Christian Piller, BSc

Active Load Modulation
Development of a Test Bench for
Proximity Coupled Devices

MASTER'S THESIS

to achieve the university degree of

Master of Science

Master's degree programme: Electrical Engineering

submitted to

Graz University of Technology

Supervisor

Ass.Prof. Dipl.-Ing. Dr.techn. Peter Söser

Institute for Electronics

Dipl.-Ing. Stephan Rampetzreiter, Infineon Technologies Austria, DC Graz
Dipl.-Ing. Andreas Wörle, Infineon Technologies Austria, DC Graz

Graz, January 2016

AFFIDAVIT

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

Date

Signature

Active Load Modulation
Development of a Test Bench for Proximity Coupled Devices

Christian Piller, BSc.

January 2016

Abstract

In recent times RFID has seen an incredible ascension, not only in availability and usability but also in public perception. This is also proven by the enormous growth in the contactless payment sector. However, standardization institutes are already lagging behind and are struggling to keep up with proper methods to represent real-world applications properly. Active load modulation is becoming more and more relevant due to limiting factors of traditional passive load modulation, such as decreasing transmission quality or the diminishing of available power for the transmission of data between readers and transponders due to smaller antenna sizes, batteries or metal housings.

In the course of this thesis, the different standards shall be shown. An existing actively modulating PICC on the basis of the EMV-TEST PICC V2.1 shall be utilized as a new reference PICC, in order to build and test a fully functional test bench as a proof-of-concept. The test bench shall be able to properly evaluate the limits of a reader - transponder system. The different possibilities to synchronize the readers RF field with the transponders RF field are examined and a system being able to lock the phase of the transponder signal onto the reader signal is established. Furthermore an evaluation software is implemented and exhibited to determine the actual amplitude and phase.

Zusammenfassung

RFID sah in jüngster Zeit einen unglaublichen Aufstieg, nicht nur in ihrer Verfügbarkeit und ihrer Anwendungsfreundlichkeit, sondern auch in ihrer öffentlichen Wahrnehmung. Dies wird auch belegt durch den enormen Zuwachs im kontaktlosen Payment Sektor. Standardisierungseinrichtungen hinken diesem Wachstum bereits hinterher und sind bemüht passende Methoden zu entwickeln um Applikationen der realen Welt sachgerecht zu repräsentieren. Aktive Last-Modulation wird mehr und mehr relevant auf Grund limitierender Faktoren traditioneller passiver Last-Modulation, wie abnehmende Übertragungsqualität, oder die Verringerung der zur Verfügung stehenden Leistung bei der Übertragung von Daten zwischen Readern und Transpondern aufgrund kleinerer Antennen, Akkus oder Metalgehäusen.

Im Rahmen dieser Arbeit werden die unterschiedlichen Standards beleuchtet. Eine bereits existierende aktiv-modulierende PICC, auf Basis des EMV-TEST PICC V2.1 soll als Referenz-PICC genutzt werden, um eine voll-funktionstüchtige Test-Bench, als Proof-of-Concept, zu erstellen und zu testen. Diese Test-Bench soll in der Lage sein, die Limitierungen eines Reader-Transponder Systems korrekt zu evaluieren. Unterschiedliche Möglichkeiten zur Synchronisierung eines Transpondersignals mit einem HF Reader-Feld werden untersucht und ein System, welches es erlaubt, die Signal-Phase des Transponders auf die Signal-Phase des Readers zu locken, wird etabliert. Zudem wird eine Evaluierungs-Software implementiert, um die aktuellen Phasen- und Amplitudenverhältnisse festzustellen.

Acknowledgments

Ich möchte an dieser Stelle meine Dankbarkeit dem Unternehmen Infineon Technologies Austria AG aussprechen, welche mir die Möglichkeit gab, diese an Themen breitgefächerte Masterarbeit durchzuführen. Speziell möchte ich hierbei meinen Betreuern Stephan Rampetzreiter und Andreas Wörle danken, die mir stets mit Rat zur Seite standen und mir in kniffligen Momenten eine weitere bildliche Tür öffnen konnten. Zum Abschluss danke ich noch Herrn Ass.Prof. Dipl.-Ing. Dr.techn. Peter Söser der TU Graz für seine Tätigkeiten als Mentor und Gutachter. Ein Dankeschön möchte ich auch Schoasch und Ivan für ihre Freundschaft und Unterstützung aussprechen.

Danke Mama und Papa für das ständige Antreiben, Barbara für das offene Ohr und meiner Monisia dafür, dass es sie gibt. Ohne euch wäre vieles nicht möglich oder nur halb so schön gewesen. Danke.

Christian

Contents

1 List of Terms **3**

2 Introduction **5**

3 Proximity Coupling RFID Systems **6**
3.1 PICC - Proximity Integrated Circuit Card 7
3.2 PCD - Proximity Coupling Device 8
3.3 System Interaction 8
3.3.1 Resonance 8
3.3.2 Power Supply of the PICC 9
3.3.3 Load Modulation 12
3.4 Baseband Coding 14
3.4.1 PCD to PICC in Proximity Coupling Systems 14
3.4.2 PICC to PCD in Proximity Coupling Systems 14
3.5 Principles of Digital Modulation 16
3.5.1 Modulation: PCD to PICC 17
3.5.2 Modulation: PICC to PCD 18
3.6 Demodulation 26
3.6.1 Demodulation of Load Modulation 26

4 Active Load Modulation **28**
4.1 Motivation 28
4.2 Principles of Active Load Modulation 30
4.3 Testing against Standards 33
4.3.1 Context 33
4.3.2 Introduction to Contactless Standards 34
4.3.3 Different Standards, Different Scopes 43
4.3.4 Relationship between EMV and ISO/IEC Specifications 43
4.3.5 ISO/IEC 14443 and ALM 46

5 Components of the Test Bench **48**
5.1 RF Current Source for Active Load Modulation 50
5.1.1 Motivation 50

5.1.2 Proposed Circuitry . . . 51
5.1.3 Circuitry Improvements . . . 54
5.1.4 Concluding Thoughts . . . 57
5.2 Carrier/Clock Recovery and Synchronization . . . 58
5.2.1 Signal Acquisition . . . 58
5.2.2 Fundamentals of Synchronization . . . 60
5.2.3 Clock Recovery Circuit . . . 63
5.3 PICC Emulation . . . 69
5.3.1 Proposed PCD Reception Tests . . . 69
5.3.2 Realization via Vector Signal Generator . . . 72
5.4 Evaluation Software . . . 83
5.4.1 Hilbert Transform - Hilbert Transformer . . . 83
5.4.2 Implementation . . . 86
5.4.3 Discussion of Proposed Methods . . . 105

6 Verification regarding ISO/IEC 14443 107
6.1 Test Setup . . . 107
6.2 Calibration Steps . . . 108
6.3 Measurement and Evaluation . . . 110
6.3.1 PCD Reception Test Case 2: Type A, 106 kbit/s . . . 110
6.3.2 PCD Reception Test Case 3: Type A, 106 kbit/s . . . 112
6.3.3 Test Case 5° Sweep: Type A, 106 kbit/s . . . 114
6.4 Discussion . . . 119

