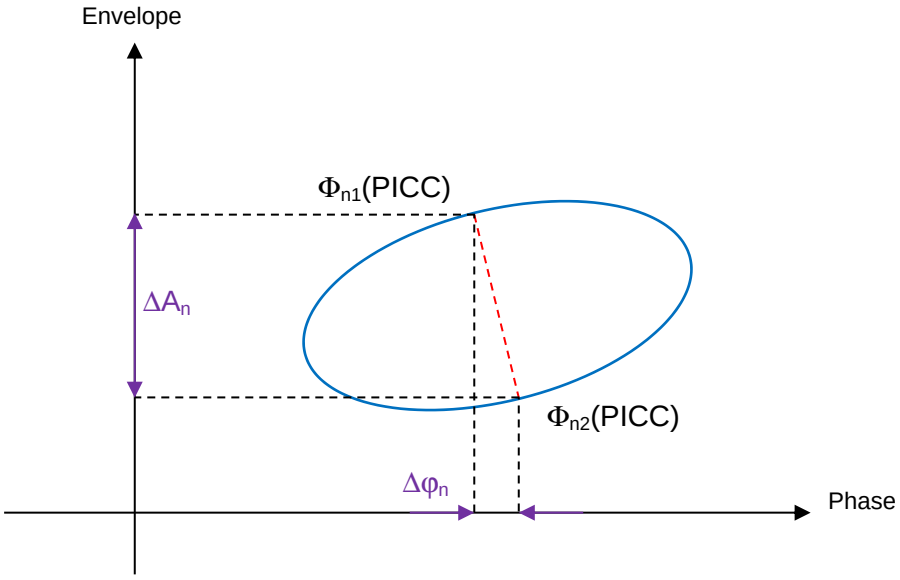


Figure 7-2: Definition of Φ_{n1}(PICC) and Φ_{n2}(PICC)

As for the amplitude of the modulation signal, the amplitude of the distortion is given through a change in envelope ΔA_n and a change in phase $\Delta\varphi_n$.

The amplitude of the distortion needs to be kept within limits to ensure interoperability between the tested PICC and PCDs deployed in the field.

7.2 Implementation

The test of a PICC for its maximum distortion amplitude is shown on the basis of measurements taken with the citizen ID card sample T1S1 at 5.5A/m.

As described in section 5, the constellation plot of the PICC is generated. In this constellation plot, for each recorded subcarrier cycle, the points Φ_1(PICC) and Φ_2(PICC) as well as Φ_{n1}(PICC) and Φ_{n2}(PICC) are determined. Afterwards the envelope change ΔA_n and phase change $\Delta\varphi_n$ are taken from the subcarrier cycle that shows the largest distance between Φ_{n1}(PICC) and Φ_{n2}(PICC).

Φ_1(PICC) and Φ_2(PICC) are found by analysing the correspondence between the sample point distribution maxima in the envelope and the phase shift as shown in Figure 7-3.

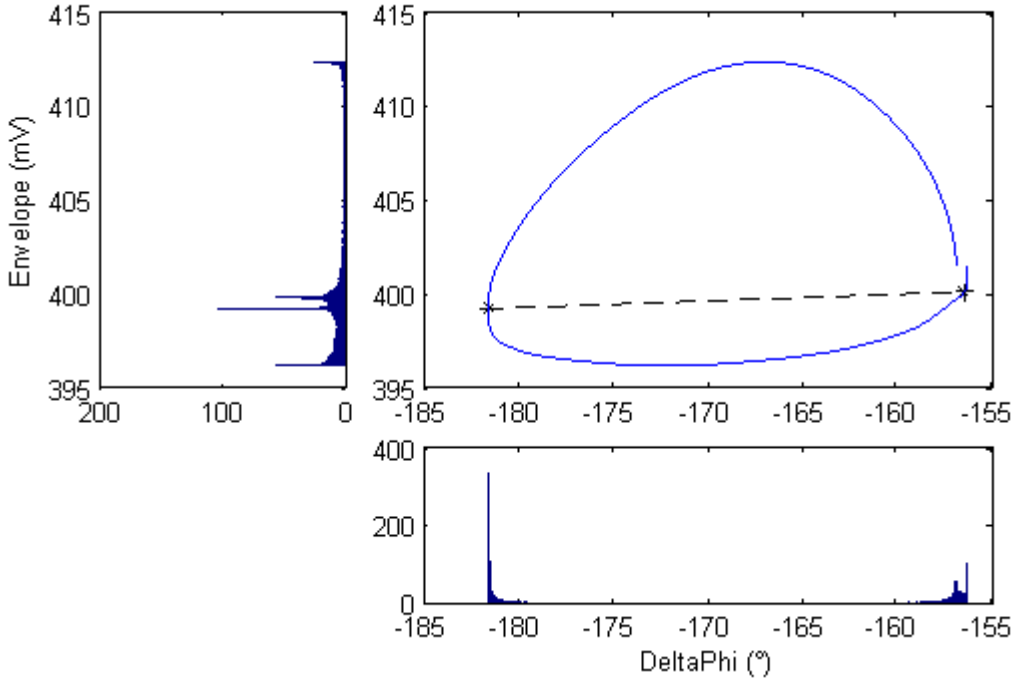


Figure 7-3: Determination of Φ_1(PICC) and Φ_2(PICC)

The two histograms to the left of and below the constellation plot show the sample point distribution in phase and amplitude. In the case of the T1S1 PICC the envelope distribution shows four maxima due to the distortions observed in the load modulation. However, as only two of the maxima correspond with maxima in the phase shift histogram, those caused by distortion can easily be discarded.

This method for determining Φ_1(PICC) and Φ_2(PICC) works successful for all tested PICCs. There may be PICCs that exhibit distortions that lead to multiple corresponding maxima in phase shift and envelope. If such examples are found in the future this algorithm may need to be adjusted.

With Φ_1(PICC) and Φ_2(PICC) determined, the linear function for the major axis of the constellation plot is set.

$$y_{major} = k_{major} \cdot \Delta\varphi + d_{major}$$
$$k_{major} = \frac{\Delta\varphi_{\Phi_1(PICC)} - \Delta\varphi_{\Phi_2(PICC)}}{Envelope_{\Phi_1(PICC)} - Envelope_{\Phi_2(PICC)}}$$
$$d_{major} = Envelope_{\Phi_2(PICC)} - k_{major} \cdot \Delta\varphi_{\Phi_2(PICC)}$$

Equation 7-1: Linear equation for major axis

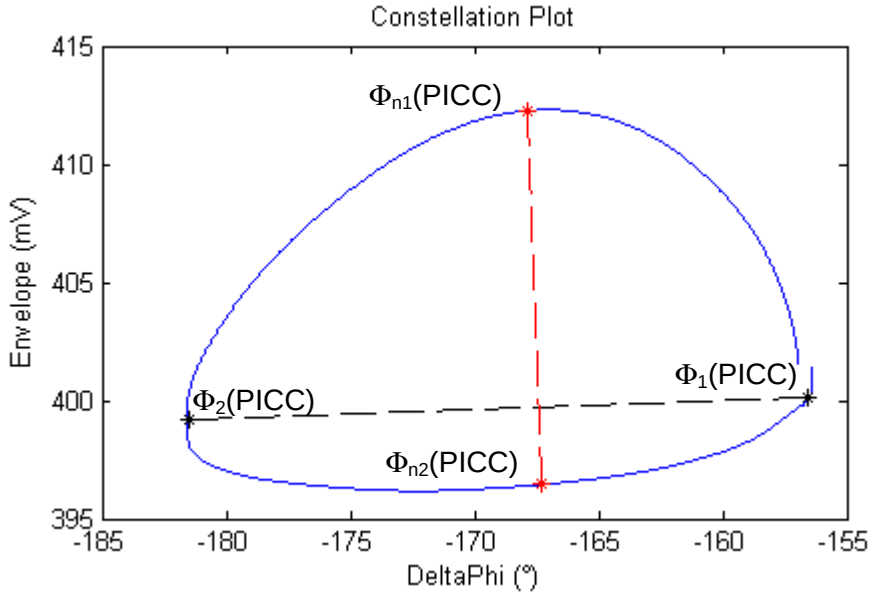
With the gradient of the major axis, the gradient of the perpendicular line connecting the two distortion points Φ_{n1}(PICC) and Φ_{n2}(PICC) can be calculated.

$$k_{distortion} = -\frac{1}{k_{major}}$$

Equation 7-2: Gradient calculation of connection line for Φ_{n1}(PICC) and Φ_{n2}(PICC)

With this gradient for each point of the lower half of the constellation plot the corresponding intersection point of the upper half is calculated and the distance evaluated.

The two points with the greatest distance between them are then chosen as the distortion points Φ_{n1}(PICC) and Φ_{n2}(PICC) of this particular subcarrier cycle.