7 Conclusion and Outlook 120

Bibliography 122

Chapter 1

List of Terms

ALM	Active Load Modulation	28
AM	Amplitude Modulation	13
ASK	Amplitude Shift Keying	16
AWG	Arbitrary Waveform Generator	48
BBG	Baseband Generator	73
BPSK	Binary Phase Shift Keying	16
BP	Bandpass	88
CMR	Common Mode Rejection	39
DC	Direct Current	51
DIN	Deutsches Institut für Normung	46
DFT	Discrete Fourier Transform	95
DSB	Dual Sideband Modulation	31
DUT	Device Under Test	94
EMF	Electromotive Force	28
EMVCo	Europay International, Mastercard and Visa Contactless	38
etu	Elementary Time Unit	69
FFT	Fast Fourier Transform	37
FSK	Frequency Shift Keying	14
GPIB	General Purpose Interface Bus	73
HF	high-frequency	16
HHB	Helmholtz Bridge	35
IEEE	Institute of Electrical and Electronics Engineers	73
IEC	International Electrotechnical Commission	5
ISO	International Organization for Standardization	5
IC	Integrated Circuit	51
JIS	Japanese Industrial Standard	40
k	coupling factor	29
kbit/s	kilo bits per second	28
LDO	Low Dropout Regulator	65

LMA Load Modulation Amplitude 37
NRZ Non-Return-to-Zero Encoding 14
M Mututal Inductance 29
MNO Mobile Network Operator 40
MOSFET Metal Oxide Semiconductor Field Effect Transistor 51
MS Modulation State 92
NFC Near Field Communication 33
OOK On-Off Keying 17
PCB Printed Circuit Board 34
PCD Proximity Coupling Device 7
PICC Proximity Integrated Circuit Card 6
PLL Phase Lock Loop 27
PLM Passive Load Modulation 28
PM Phase Modulation 13
PSD Power Spectral Density 96
PSK Phase Shift Keying 14
QPSK Quarterny Phase Shift Keying 23
RefPICC Reference Proximity Integrated Circuit Card 35
RF Radio Frequency 21
RFID Radio Frequency Identification 5
RX Receive 70
SCPI Standard Commands for Programmable Instruments 73
SD Storage Device 29
SIM Subscriber Identity Module 29
SMA SubMiniature Version A 51
STFT Short-Time Fourier Transformation 105
TX Transmit 94
VCO Voltage-Controlled Oscillator 61
VLMA Voltage Load Modulation Amplitude 70
WG8 Working Group 8 46

Chapter 2

Introduction

Radio Frequency Identification (RFID) systems are being used in a huge number of applications such as payment (credit cards), ticketing (public transport and events), access control (company card) and identity verification (ePass, eID). The following work is referring on inductively coupled RFID systems operating at a carrier frequency of 13.56 MHz which are primarily covered by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standards 14443[1], 15693, 18000-3 and 18092.

The majority of applications, mentioned above, operate in accordance with ISO/IEC 14443 standardizations. These standards were designed not only, but also for high security communication with transponders with ID1[2] sized (smart card) transponders at proximity distances usually up to 15 cm. According transponders are powered by an electromagnetic field and use passive load modulation with subcarrier, a double-sideband modulation scheme, to transmit data back to a reader producing the electromagnetic field.[21]

[1] International standard that defines proximity coupling smart cards used for identification, and the transmission protocols for communicating with it.

[2] Different card/antenna sizes with up to six different antenna classes, defined by *ISO/IEC 7810 Identification cards - Physical characteristics* , an international standard that defines the physical characteristics for identification cards.

Chapter 3

Proximity Coupling RFID Systems

The two essential components of an RFID system are the reader device and the transponder. ISO/IEC 14443 defines proximity coupling RFID systems as devices, coupled by the reader's generated electromagnetic field, with a carrier frequency of 13.56 MHz. ISO/IEC 14443 refers to such a transponder as Proximity Integrated Circuit Card (PICC). These devices are able to communicate with the reader device over distances of up to $7-15\,\mathrm{cm}$ [20]. This range is well inside the near field of the electromagnetic field of the reader which can therefore be considered as a time varying magnetic field.

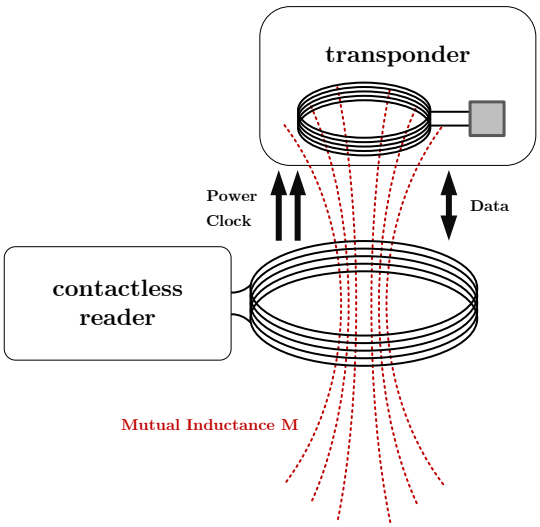


Figure 3.1: An inductively coupled RFID system uses mutual magnetic coupling to transfer power and data.

Proximity coupling RFID systems belong to the class of systems that employ inductive coupling, not only for communication, but also to supply the mostly passive transponders with the energy necessary for the device to operate. Figure 3.1 shows the basic configuration of a proximity coupling RFID system.

The fundamental components of such a system will be explained in terms of their electrical representation in the following sections.

3.1 PICC - Proximity Integrated Circuit Card

The simplest form of a transponder or PICC consists of an antenna coil and a chip. The antenna coil provides the interface to the alternating magnetic field generated by the reader, or the Proximity Coupling Device (PCD), at a transmission frequency of 13.56 MHz. The chip comprises of several digital and analogue functions in order to function properly. Figure 3.2 shows a simplified equivalent circuit of a PICC.

The antenna of the PICC is depicted as a (secondary) inductor L_2 with a series resistor R_2. To be able to induce voltages high enough from the PCD into the PICC's antenna, its resonance frequency f_{res} is tuned to a value close to the carrier frequency of the PCD magnetic field. In order to accomplish this, a tuning capacitor C_{tune} is introduced. The chip in its simplest form is represented as a capacitor C_{chip} forming a parallel circuit with a resistor R_{chip}. The majority of these components are either nonlinear, frequency dependent or even both.

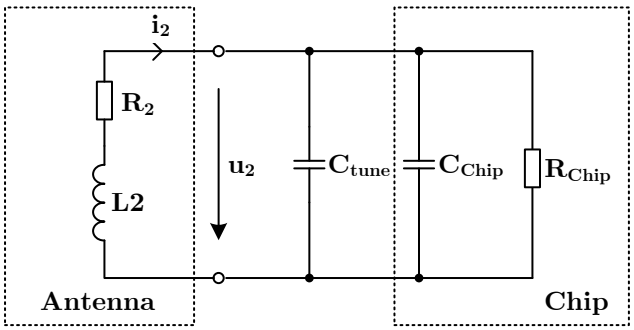


Figure 3.2: Simplified equivalent circuit of a PICC [28]

3.2 PCD - Proximity Coupling Device

The simplest electrical equivalent of a reader or PCD is depicted in figure 3.3. The PCD consists of signal source along with an internal resistor in series R_i and an inductor L_1 in series to a resistor R_1 representing the antenna. To match the antenna to the source, between the two parts a matching network consisting of capacitors C_{ms} and C_{mp} is introduced. If matched accordingly, the load and the internal impedance of the signal source are equal. In this case, the maximum power is transferred from the source to the load. Note that with the matching circuit shown in figure 3.3 only matching at a specific frequency is possible. In case of systems according to ISO/IEC 14443, this will be the carrier frequency of 13.56 MHz.

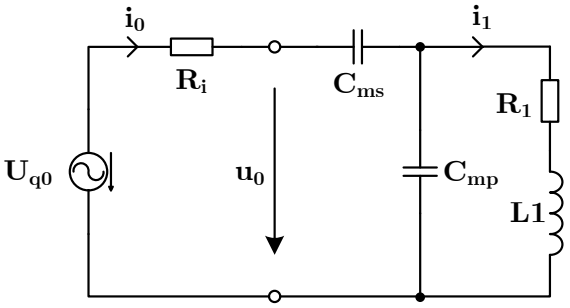


Figure 3.3: Simplified equivalent circuit of a PCD [28]

3.3 System Interaction

3.3.1 Resonance

By exposing a PICC to the alternating magnetic field of a PCD, a voltage u_i is induced into the coil L_2. This induced voltage provides the power supply for the PICC. The introduced parallel capacitor significantly improves the efficiency of the whole circuit, as it forms a parallel resonance circuit with a resonance frequency corresponding with the carrier frequency of the PCD[1].

[1] In reality (13.56 MHz) the selected resonance frequency is even a bit higher to minimize interfering influences.

The equation to form the resonance frequency based on figure 3.2 is:

$$f = \frac{1}{2\pi\sqrt{L_2 \cdot C_{tune}}} \tag{3.1}$$

C_{tune} can be even split up further into a parasitic part C_p and a parallel part C'_{tune}, $C_{tune} = C_p + C'_{tune}$. So considering this parasitic capacitor one would end up with:

$$C'_{tune} = \frac{1}{(2\pi f)^2 L_2} - C_p \tag{3.2}$$

3.3.2 Power Supply of the PICC

The following figure shows the equivalent circuit of the real PICC.

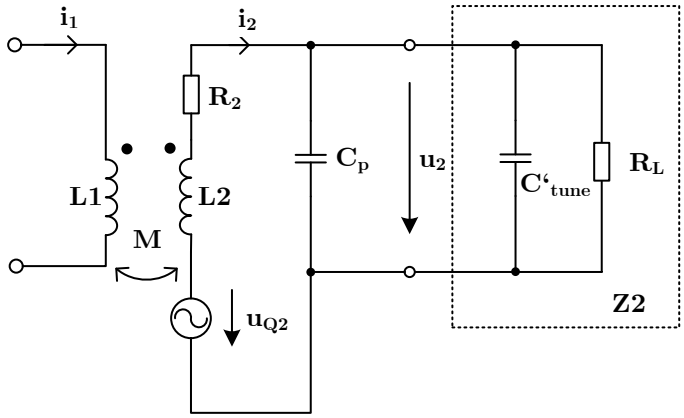


Figure 3.4: Equivalent circuit of magnetically coupled conductor loops

The induced voltage $u_i = u_{Q2}$ can be denoted as:

$$u_{Q2} = j\omega M i_1 \tag{3.3}$$

Equation 3.3 is the complex notation of the induced voltage due to *Faraday's law*, where $\omega = 2\pi f$ represents the angular frequency of the sinusoidal magnetic field and i_1 is the current through the PCD's coil. The mutual inductance M describes the coupling of two circuits via magnetic field. In this case L_1 and L_2 of both coils in reader and transponder are the determinants. In practice, this coupling factor is mostly influenced by the coupling factor k:

$$M = k \cdot \sqrt{L_1 L_2} \tag{3.4}$$

Using these equations one can obtain the following equation:

$$u_2 = u_{Q2} \frac{\frac{R_L}{1 + j\omega R_L (C_p + C'_{tune})}}{R_2 + j\omega L_2 + \frac{R_L}{1 + j\omega R_L (C_p + C'_{tune})}} \tag{3.5}$$

Regarding equation 3.3 and equation 3.4 and after some summarizing and simplification the equation reads as follows:

$$u_2 = \frac{j\omega k \cdot \sqrt{L_1 L_2} i_1}{1 + \frac{R_2}{R_L} - \omega^2 L_2 C_{tune} + j\omega \left(R_2 C_{tune} + \frac{L_2}{R_L} \right)} \tag{3.6}$$

So by looking at the non-complex version of equation 3.6 it is revealed [24]

$$u_2 = \frac{\omega k \cdot \sqrt{L_1 L_2} i_1}{\sqrt{\left(\omega R_2 C_{tune} + \frac{\omega L_2}{R_L} \right)^2 + \left(1 + \frac{R_2}{R_L} - \omega^2 L_2 C_{tune} \right)^2}} \tag{3.7}$$

and additionally keeping the current i_1, the resistors R_2 and R_L, as well as the inductance L_2 and mutual inductance M constant, an observation reveals following: By

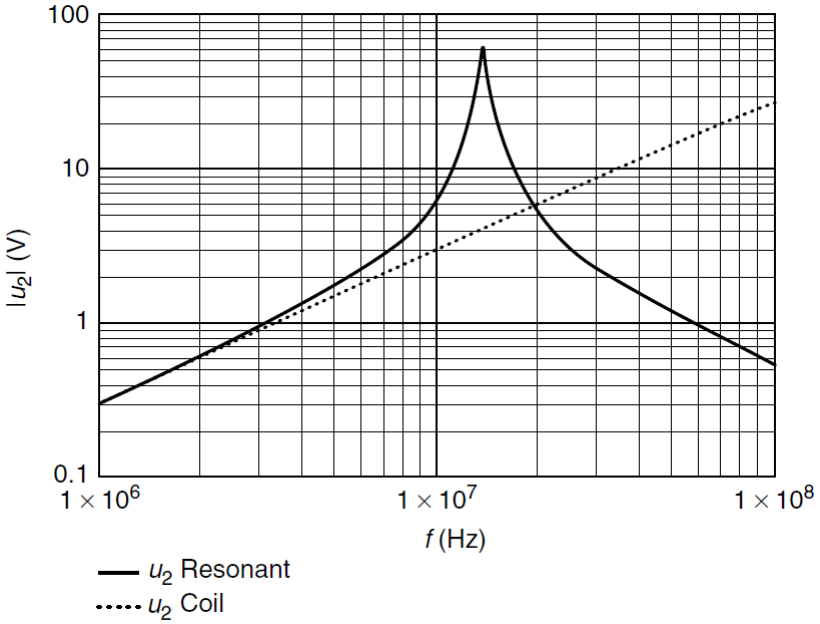


Figure 3.5: Transponder coil for a constant magnetic field strength H with resonance at $f_{res} = 13.56\,\text{MHz}$ [20]

.

reaching the resonance frequency the voltage u_2 in the resonant circuit reaches a maximum and becomes actually by the power of ten higher compared to a voltage in the existing coil alone. At resonance frequency, the denominator of equation 3.6 will reach its minimum, the current becomes only limited by the reactance, with the ohmic part becoming theoretically zero.