Equation 7-3: Single subcarrier constellation plot with all defined points

After the analysis, the subcarrier cycle with the greatest distances between its points Φ_{n1}(PICC) and Φ_{n2}(PICC) is kept and ΔA_n and $\Delta\varphi_n$ are determined.

$$\Delta A_n = Envelope_{\Phi_{n1}(PICC)} - Envelope_{\Phi n2(PICC)}$$
$$\Delta\varphi_n = \Delta\varphi_{\Phi_{n1}(PICC)} - \Delta\varphi_{\Phi n_2(PICC)}$$

Equation 7-4: Calculation of ΔA_n and $\Delta\varphi_n$

To achieve a single amplitude value for the distortion, an artificial load modulation with a relative amplitude change of ΔA_n and a phase change of $\Delta\varphi_n$ is generated.

This load modulation is then analysed in accordance with the load modulation amplitude test defined in [ISO05]. However, in this instance the result of the sideband amplitudes is not representative of the amplitude of a PICC's load modulation, but rather of the distortion.

To generate the artificial load modulation two square waves with a frequency of fs (847.5kHz) are defined. One with an amplitude of ΔA_n for the envelope and one with an amplitude of $\Delta\varphi_n$ for the phase. The sign of the values can be ignored as it does not impact the amplitudes of the generated sidebands. As initial values, an amplitude of 100mV and a phase shift of -90° are chosen.

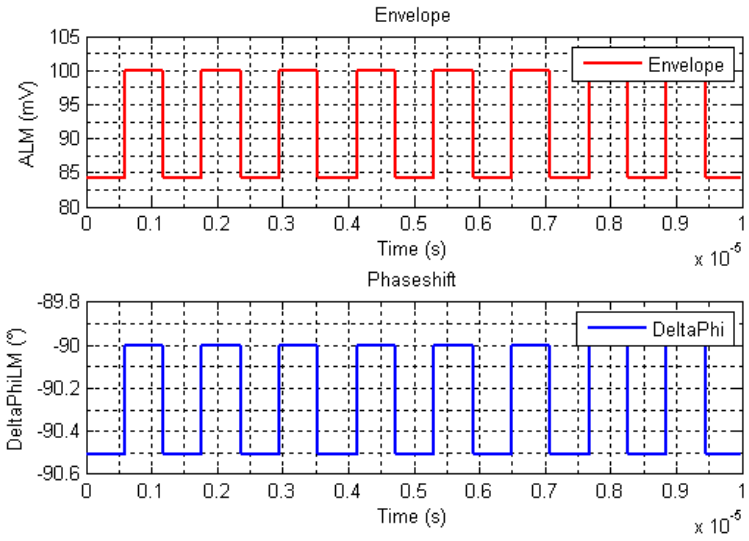
$$A_{LM} = A_{initial} - \frac{|\Delta A_n|}{2} * (1 + square(2\pi \cdot fs \cdot t))$$
$$\Delta\varphi_{LM} = \Delta\varphi_{initial} - \frac{|\Delta\varphi_n|}{2} * (1 + square(2\pi \cdot fs \cdot t))$$

$A_{initial}$ Initial Amplitude (100mV)
$\Delta\varphi_{initial}$ Initial Phaseshift (-90°)
fs Subcarrier Frequency (847.5kHz)
t Time

Equation 7-5: Square waves for artificial load modulation signal

Note that the MATLAB® function "square" generates a square wave with a period of 2π with peaks of ±1. For that reason it is necessary to divide both ΔA_n and $\Delta\varphi_n$ by two and use 1+square(2π*fs*t) in order to achieve the required result.

In the example of the citizen ID card T1S1 ΔA_n was calculated as -15.81mV and $\Delta\varphi_n$ as 0.51°. The following figure shows the two square waves for the artificial load modulation signal.



Equation 7-6: T1S1 square waves for artificial load modulation signal

From these two square waves a load modulation signal is generated by the following equation.

$$LM = A_{LM} \cdot \sin(2\pi \cdot fc \cdot t + \Delta\varphi_{LM})$$

Equation 7-7: Calculation of artificial load modulation

This load modulation is then analysed in accordance with the load modulation amplitude test defined in [ISO05]. This means that the FFT is calculated for six subcarrier cycles and the modulation sideband levels of the amplitude spectrum are taken.

The following figure shows the artificial load modulation and the single sided amplitude spectrum for T1S1.

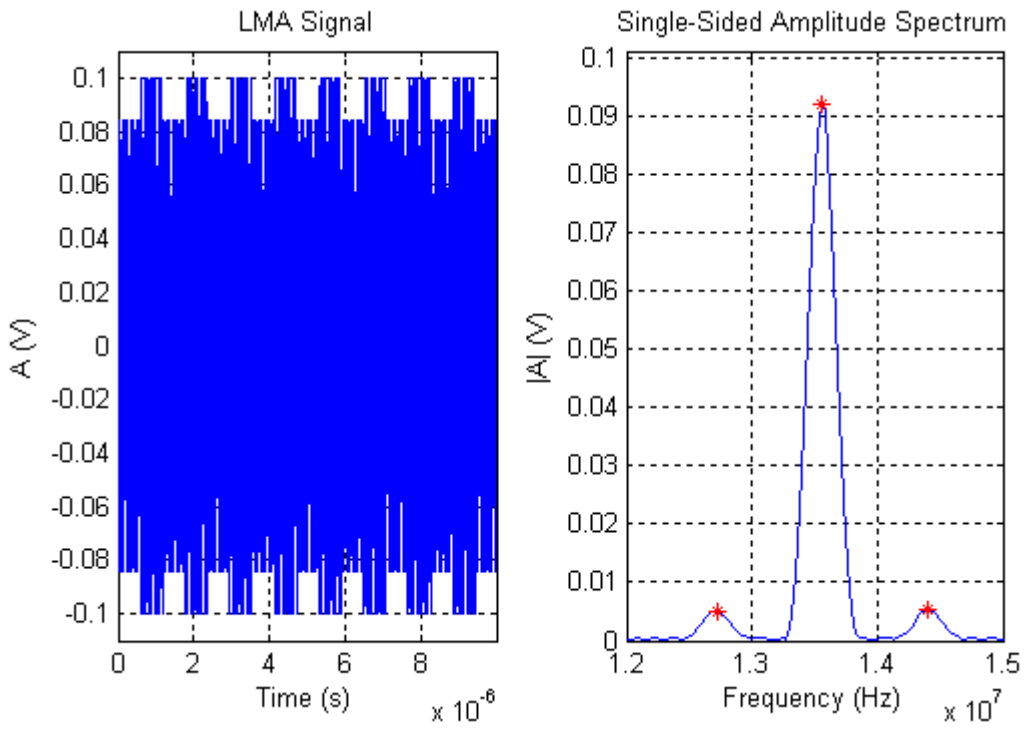


Figure 7-4: Artificial load modulation signal and spectrum for T1S1

As mentioned before, the amplitude of the sidebands in this case is not a measure of the real load modulation amplitude of the PICC, but of the distortion amplitude (opening of constellation plot). For the citizen ID card sample T1S1 this distortion calculates as 5.2mV.

The shown implementation allows the calculation of a distortion amplitude from the two-dimensional constellation plot generated for a PICC. To allow this distortion to be a testable parameter a limit definition is necessary.

7.3 Limit definition

As most RFID reader ICs do not have an automatic gain control in their receiver stage, the limit for the distortion cannot be relative to the the load modulation amplitude, but needs to have an absolute value. This means that a PICC with a larger load modulation amplitude cannot exhibit stronger distortions, because for PCDs it would be sufficient for the distortion to exceed a certain threshold.

Additionally variations in sensitivity with field strength of need to be considered. The current test limit for the load modulation amplitude already takes this effect into account.

[ISO01] stipulates that the load modulation amplitude of a PICC needs to exceed $22/H^{0.5}$ [mV(peak)], when measured in accordance to [ISO05], where H is the magnetic field strength in A/m. At the same time a PCD needs to be able to decode a load modulation signal of at least $18/H^{0.5}$[mV(peak)].