To better understand the interaction between the different parameters and their influence on the voltage u_2 the *quality factor*, or *Q-factor* is introduced, a measure for the voltage and current step-up in a resonant circuit at resonance [20]. For the circuit in figure 3.4 it's relatively easy to derive:

$$Q = \frac{1}{\frac{R_2}{\omega_{res} L_2} + \frac{\omega L_2}{R_{chip}}} \tag{3.8}$$

Equation 3.8 shows explicitly that both, for very high values of R_2 and very low values of R_L, the Q-factor tends towards zero. By implication, this means a very high Q-factor can be achieved by having a very low R_2 (representing a low antenna resistance) and very high R_L (corresponding to a low current consumption of the RFID chip). The voltage u_2 is proportional to the Q-factor, therefore the same can be applied and a very high voltage u_2 can be achieved.

3.3.3 Load Modulation

Inductively coupled systems use a *transformer-type coupling* between the coils of reader and transponder. If the resonant transponder antenna is located in the *near field* of the reader's transmitter antenna, the transponder can draw energy from the alternating magnetic field. The *near field* denotes the *"area from the antenna to the point where the electromagnetic field forms"* and can be calculated via $\frac{c}{2\pi f}$, with c as the speed of light and f as the frequency of radiation [20]. For a resonance frequency of $f_{res} = 13.56\,\text{MHz}$ this corresponds to approxiamtely 3.5 m.

So by being supplied by the magnetic field of the PCD, the PICC itself will produce a magnetic field, which due to *Lenz's law*[2] will have an effect on the current in the PCD antenna. This influence can be represented as a *transformed impedance* Z_T (see also [20] for a detailed remarks), an additional load in series of the antenna coil of the PCD.

Toggling a load on and off in the PICC antenna coil would then equally mean a change in this transformed impedance Z_T. This is equatable with the modulation of the voltage U_L present at the primary coil of the reader. Moreover, if this load is varied deliberately and controlled in time by a data stream, this data can thus be transferred from the PICC to the PCD. This specific way of transferring data is called *load modulation*. To make use of the data, a demodulation technique is needed to rectify the tapped signal on the reader's side.

The switching of an additional load in the transponder at a high frequency of f_{sub} leads to spectral lines $\pm f_{sub}$ around the transmission frequency f_{reader} of the reader. This frequency is also commonly referred to as *subcarrier*. So, load modulation with a subcarrier f_{sub} creates two modulation sidebands $\pm f_{sub}$ distant to the reader or *carrier* frequency.

The load modulation is now the most common procedure when it comes to data transmission from a PICC to PCD. The load on the PICC resonance circuit can be now everything from a resistor to a capacitance and all in-between. This allows for the influence - and therefore modulation - of both, magnitude (resistive) and phase (reactive) of the transformed transponder impedance Z_T. Normally, only two circuit parameters in the PICC are influenced by the data carrier, the load resistance R_L and the parallel capacitance C_2.

Ohmic Load Modulation

In ohmic load modulation, as shown in figure 3.6, a resistor R_{mod} is toggled on and off. This results in different ohmic loads. Toggling the additional resistor on, the resulting

[2] *"If an induced current flows, its direction is always such that it will oppose the change which produced it."*

ohmic load is lowered, leading also to a lower quality factor Q and thus a lower transformed impedance Z_T which corresponds to a reduction of the voltage step up due to resonance.

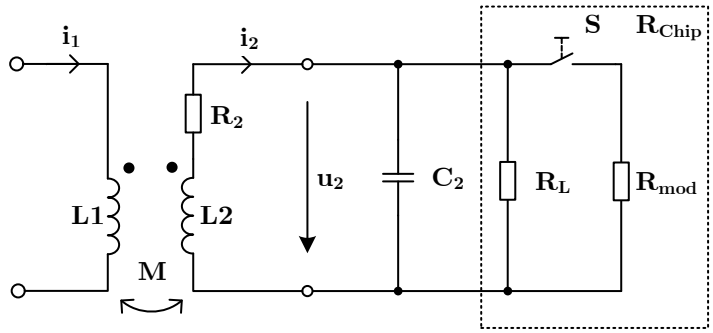


Figure 3.6: Ohmic load modulation (adapted from [28])

This appears as a change in magnitude and phase of the transformed transponder impedance and in the terminal voltage of the reader's antenna. The modulation of the magnitude of the field in order to transmit data is referred to as Amplitude Modulation (AM). The technique to transmit data by varying the phase of the carrier signal is referred to as Phase Modulation (PM). In reality the load is never truly resistive nor reactive, thus the result is always a combination of both AM and PM. Under the circumstance, that the PICC's resonance frequency is close to the PCD's carrier frequency, AM will be always the dominant part.

3.4 Baseband Coding

To transmit data from a PCD to a PICC and vice versa, RFID systems usually use different types of baseband codes. ISO 14443 however provides two types of baseband codes according to the direction of the communication and depending on the chosen communication interface type, respectively.

3.4.1 PCD to PICC in Proximity Coupling Systems

For the *downlink* these two types of baseband codes would be:

Non-Return-to-Zero Encoding (NRZ) code
Used almost exclusively with Frequency Shift Keying (FSK) and Phase Shift Keying (PSK) transponders, *Non-Return-to-Zero* code represents a binary 1 as a 'high' level and a binary 0 as a 'low' level of the present electrical signal. NRZ code is used by *Type B* transponders (figure 3.7).

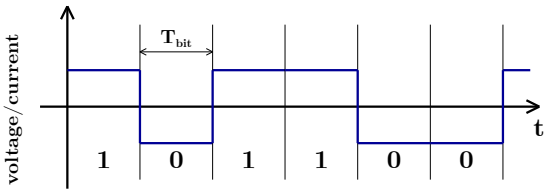


Figure 3.7: NRZ code (Non-Return-to-Zero)

Modified Miller code
Modified Miller is, as the name explains, essentially a modified version of the *Miller code*. A binary 1 is always represented in the same way: a negative pulse in the second half of a bit period. A binary 0 can be distinguished by two possible cases: a binary 0 following a binary 0, and a binary 0 following a binary 1. In the latter case no negative pulse is initiated, in the former case a negative pulse at the start of the bit duration of the second binary 0 is initiated.