The following figure plots the specified limits for PCD and PICC:

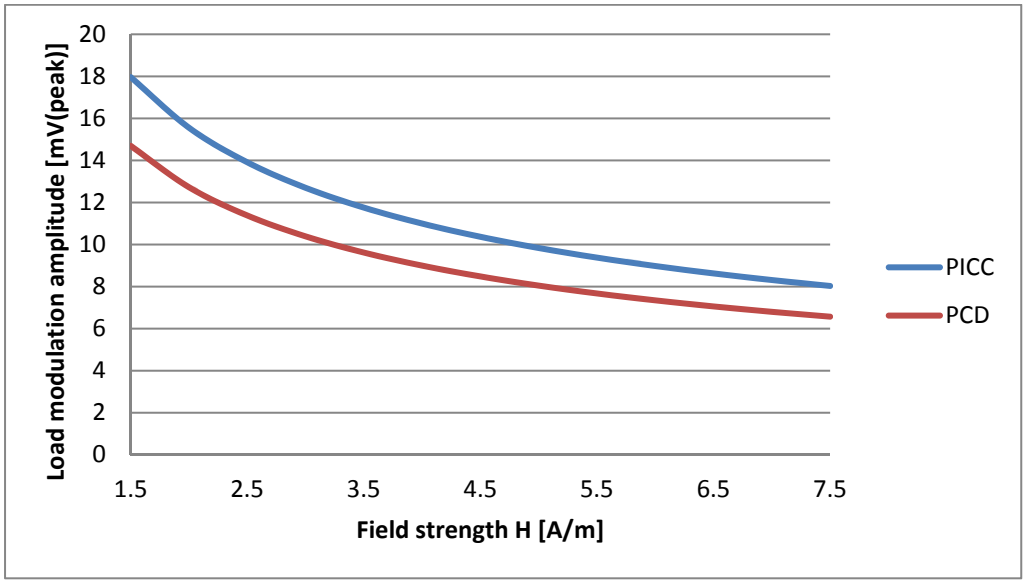


Figure 7-5: Load modulation amplitude limits according to [ISO01]

These limits were empirically determined and already consider the effect that a PICC will have a lower load modulation amplitude at higher field strengths. This is due to the lower quality factor, caused through the shunt voltage regulator of the PICC. Also a PCD typically shows a higher sensitivity at high field strengths. This, however, has its root cause in the fact that a higher field strength produced by the PCD indicates a stronger coupling with the PICC and this allows for more of the load modulation to be actually received.

The maximum amplitude of the distortion within the load modulation of a PICC always needs to stay below the PCD's sensitivity to ensure successful communication. To allow this, a certain margin between the minimum PCD sensitivity and the maximum distortion amplitude needs to be defined.

Measurements on working PICC samples indicate that a maximum distortion amplitude of $6/H^{0.5}$ is an appropriate initial compromise.

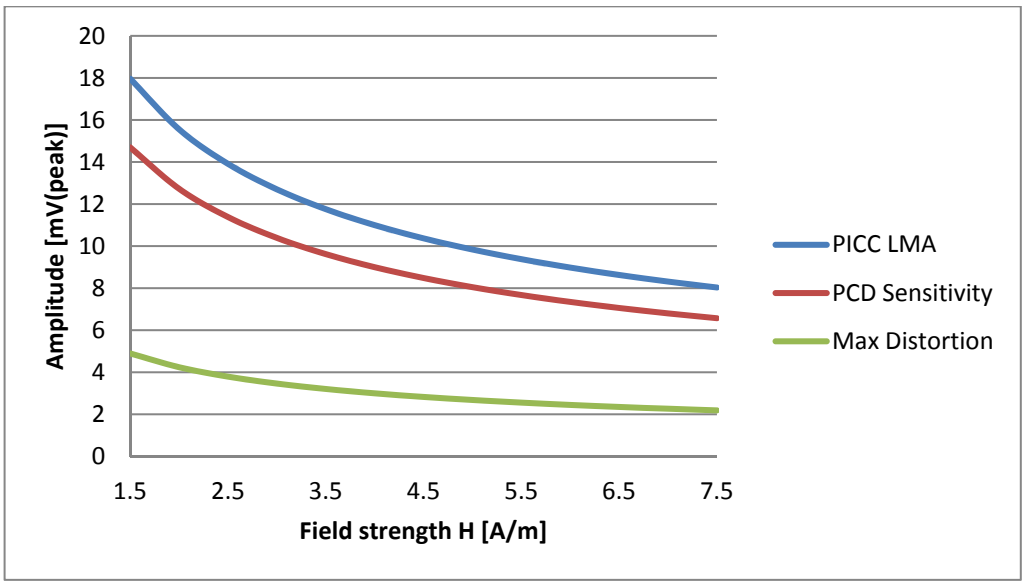


Figure 7-6: Maximum distortion amplitude in load modulation

The following table shows some of the distortion amplitudes measured for PICCs tested during the work for this thesis.

Table 7-1: Distortion amplitudes for various PICCs

PICC	H [A/m]	Distortion Amplitude [mV]	Limit [mV]	Result
Reference PICC SRF = 16.5MHz VDC = 3VDC	1.5	2.9	4.9	Pass
	3.5	<1	3.2	Pass
	5.5	<1	2.6	Pass
Citizen ID card sample T1S1	3.5	5.5	3.2	Fail
	5.5	5.2	2.6	Fail
Citizen ID card sample T2S1	3.5	1.63	3.2	Pass
	5.5	1.53	2.6	Pass
NXP SmartMX	3.5	1.0	3.2	Pass
	5.5	<1	2.6	Pass

The results show that the citizen ID card sample T2S1 passed the test in the conducted measurement. The problem with this sample is, that due to the random phase jitter, the distortion amplitude is different for each measurement. Other measurements were taken were the distortion amplitude was calculated as 3mV at 5.5A/m which would mean a fail.

To allow this test to be effective a sensible number of subcarrier cycles needs to be measured and analysed to ensure that also random events are captured. Also the actual limit value may need to be readjusted when a larger database of results is available.

7.4 Standard extension

In order to accommodate the new test parameters and procedures described in this thesis, an extension to the ISO/IEC14443-2 and ISO/IEC10373-6 standards is necessary.

In this section a rough outline of the required modifications is provided.

7.4.1 ISO/IEC14443-2 extension

Section 8.2.2 of the ISO/IEC14443-2 describes the limits for the load modulation amplitude. To include the new parameter of distortion, a new section 8.2.3 may be inserted with the title “load modulation distortion”.

In this section it should state that the load modulation signal of a PICC is composed of both phase and amplitude changes and that a lack of correspondence between those two components, caused by distortions, can lead to communication problems. This section should also state that the maximum distortion amplitude of the PICC should never exceed $6/H^{0.5}$ [mV(peak)] when measured as described in ISO/IEC10373-6, where H is the (rms) value of magnetic field strength in A/m.

This extension should also describe the constellation plot with its defined points as per section 7.1 in this document.

7.4.2 ISO/IEC10373-6 extension

The signal analysis procedure required to compute the distortion amplitude may be added to a new annex of the standard. ISO is currently working on a new tool that determines the continuous phase drift of active modulation PICCs (whereby instead of loading the PCD the PICC actively transmits the subcarrier cycles, which allows for smaller form factors). This tool may be extended with the required signal analysis calculations shown in this thesis, to also determine the distortion amplitude. Sample source code would also be provided within the standard.

Section 7 of the ISO/IEC10373-6 describes all tests of ISO/IEC14443-2 parameters and is subdivided into section 7.1 for PCD and 7.2 for PICC tests.

A new section 7.2.5 with the title “load modulation distortion” may be added. As for other tests defined within this standard, the section needs to be subdivided into purpose, test procedure and test report. The following provides an outline of what needs to be captured in the individual subsections.

Purpose:

The purpose of this test is to determine the maximum distortion amplitude of the PICC’s load modulation within the operating field range specified in ISO/IEC14443-2.

Test procedure:

Step1: The load modulation test circuit (Figure 5-2) and the test PCD assembly (Figure 5-1) are used.

Connect the output of the load modulation test circuit (sense coil voltage) and the calibration coil to a digital sampling oscilloscope. Adjust the RF power delivered by the signal generator to the test PCD antenna to the required field strength, as measured by the calibration coil. The 10Ω potentiometer P1 shall be trimmed to minimize the residual carrier at the load modulation test circuit.

Step2: The PICC under test shall be placed in the DUT position, concentric with sense coil a. A command sequence as defined by ISO/IEC14443 shall be send by the test PCD to obtain a signal or load modulation response from the PICC with a frame length of 256bytes.

Note that the long frame length is chosen, in order to ensure that PICCs such as T2S1, which show the problem only intermittently, are properly tested.

Display the calibration coil voltage and the frame sent by the PICC under test on the digital sampling oscilloscope and store the sampled data in a file for analysis by a computer software program (see Annex XY).

Note that the digital oscilloscope should have a minimum overall bandwidth of 250MHz, a minimum sampling rate of 100 million samples per second and a resolution of at least 8bit for this test.

The resulting peak distortion amplitudes shall be below the value defined in ISO/IEC14443-2, 8.2.3.

Test report:

The test report shall provide the measured peak distortion amplitudes at 1.5, 2, 2.5, … 7.5 A/m.

8 Conclusions and Outlook

This section summarizes the results and provides an outlook on future steps as well as further optimization possibilities. In addition an assessment of the conducted work from the author's point of view is provided.

8.1 Conclusion

Tests have shown that PCD's and PICC's can be certified against today's standards, yet still be incompatible with each other. The work within this thesis identified distortions in the load modulation as the root cause for the observed issues in at least two of these problem cases. It was also shown that today's test regime does not cover the question of modulation waveforms for PICCs, as only the sideband levels of the amplitude spectrum are available.

To overcome this issue a new PICC modulation analysis procedure was introduced that takes the dynamics of the load modulation into consideration and allows the calculation of a distortion amplitude. This procedure is based on a constellation plot and successfully identifies PICC's, which show communication problems with certified PCD's. The various signal analysis calculations were implemented with MATLAB®.

In addition a proposal on the extension of the current standards was created.

8.2 Outlook

As already mentioned in section 1.2, the results from this thesis will be presented to the ISO committee with the goal of extending the current test standards.

During this submission process it is expected that further technical refinements and specifications will be discussed. Those will most likely include the refinement of the test limit, based on a larger test database, as well as the other test parameters like the minimum number of subcarrier cycles that needs to be analysed.

First presentations of the observations and the idea for the test concept defined in this work were met with great interest by the RFID community and led to encouraging feedback also from parties within the ISO committee.

8.3 Assessment of work

The scope of work was fully satisfied within the context of this thesis. The analysis results have shown that the observed interoperability issues between PCDs and PICCs are caused by a lack of correspondence between the phase shift and the envelope of the PICC's field contribution. The extension of the existing tests proposed in this document defines parameters and methods, which will allow further improvement to the interoperability of ISO/IEC14443 RFID systems in the future.

As mentioned before, there may still be refinements and additional measurement specifications necessary to fulfil the requirements of a standardized test procedure. However, the conducted work provides a solid base for a new test method that allows the identification of critical PICC modulation distortion.

In addition the document provides a short overview on different RFID systems and the RF interface of ISO/IEC14443 systems.

References

[BSI2010] BSI TR-03105: Test plan for official electronic ID documents with secure contactless integrated circuit, 53133 Bonn Germany, BSI, 2010

[FinKl2002] Finkenzeller, Klaus: RFID-Handbuch, Munich Germany, Hanser, 2002

[ICAO2007] ICAO Technical Report: RF Protocol and Application Test Standard for E-Passport V1.01 – Part 4, Montreal Canada, ICAO, 2007

[ISO01] ISO/IEC14443-2:2010: Radio frequency power and signal interface, 1211 Geneva Switzerland, ISO/IEC, 2010

[ISO02] ISO/IEC14443-2:2010/AMD1:2011: Limits of electromagnetic disturbance levels parasitically generated by PICC, 1211 Geneva Switzerland, ISO/IEC, 2010

[ISO03] ISO/IEC14443-2:2010/AMD2:2012: Additional PICC classes, 1211 Geneva Switzerland, ISO/IEC, 2010

[ISO04] ISO/IEC14443-2:2010/AMD3:2012: Bit rates of fc/8, fc/4 and fc/2, 1211 Geneva Switzerland, ISO/IEC, 2010

[ISO05] ISO/IEC10373-6:2011: Test methods proximity cards, 1211 Geneva Switzerland, ISO/IEC, 2010

[ISO06] ISO/IEC10373-6:2011/AMD1:2012: Additional PICC classes, 1211 Geneva Switzerland, ISO/IEC, 2010

[ISO07] ISO/IEC10373-6:2011/AM2:2012: Exchange of additional parameters, block numbering, unmatched AFI and TR2, 1211 Geneva Switzerland, ISO/IEC, 2010

[Marple1999] Marple, S.L.: Computing the discrete-time analytic signal via FFT, New York USA, IEEE, 1999

Appendices

Appendix A. Simulation of PICC Field Phase

As the magnetic field contributions of the PICC and PCD are proportional to their antenna currents, the possible phase relation can be simulated by looking at these currents. For this a simplified model was used:

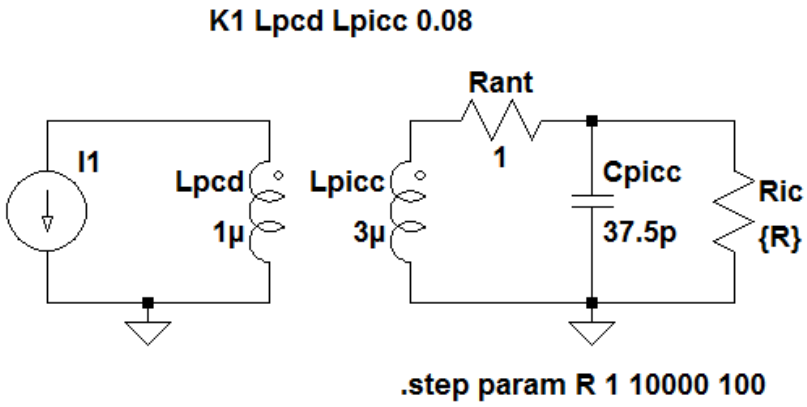


Figure A-1: Simplified PCD and PICC model for phase shift simulation

Lpcd represents the PCD's antenna with a typical inductance of 1µH. Lpicc represents the PICC's antenna with a parallel capacitor Cpicc that results in a resonance frequency of about 15MHz which is a common value. Ric represents the load of the PICC's circuit and is varied from 1Ω to 10kΩ. For real PICCs this variation can be caused by either the shunt regulator or the load modulation unit. The coefficient of coupling between the PCD and PICC antennas was set to 8%, which again is a common value for real life RFID systems.

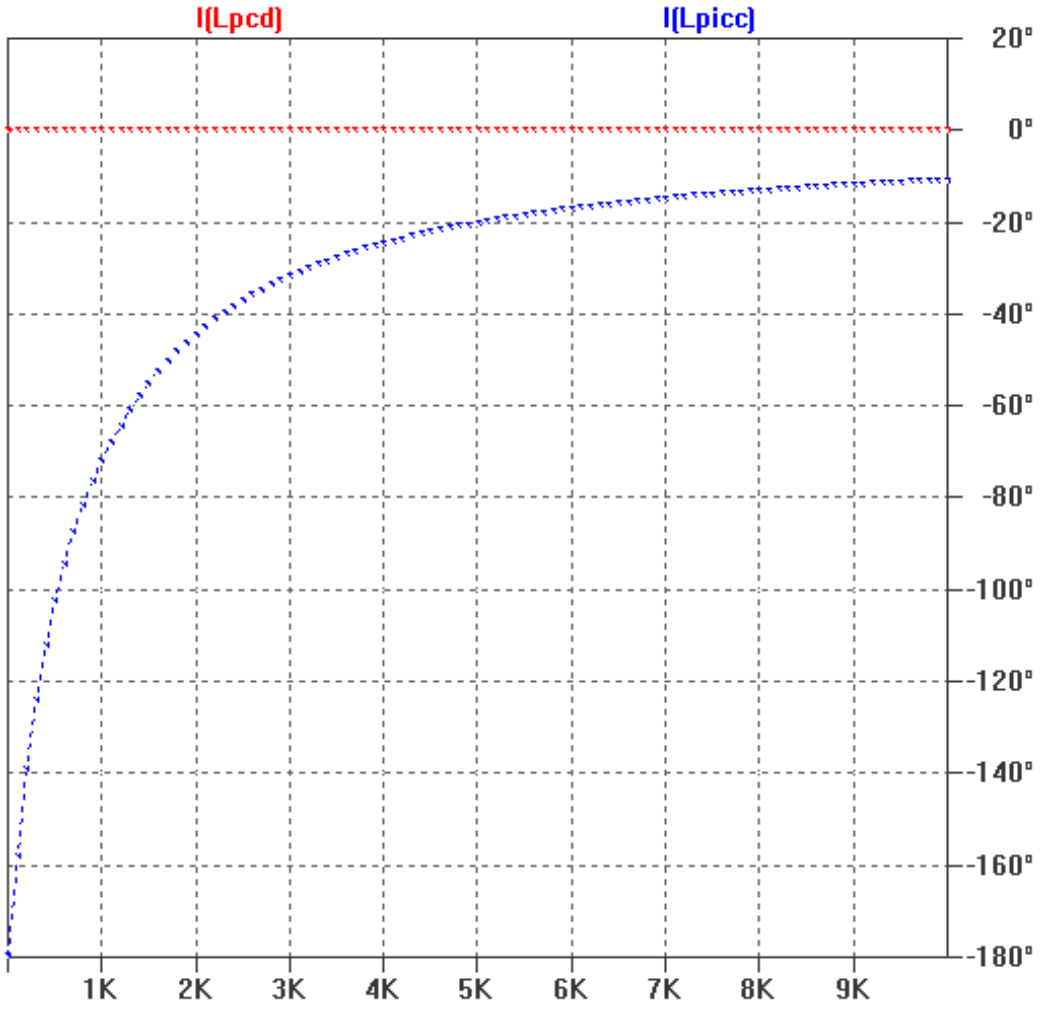


Figure A-2: Phase shift caused by quality factor variation

The result of the AC analysis at 13.56MHz shows that the phase shift of the current through Lpicc (I(Lpicc)) varies from -180° to -11° depending on Ric, which essentially determines the quality factor of the PICC antenna.

$$Q = \frac{2\pi f \cdot Lpicc \cdot Ric}{(2\pi f)^2 Lpicc^2 + Rant \cdot Ric}$$

Q quality factor

f frequency (13.56MHz)

Equation A-1: Quality factor of PICC antenna

A PICC may create load modulation by switching a resistor (ohmic load modulation), but also by switching a capacitance (capacitive load modulation). The change of capacitance causes a change in the resonance frequency, which changes both the amplitude and the phase.

To simulate such a load modulation, Ric was fixed to 5kΩ and Cpicc was varied from 1pF to 60pF.