These very short pulse durations ($T_{bit} >> t_{pulse}$) are the reason why the *Type A* communication interface utilizes *Modified Miller* encoding (figure 3.8).

3.4.2 PICC to PCD in Proximity Coupling Systems

For the *uplink* again two types of baseband codes are relevant. Transponders using *Type B* again generate their baseband signal using the NRZ coding procedure.

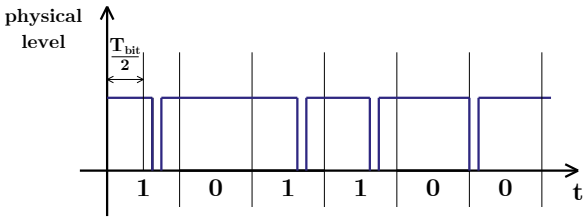


Figure 3.8: Modified Miller code

Type A transponders however use again a different procedure:

Manchester code

Somewhat similar to the *Miller code* it uses pulses (falling and rising edges) usually at the half of a bit period: a binary 0 is represented by a rising edge, a binary 1 by a falling edge. The pulses appear at the start of a bit period if similar binaries appear consecutively (figure 3.9).

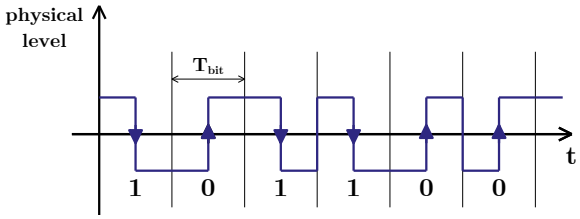


Figure 3.9: Manchester code

3.5 Principles of Digital Modulation

Modulation is the process of altering one or more signal parameters of a periodic, generally sinusoidal, carrier signal.

Furthermore the term *baseband signal* shall be introduced. The term describes the representation of binary digits in form of an electrical wave shape [25]. Generally, a baseband signal can be represented as a sequence of binary 0 or binary 1, represented by electrical pulses. The coding into these pulses is achieved in the frequency range of the transmitted signal and is therefore referred to as *baseband encoding*.

The process of modulation causes sidebands symmetrically around the carrier when observing the frequency domain[3]. Sidebands represent a band of frequencies containing power and consist of all Fourier elements of the modulated signal. The spectrum as well as the amplitude of the, lower and higher, sidebands are therefore affected not only by the spectrum of the baseband signal, but also by the chosen modulation procedure. Proximity coupling RFID systems (ISO 14443) use primarily digital modulation techniques like Amplitude Shift Keying (ASK) and Binary Phase Shift Keying (BPSK).

Proximity coupling RFID systems are represented by a PCD and a PICC and are, as shown in figure 3.1, inductively coupled systems. The reader (PCD) is generating the magnetic sinusoidal field and is thus representing the sinusoidal, high-frequency (HF) carrier. The carrier signal $s(t)$ can be described mathematically as follows:

$$s(t) = A(t) \cdot \cos\{(2\pi f(t))\, t + \varphi(t)\} \tag{3.9}$$

A ... signal amplitude

f ... signal frequency

φ ... signal phase

Equation 3.9 reveals three signal parameters possible to be altered according to the data to be transmitted. These three options simultaneously represent the three fundamental modulation procedures: *amplitude*, *phase* and *frequency modulation*. The latter two both originate from the the same type of modulation, the *angle modulation*, and are mathematically related to each other by $\frac{\mathrm{d}\varphi(t)}{\mathrm{d}t} = f(t)$.

In proximity coupling systems, linear modulation schemes are used to modulate the carrier with digital data. Consecutively, discrete values (symbols) are assigned to amplitude, phase and frequency of the carrier, as shown in the following table[4]:

[3] There are not always necessarily two sidebands, depending on the actual modulation procedure.

[4] Many textbooks use the angular frequency $\omega = 2\pi f$ instead of the actual frequency f.

Amplitude Shift Keying (ASK)	Phase Shift Keying (PSK)	Frequency Shift Keying (FSK):
$s(t) = A(t) \cdot \cos(\omega_0 t + \varphi_0)$	$s(t) = A_0 \cdot \cos(\omega_0 t + \varphi(t))$	$s(t) = A_0 \cdot \cos(\omega(t)\, t + \varphi_0)$

Table 3.1: mathematical description of ASK, PSK and FSK

3.5.1 Modulation: PCD to PICC

Amplitude Shift Keying (ASK)

Amplitude shift keying is the preferred modulation scheme used in proximity coupling RFID data transmission from a PCD to a PICC. The amplitude of the RF sinusoidal carrier is switched according to the to be transmitted data in the baseband. The baseband signal knows two distinct levels: low (LO) and a high (HI). This process, in its simplest form, is denoted as On-Off Keying (OOK). The amplitude is toggled between the two states of the baseband, effectively on and off.

A binary ASK such as the OOK can be characterized by *modulation index m* a parameter describing the ratio between amplitudes of the carrier signal's modulated and its unmodulated level.

$$m = \frac{A_{HI} - A_{LO}}{A_{HI} + A_{LO}} \cdot [100]\%. \tag{3.10}$$

The modulation index in standard ASK usually ranges from 0 to 100 %, whereas 100 % implicates one of the two amplitude levels to be zero and 0 % means no modulation.

Figure 3.10 depicts the PCD's magnetic field in the case of data transmission from reader to transponder regarding the prior mentioned ISO 14443 communication interface types:

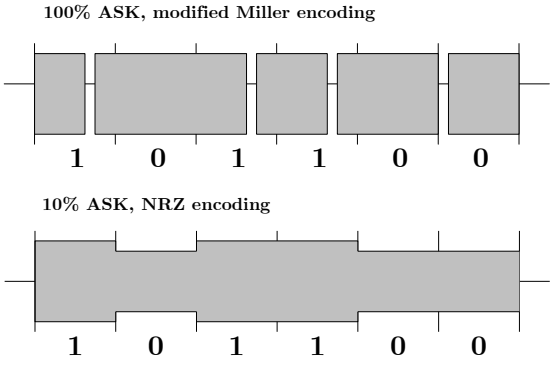


Figure 3.10: Downlink modulation procedures [3]

Mathematically, a modulation is a multiplication of a carrier signal and a data signal. In the case of OOK, an unipolar digital baseband signal, represented by two amplitude levels, and an RF sinusoidal carrier signal. OOK, with a modulation index of $m = 100\%$ would set the LO level of the baseband signal and therefore the modulated carrier signal alike, to zero:

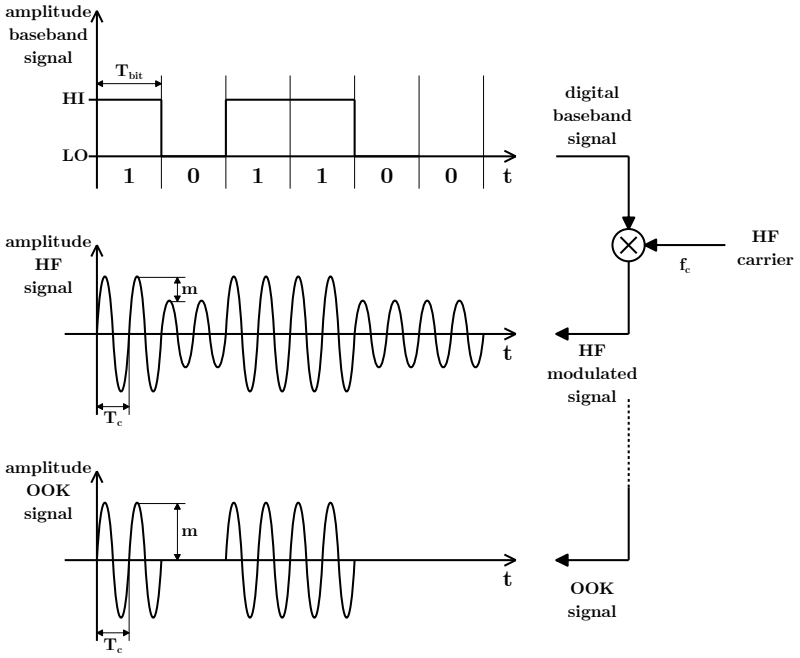


Figure 3.11: Binary ASK modulation and OOK modulation (adapted from [20])

3.5.2 Modulation: PICC to PCD

When it comes to transferring data from the PICC back to the PCD there is one glaring issue: the PICC is usually not generating its own carrier signal, it is utterly dependent on the sinusoidal magnetic field of the reader. The magnetic field is utilized as RF carrier signal.

The process in which the PCD's magnetic field is modulated by keying the electrical characteristics of the PICC has been described in section 3.3.3 and is denoted as *load modulation*. Depending on the type of load modulation, the appropriate electrical parameter is altered according to the data signal to be transmitted. Due to the physics of inductively coupled systems, the changes of the magnetic field are detectable in reader's electrical quantities like the voltage at or the current in the coil of the reader's an-

tenna. Hence, by demodulating one of these quantities the modulating data signal can be recovered.

As previously discussed in section 3.3.3, load modulation causes the simultaneous modulation in amplitude and phase of the PCD's magnetic field: the carrier signal. Considering equation 3.9 and table 3.1 the carrier signal can be denoted mathematically by

$$s(t) = A(t) \cdot \cos(2\pi f_c + \varphi(t)), \tag{3.11}$$

a combination of ASK and PSK. In the case of proximity coupling systems even as combination of *binary* ASK and *binary* PSK, as the transition happens commonly only between two states.

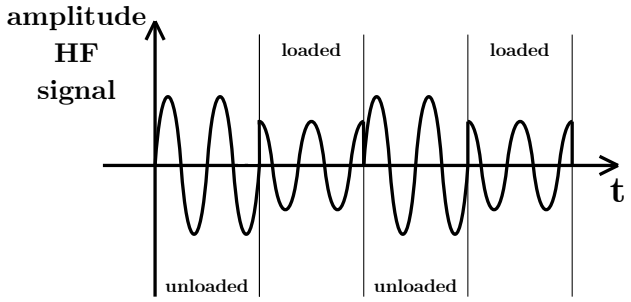
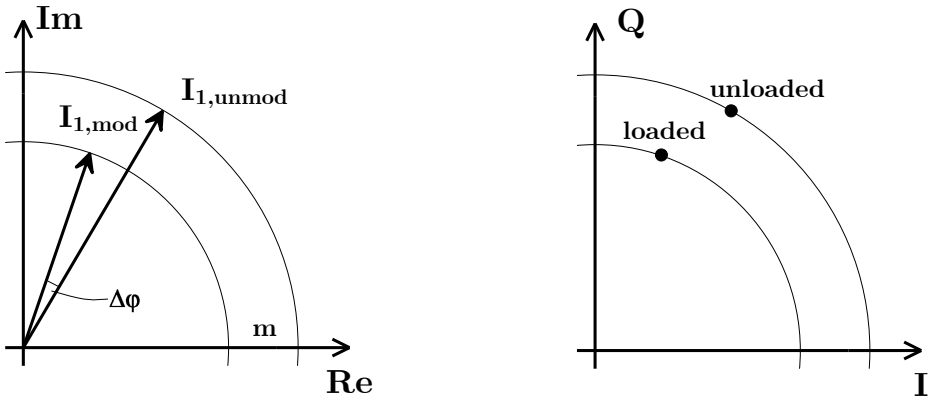


Figure 3.12: ASK and PSK present in a load modulated carrier signal

Figure 3.12 shows what a typical signal, modulated by a binary toggled load might look like, as denoted in equation 3.11: the binary states representing the *unloaded* and *loaded* state.

When there is a digital modulation procedure involved where, in the case of load modulation, a combination of ASK and PSK is given, *constellation diagrams* are used to analyze signals in relation to their modulating baseband signal in the complex plane. Constellation diagrams are used in digital communications and depict the possible amplitude and phase states of the modulated carrier signal and are therefore tantamount to the information of how many symbols can be transmitted. Such diagrams are depicting how many different amplitude levels and phase states the modulated carrier has and therefore how many symbols are transmittable using this carrier. Its analogous pendent would be the *phasor diagram*.

Regarding load modulation, the primary current, $i_1(t)$ through the PCD's antenna coil can be depicted as phasor, which translates also into an according constellation diagram.



(a) Phasor diagram of current $\underline{I}_1$

(b) Constellation diagram of current $\underline{I}_1$

Figure 3.13: Relation between phasor and constellation diagram for load modulation

Due to the nature of digital modulation and baseband signals alike, the first step however is to depict the time domain signal $s\,(t)$ from equation (3.11) in its complex notation, using *Euler's Identity*:

$$\begin{aligned} s\,(t) &= A\,(t) \cdot \cos\left(\omega_0 t + \varphi\,(t)\right) = \\ &= \Re\{\underbrace{A\,(t) \cdot e^{j(\omega_0 t + \varphi(t))}}_{analytic\ signal\ \underline{s}_a(t)}\} \end{aligned} \tag{3.12}$$

To be able to simultaneously and separately modulate a signal's amplitude and phase it is of practical use to separate the signal into another set of independent orthogonal components. Starting from equation 3.12 a trigonometrical relation

$$\sin(\alpha + \beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta) \tag{3.13}$$

combined with f_C being the carrier frequency and $2\pi f_C(t) = \omega_C(t) \equiv \omega_C$ leads to the following equation:

$$\begin{aligned} A(t) \cdot \sin\left(\omega_C t + \varphi(t)\right) = \\ A(t) \cdot \sin(\omega_C t)\cos(\varphi(t)) + A(t) \cdot \cos(\omega_C t) sin(\varphi(t)) \end{aligned} \tag{3.14}$$

Equation 3.14 can be split into two parts:

$$s_I(t) = A(t) \cdot \cos(\varphi(t)) \sin(\omega_C t) \tag{3.15}$$

$$s_Q(t) = A(t) \cdot \sin(\varphi(t)) \cos(\omega_C t) \tag{3.16}$$

Equations 3.15 and 3.16 mathematically describe the signal's in-phase component, $s_I(t)$, and its quadrature component, $s_Q(t)$, whose phase is shifted by 90° ($\pi/2$) in relation to the carrier signal $sin(\omega_C t)$.