Note that very small values of Cpicc result in a very high resonance frequency and prevent the PICC from absorbing much energy from the PCD's field. This may still represent a valid case if a PICC modulates the field by disconnecting the capacitance used to achieve its normal SRF (close to 13.56MHz) rather than adding additional capacitance.

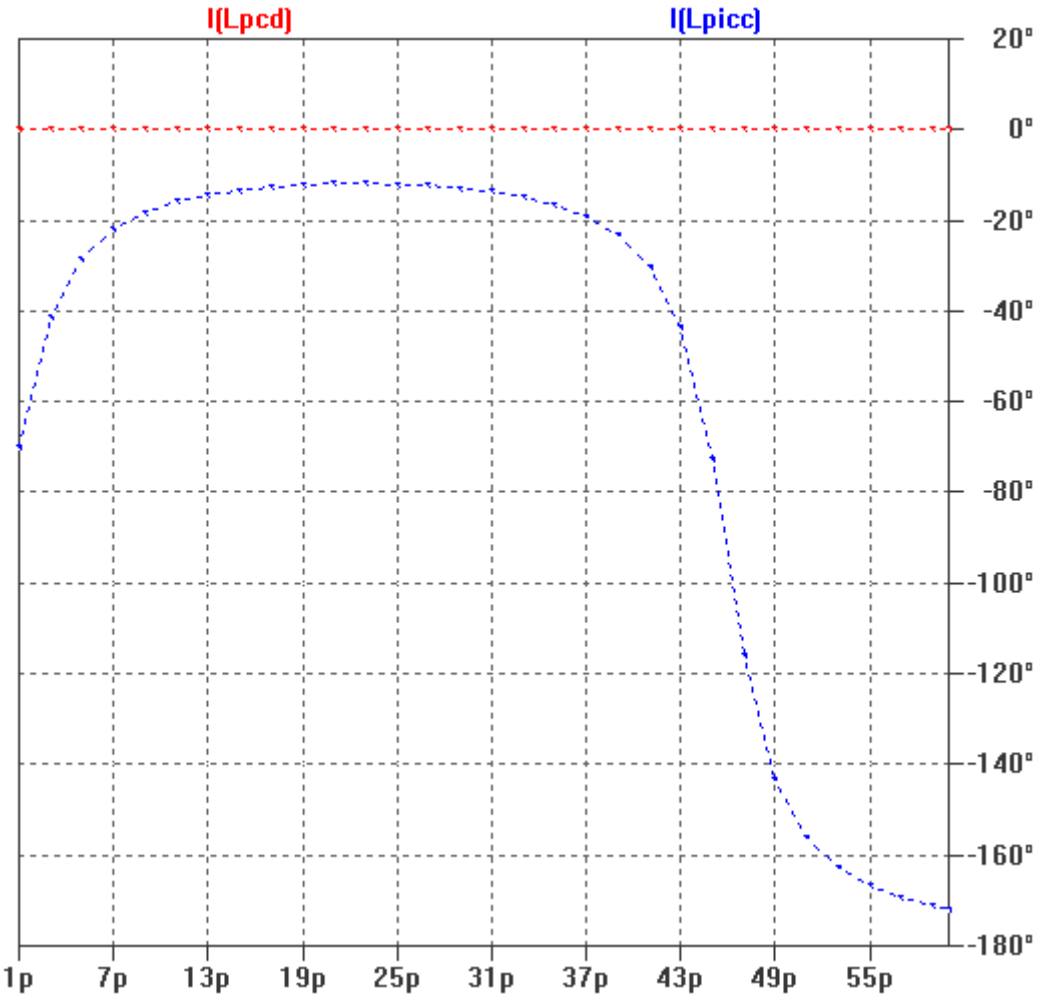


Figure A-3: Phase shift caused by SRF variation

To get a better overview of the possible phase shift conditions another simulation was conducted. It shows the phase shift for variations of both Ric and Cpicc. This is important as the relative phase shift caused by a quality factor change also depends on the SRF of the PICC.

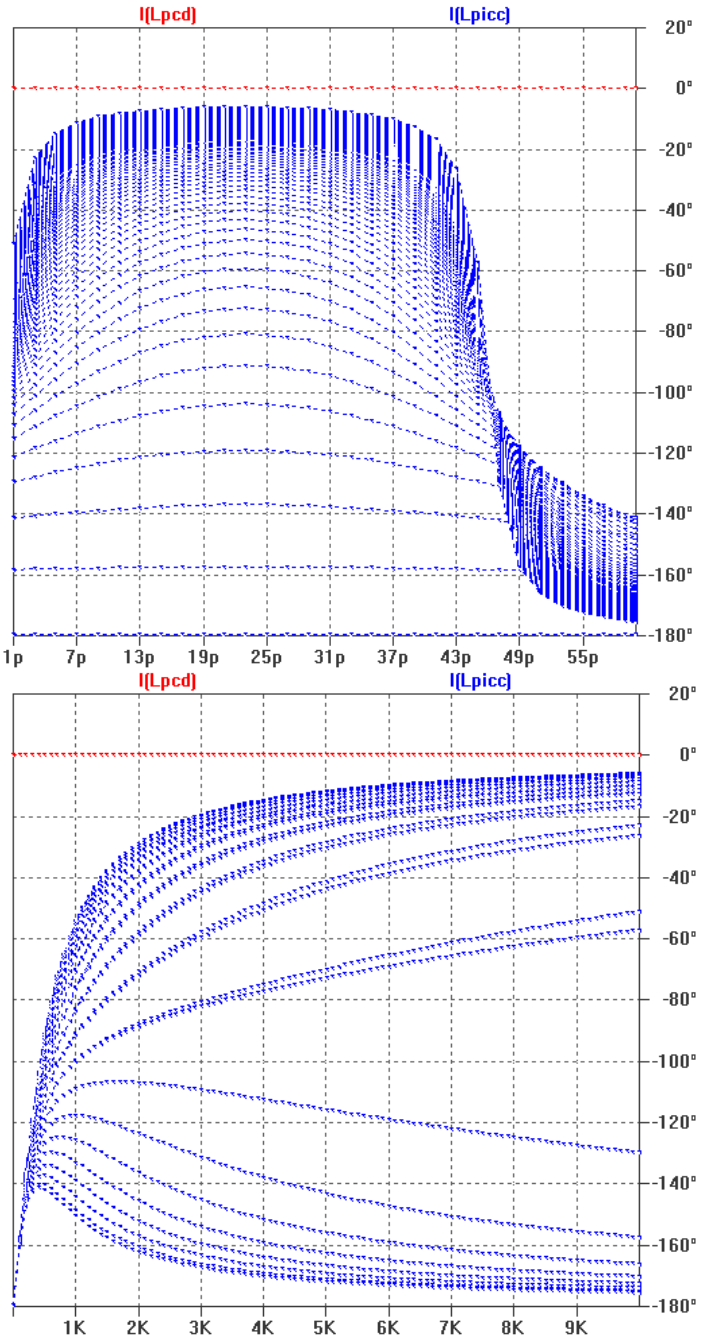


Figure A-4: Phase shift with variation of quality factor and SRF

The simulation results show that the phase shift of the PICC can be anywhere between -180° and -5° depending on the impedance of the PICC's IC. This confirms the assumptions of section 3.1.

Appendix B. Reader IC Tuning Circuit

A PCD's RF interface typically consists of a matching network, a tuning network and the antenna itself, besides the RFID reader IC's driver. The two main divisions are single-ended and double-ended (push-pull) drive. In the single-ended scheme the antenna circuit is driven with respect to ground along a single conductor and the current returns along the ground line.

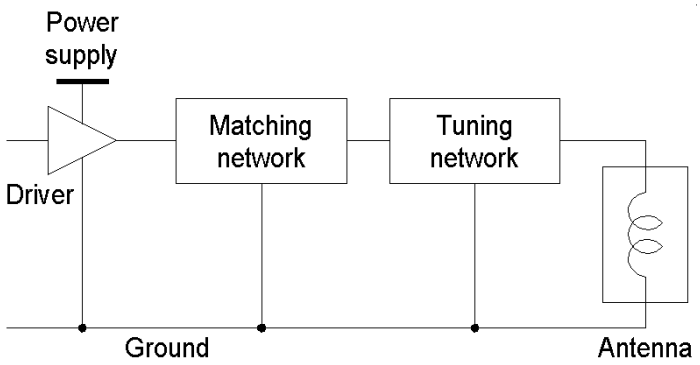


Figure B-5: Single ended PCD RF interface

In the double-ended scheme two drivers output in anti-phase and the current output by one returns to the other so that the ground connection carries little or no current.

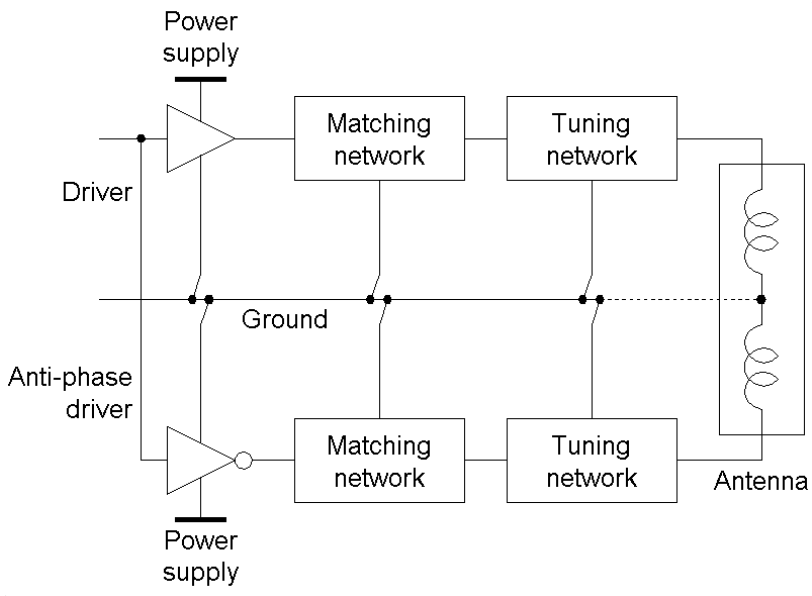


Figure B-6: Double ended PCD RF interface

The purpose of tuning is to arrange for the maximum amount of power to be delivered from the driver to the antenna. The driver operates from a power supply at voltage Vs and is able to deliver an output current up to some maximum value (Itmax) specified in the datasheet. This will be achieved by setting the value of the load impedance, Zt, as required, and this impedance should be a real value. The matching network converts this to a different voltage and current for connection to the tuned antenna, which presents a second impedance, Za, which should also be a real value.

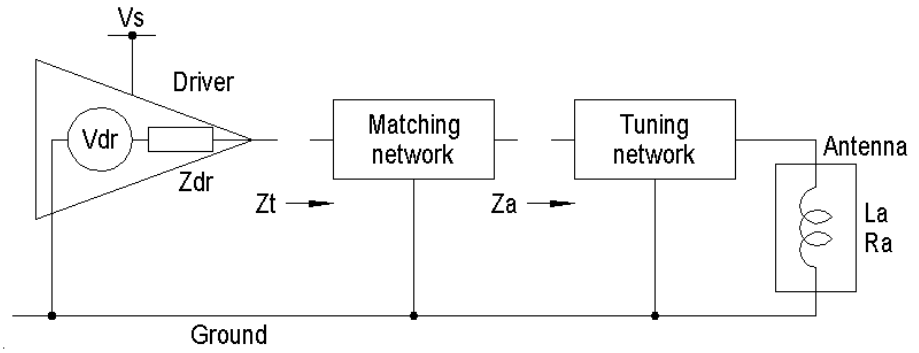


Figure B-7: Key impedances in PCD RF interface

The matching network commonly consists of an LC lowpass. One significant benefit of it is that it also serves to reduce the amplitude of any harmonics of the carrier frequency and this helps with EMC: For this reason the matching network is often called the EMC filter.

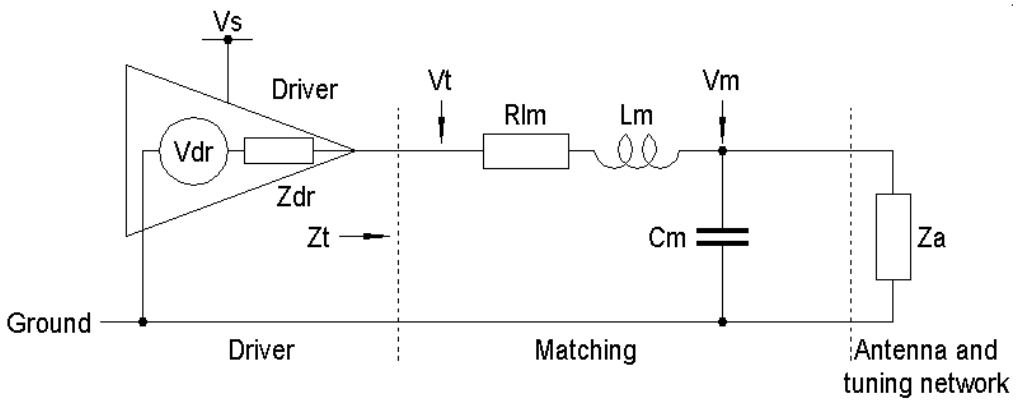


Figure B-8: Typical PCD matching network

The tuning network in most cases simply consists of two capacitors and a series or parallel resistor to control the quality factor of the antenna.

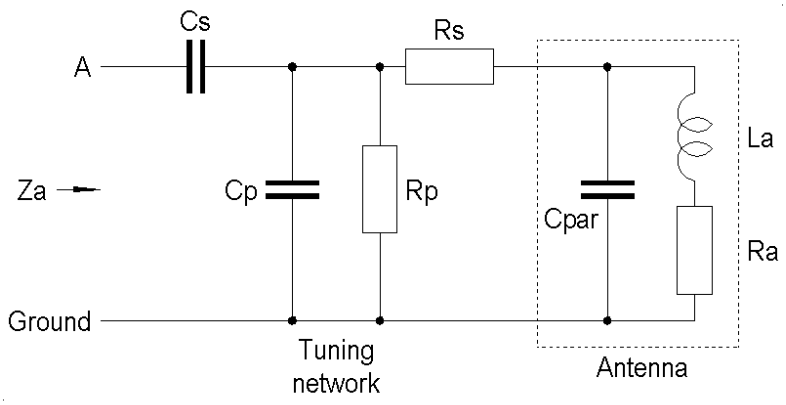


Figure B-9: Typical PCD tuning network

The receiver circuit takes its signal input either directly from the reader's antenna (source A) or from a point after the matching network (source B).

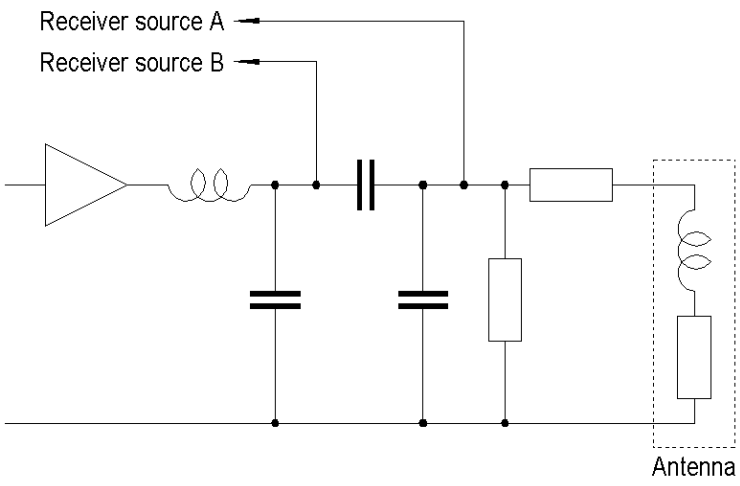


Figure B-10: Receiver connection on PCD RF Interface

In both cases the amplitude of the carrier is very large compared to the received signal and attenuation is required to prevent saturation of the receiver. The most common way to achieve this is a voltage divider external to the RFID reader IC.

However, if simple attenuation is applied then the answer signal of a PICC is attenuated to the same extent as the carrier and this represents a loss of useful signal. Fortunately, the PICC modulation is at a different frequency to the carrier (see 2.2.2), so some PCDs selectively suppress the carrier using a parallel LC resonant notch filter or similar.

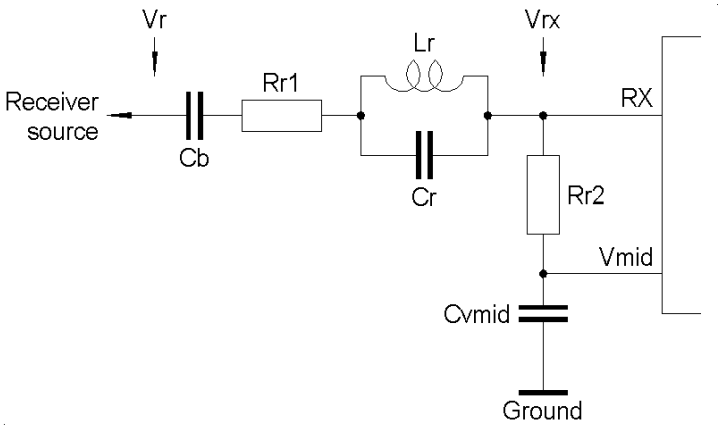


Figure B-11: Typical PCD receiver circuit with notch filter

Appendix C. Reference PICCs

Today's test methods largely rely on the use of equivalent circuit models of PICCs. A good model requires at the least the following features:

- The SRF of the PICC needs to be adjustable
- The shunt regulator of a real PICC needs to be modelled by an adjustable load
- The load modulation amplitude needs to be adjustable

The test standard [ISO05] defines a model for a Reference PICC used for the current test procedures.