The complex signal in equation 3.12 is also referred to as *analytic signal* $\underline{s}_a(t)$, which is utilized in the complex time domain. The analytic signal $\underline{s}_a(t)$ is a representation of the baseband as well as the carrier of the signal:

$$\begin{aligned} \underline{s}_a(t) &= \underbrace{A(t) \cdot e^{j\varphi(t)}}_{baseband} \cdot \underbrace{e^{j\omega_C t}}_{carrier} \\ \underline{s}_a(t) &= [\underbrace{A(t) \cdot \cos(\varphi(t))}_{in-phase} + j \cdot \underbrace{A(t) \cdot \sin(\varphi(t))}_{quadrature\ phase}] \cdot e^{j\omega_C t} \end{aligned} \tag{3.17}$$

Equation 3.17 shows the relation between the analytic signal $\underline{s}_a(t)$ and the in-phase component, $s_I(t)$, and its quadrature component, $s_Q(t)$. For a better understanding further simplifications can be made:

$$I(t) = A(t) \cdot cos(\varphi(t)) \tag{3.18}$$

$$Q(t) = A(t) \cdot sin(\varphi(t)) \tag{3.19}$$

Equations 3.18 and 3.19 show the so-called *I (in-phase)* and *Q (quadrature)* components of the signal independent from the carrier signal, also depicted in figure 3.14 illustrating the basic concept of an I/Q modulator.

The baseband signal I is multiplied with a sinusoidal Radio Frequency (RF) carrier signal, the baseband signal Q with the same RF carrier signal shifted in phase by 90° ($^{\pi}/_{2}$). This procedure is known as *quadrature upconversion.* The I/Q modulator directly builds the sum of the I and Q branches, $s_I(t)$ and $s_Q(t)$. The amplitudes and phases in I and Q data can be influenced to create signals of any magnitude and phase on the modulator's output. Flexibility and simplicity of an I/Q modulator lead to a rather popular use in practice. [30]

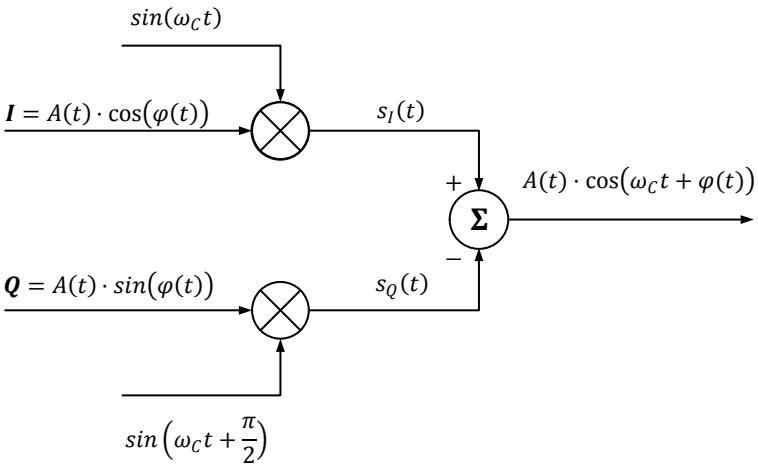


Figure 3.14: Concept of a simple *I/Q Quadrature-Modulator*

With I and Q the phasor of the analytic signal is defined. Its length is represented by the amplitude A (equation 3.20) and its angle is represented by the phase φ (equation 3.21). The carrier cannot be seen directly, but is considered by the phasor's actual rotation with the angular carrier frequency of ω_C.

$$A(t) = \sqrt{(I(t))^2 + (Q(t))^2} \tag{3.20}$$

$$\varphi(t) = \arctan \frac{|Q(t)|}{|I(t)|} \tag{3.21}$$

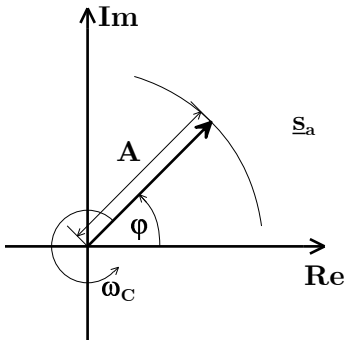


Figure 3.15: Phasor diagram of an analytic signal $\underline{s}_a(t)$

By varying the I and the Q component of $s(t)$ the carrier signal can take every phase and amplitude state. The figure exemplified above is also known as *Quarterny Phase Shift Keying (QPSK)*.

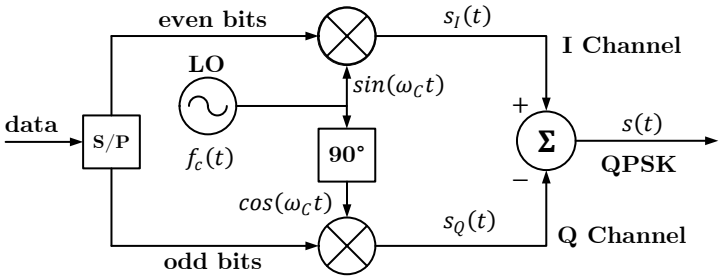


Figure 3.16: QPSK modulator (adapted from [30])

Figure 3.16 is based on the findings made before and subsequently leading to figure 3.14. The bit stream of the baseband signal is split into two branches (even and odd) and then fed into the IQ modulator. The signals in both channels, I and Q, are BPSK modulated. The two resulting BPSK modulated signals, $s_I(t)$ and $s_Q(t)$, result ultimately in a QPSK modulated carrier signal. Therefore, the QPSK modulation scheme leads to four discrete phase states of the modulated carrier.

Phase Shift Keying (PSK)

In PSK methods, symbols are represented by discrete phase states of the carrier signal. Contrary to ASK, the baseband information is present in the phase of the carrier, φ. Binary phase shift keying represents the simplest PSK modulation scheme, with two discrete phase states representing a high and low state of the baseband signal.

This can be mathematically described as a multiplication of a bipolar baseband with an RF sinusoidal carrier signal, resulting in a phase shift of 180° (π) between the two states of the carrier signal. The absolute phase is dependent on the carrier's initial phase.

As mentioned in section 3.5.2, digital modulation signals can be represented in the complex plane as a sum of an in-phase component I and a quadrature component Q and as a result depicted in constellation diagrams. Each point in the complex I/Q plane represents a discrete state of phase and amplitude of the modulated carrier. The transition into each state can be achieved by varying amplitudes of these previously introduced I and Q components. This allows for the creation of any modulation signal just by a combination of two amplitude-modulated signals.