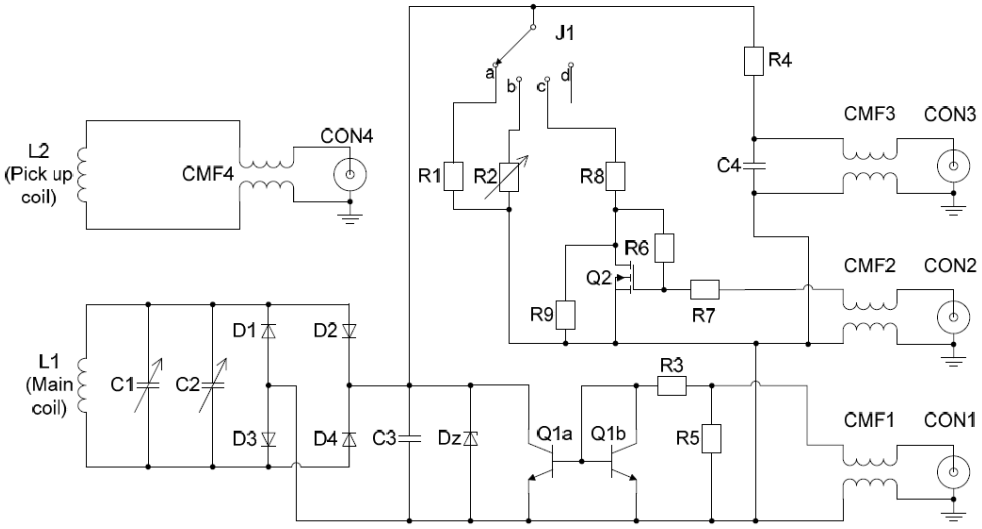


Figure C-12: Reference PICC circuit (source: [ISO05])

To test the receiving sensitivity of a PCD, a load modulation signal is created by an external source connected to CON1. Load modulation is applied by the current mirror circuit (Q1a and Q1b) and the sideband levels are determined by the amplitude of the signal at CON1.

The shunt regulator of the card is represented by either the potentiometer R2 or the voltage controlled resistor circuit (around Q2 – controlled by the voltage at CON2).

The pickup coil shown in the circuit is used for PCD waveform testing only.

The main coil of the Reference PICC is defined as follows:

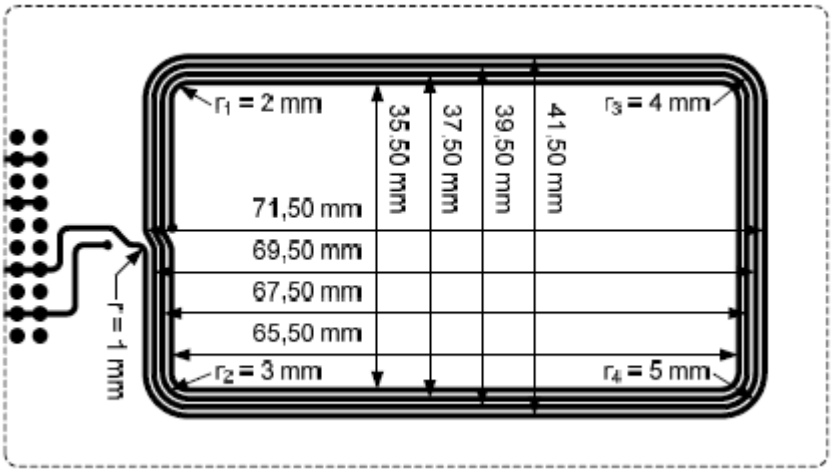


Figure C-13: Main coil Reference PICC (source: [ISO05])

Other standards use a simplified version of the Reference PICC, but apply the same principles.

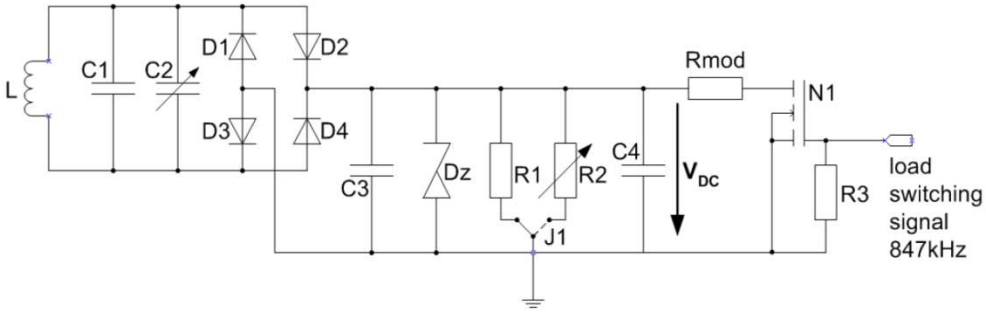


Figure C-14: Reference E-Passport (source: [ICAO2007])

For this particular example the current mirror is replaced by a resistor Rmod. The value of this resistor determines the sideband levels of the load modulation. The main coil design is equivalent to the one used in [ISO05].

Appendix D. Neumann Formula Implementation

To calculate the individual mutual inductances with a high accuracy, the double integral Neumann formula can be used.

$$L = \left(\frac{\mu_0}{4\pi} \int\int \frac{1}{|r_{ij}|} ds_i ds_j\right) + \frac{\mu_0}{4\pi} \cdot y$$

L inductance

μ_0 magnetic constant

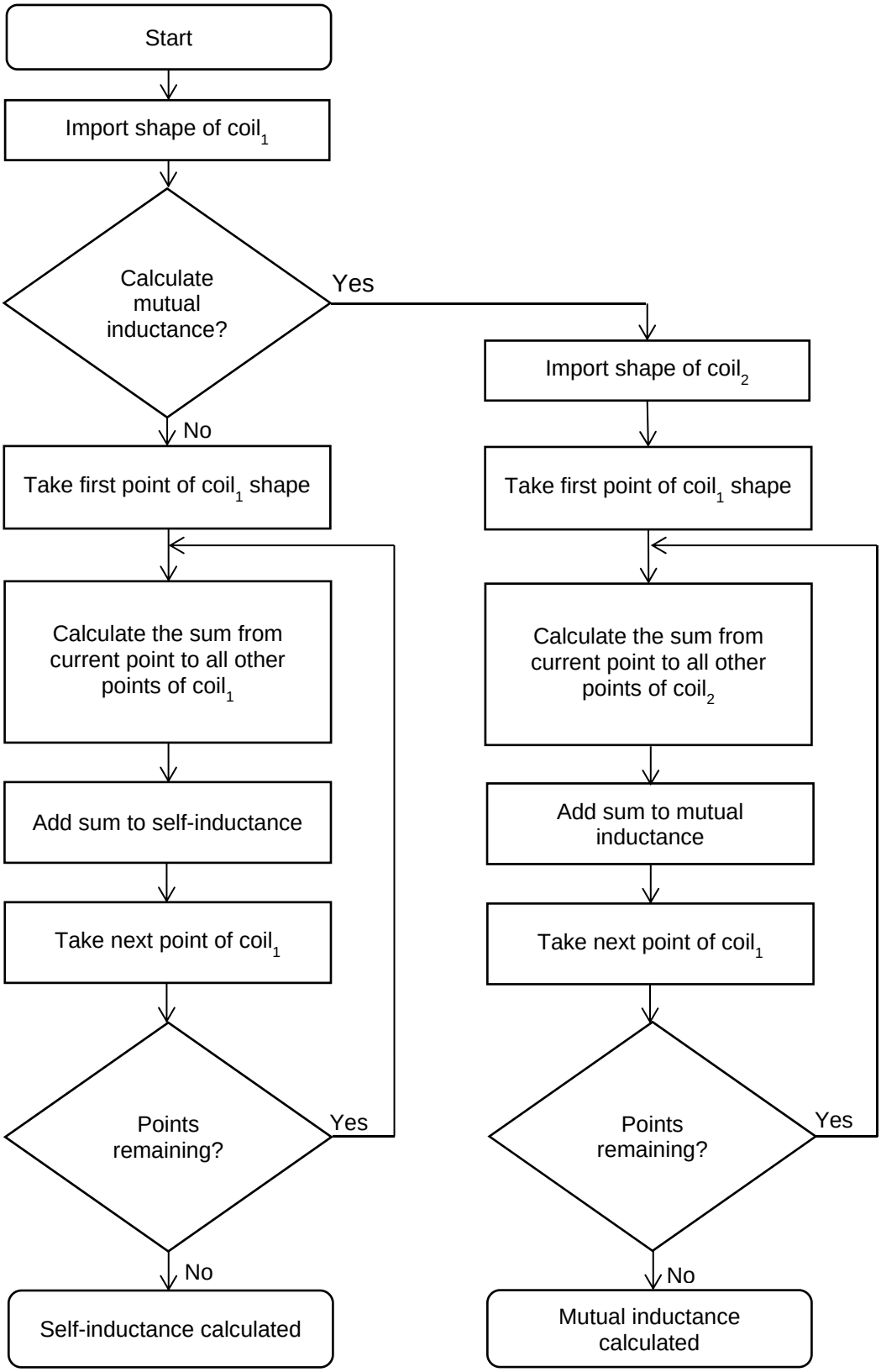
r_{ij} distance between two points

y constant that depends on distribution of current in the wire

Equation D-2: Neumann formula

The formula cannot be solved for all coil shapes. Due to that a finite element analysis based on the formula was implemented in Mathematica®.

Depending on whether the integral is used to sum the distances within a single coil or between two separate coils, the self-inductance (L) or the mutual inductance (M) is calculated.



Equation D-3: Flow chart of finite element analysis based on Neumann formula

To be able to import a coil shape a parts (.prt) file was defined describing the node coordinates of the shape. Each entry of a parts file has the following format:

- type x1, y1, z1, direction xc, yc, zc
- type = "L" for a line and type = "A" for a circular arc
- x1, y1, z1 are the x, y, z-coordinates of the start point of the sub-shape
- direction = "X" for a line
- direction = "A" for an arc running anticlockwise from its start point or direction="C" for clockwise
- xc, yc, zc are the coordinates of the centre point of a circular arc. If the sub-shape is a line then xc=0, yc=0, zc=0

The end point of each sub-shape is taken to be the start point of the next sub-shape. To provide the final end point of the whole coil, the last sub-shape in the file must be a line whose coordinates are the last point of the coil. Sub-shapes in the file must occur in the same sequence as sub-shapes forming the overall antenna coil and these must be in order from start connection point to end connection point. The coil may be traversed in either direction, because the direction of arcs must be specified.

From this file a matrix of coordinates of nodes of finite elements along the antenna coil is generated. The following is an example for a simple rectangular coil of 25mm x40mm with a single turn:

Table D-1: Parts file for 25mm x 40mm single turn rectangular coil

type	x1	y1	z1	direction	xc	yc	zc
L	1.0	-12.5	0	X	0	0	0
L	20.0	-12.5	0	X	0	0	0
L	20.0	12.5	0	X	0	0	0
L	-20.0	12.5	0	X	0	0	0
L	-20.0	-12.5	0	X	0	0	0
L	-1.0	-12.5	0	X	0	0	0

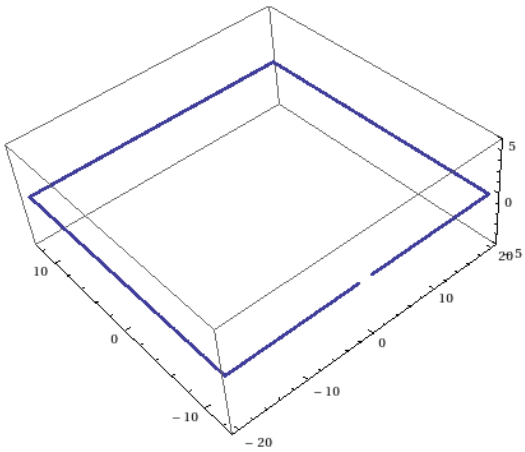


Figure D-15: Plot of finite element points generated from example parts file

The defined parts file is versatile enough to define very complex coil shapes. The following plot represents the coil of a real life PICC antenna as it can be found in many smart cards:

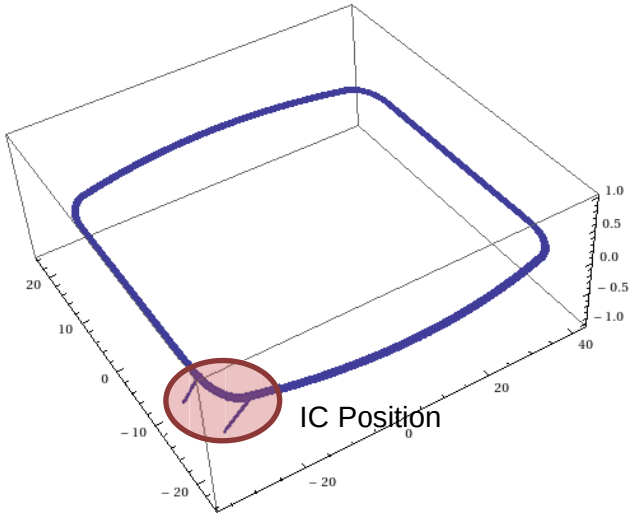


Figure D-16: Plot of finite element points from PICC antenna

To ensure the accuracy of the finite element analysis various sample measurements on existing PCB antenna coils were taken. For the measurement a calibrated Rohde&Schwarz Network Analyser model ZVR with a frequency range from 9kHz to 4GHz was used.

For the calculation, the distance between the finite element nodes (s) was changed to evaluate the best compromise between speed and accuracy.

Table D-2: Test results of self-inductance calculation

Coil	Measured self-inductance [nH]	s [mm]	Calculated self-inductance [nH]	Deviation
Test coil1	665.6	0.5	567.9	14.7%
		0.2	613.1	7.9%
		0.1	647.3	2.8%
Test coil2	1625.4	0.5	1449.0	10.9%
		0.2	1555.4	4.3%
		0.1	1636.6	-0.7%
Test coil3	5201.9	0.5	4972.0	4.4%
		0.2	5115.0	1.7%
		0.1	5227.2	-0.5%

Decreasing the distance between points below 0.1mm is not practical due to long calculation times. 0.1mm was chosen as a reasonable compromise for coil sizes up to 5uH, which covers the typical range for 13.56MHz RFID systems.

To verify the mutual inductance calculation, measurements were taken by another HID Global engineer using an HP 4263A LCR Meter at 100kHz measurement frequency.

For the test two 70mm square coils with a single turn were used and concentrically placed on top of each other in different axial separations.

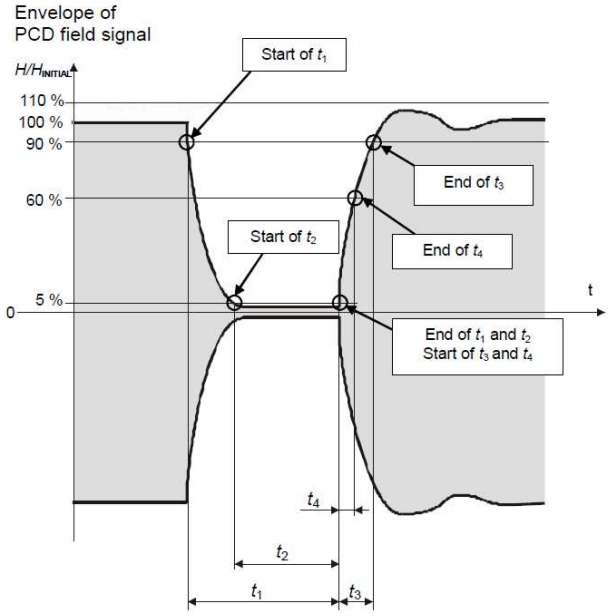
Table D-3: Test results of mutual inductance calculation

Axial separation [mm]	5	10	15	20	25	30	35	40	50
Measured mutual inductance [nH]	97.7	69.0	51.7	40.2	31.9	26.2	21.6	18.1	14.9
Calculated mutual inductance [nH]	108.0	73.3	54.6	42.4	33.8	27.4	22.5	18.6	15.6
Deviation	9.5%	5.9%	5.3%	5.2%	5.6%	4.4%	4.0%	2.7%	4.5%

Calculations have shown that convergence of the results with different point spacing is much better for mutual inductance, than for self-inductance. 0.1mm again was chosen as an acceptable compromise.

Appendix E. Quality Factor of PCD Antennas

The limits for the quality factor are given by the definition of the modulation waveforms in the standard. The parameter is not explicitly quoted but can be deduced approximately. The worst case is for the ISO/IEC14443 Type A transmit modulation, which is 100% ASK and the fall and rise times of the carrier envelope are defined.



Equation E-4: ISO/IEC14443 type A modulation pause at 106kbps (source: [ISO01])

Referring to the graph, the standard defines the following limits on times t1 and t2:

Table E-4: Limits t1 and t2 for ISO/IEC14443 type A pause

Time	Condition	Min.	Max.
t1		2.0 µs	3.0 µs
t2	t1>2.5 µs	0.5 µs	t1
	t1≤2.5 µs	0.7 µs	

For an exponential decay of a damped resonant waveform, the quality factor is equal to the number of cycles in the time taken for the envelope to decay by a factor of $e^{-\pi}$ (0.04 or roughly from 100 % to 5 %).

This allows Q to be estimated from the carrier frequency and the fall time (t1 – t2) using the formula

$$Q = f_c(t_1 - t_2)$$

f_c carrier frequency

Equation E-5: Quality factor based on exponential decay

Using this formula the following limiting values for the quality factor were calculated:

t1 – t2 (µs)	Q
1.3	18
2.5	34

Equation E-6: Limits of quality factor for a PCD

Statement of Authorship/

Selbstständigkeitserklärung

I hereby declare that this diploma thesis has been composed by myself and describes my own work, unless otherwise acknowledged in the text.

All references and external sources of information have been specifically acknowledged and have been quoted verbatim.

This thesis has not been submitted in any previous application for a degree.

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Linz, 2.10.2014

Hans-Jürgen Pirch