Regarding to ISO 14443 standard two communication interfaces have been proposed and accepted. Both use different approaches in their procedures to transfer data between

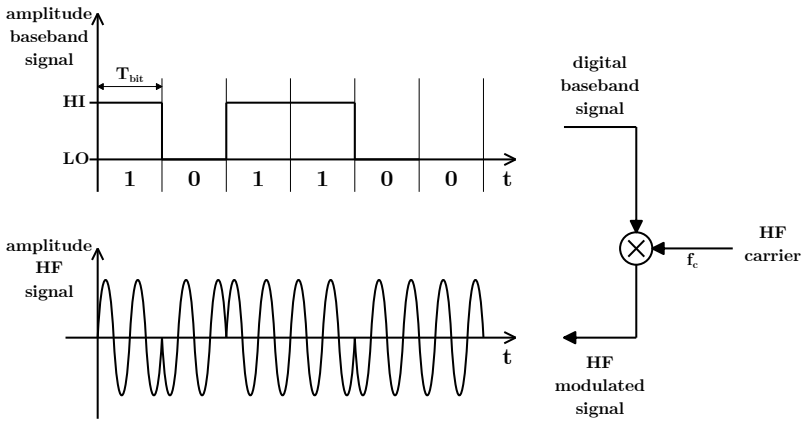


Figure 3.17: BPSK modulation of sinusoidal RF carrier signal (adapted from [20])

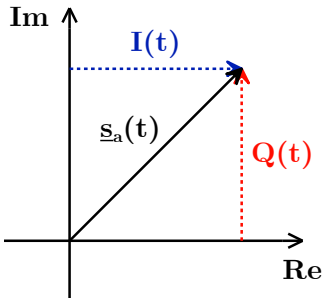


Figure 3.18: Phasor representation of an analytic signal

reader and the transponder and have their place in ISO 14443 commonly referred as to *Type A* and *Type B*. While smart cards only need to support one of these communication procedures, readers compliant to ISO 14443 must be able to handle both communication interfaces equally well. Readers switch (poll) between the communication procedures regularly while being idle, however not during an ongoing communication. [20]

ISO 14443 Communication Type A

For the data transfer from PCD to PICC, *Type A* smart cards utilize ASK modulation with a modulation depth m of 100% along with *modified Miller* coding (cf. figure 3.8). To ensure a steady power supply to the card, gaps between commands of a maximum 2 to 3μs (*Type A - gaps*) are crucial. The transient behavior in these blank intervals underlie strict standard requirements and are defined in ISO 14443.

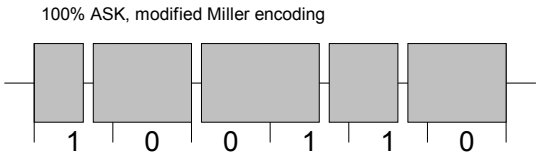


Figure 3.19: PCD to PICC, Type A modulation scheme [3]

For the data transfer from PICC to PCD, load modulation with subcarrier is used. The subcarrier frequency, f_{sub}, of 847.5 kHz (derived from 13.56/16 MHz) is modulated by On-Off Keying using a Manchester coded data stream. [20]

ISO 14443 Communication Type B

For the data transfer from PCD to PICC, *Type B* smart cards utilize ASK modulation with a modulation depth m of 10%. Other than for *Type A*, NRZ coding is used. Again, transient behavior in logical 0/1 transitions underlie standard requirements and are defined in ISO 14443.

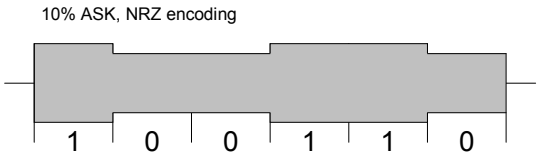


Figure 3.20: PCD to PICC, Type B modulation scheme [3]

For the data transfer from PICC to PCD, as well as for Type A, load modulation with a subcarrier, f_{sub}, of 847.5 kHz(13.56/16 MHz) is used. To modulate the subcarrier, BPSK using the NRZ coding is utilized. This means a 180° phase shift of the subcarrier [20].

3.6 Demodulation

Demodulation is the procedure to reclaim the data, carried by a baseband signal from a modulated carrier signal. From a technical point of view, modulation is a *baseband-passband transform*: The spectrum of the modulating signal is shifted from its baseband to the frequency range of the carrier signal. Consequently, demodulation is used to shift the passband signal to baseband.

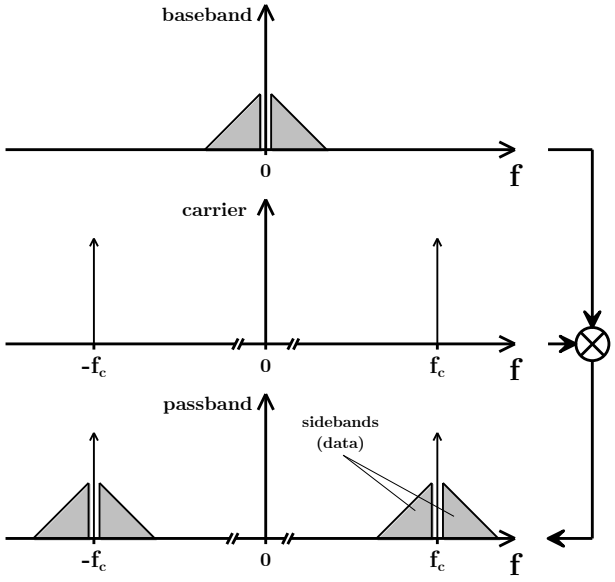


Figure 3.21: Baseband-passband transform of a sinusoidal carrier signal

3.6.1 Demodulation of Load Modulation

The previous sections revealed the nature of load-modulated signals, as being a compound of ASK and PSK of the PCD's antenna coil voltage[5] for the demodulation process. This enables two possible demodulation schemes: demodulation of the amplitude or the phase.

Common RFID readers detect load-modulated signals using a non-coherent amplitude demodulation of e.g. the PCD's antenna coil voltage. One of the greatest challenges for reader manufacturers arises from interacting factors like the mutual inductance M, or the electrical characteristics of the PICC-PCD-system. These factors cause, that

[5]This can be any electrical quantity chosen for the demodulation process.

the information is not evenly included in the phase or the amplitude of the signal. Situations emerge where the information can be predominantly included in the phase of a load-modulated signal. Common RFID readers, as mentioned before, using amplitude demodulation would fail [26].

Switching the load[6] between two quantities causes the load-modulated signal to be keyed between two amplitude, as well as two phase states. A *product detector*[7] in combination with a local oscillator (LO), generating a reference signal, can be used to coherently demodulate the load-modulated signal in order to get either amplitude or phase information.

Synchronization of the LO's and the load-modulated carrier signal the can be achieved using a Phase Lock Loop (PLL). However, this synchronization process, especially regarding the demodulation of binary-keyed signals, can be avoided using an I/Q demodulator.

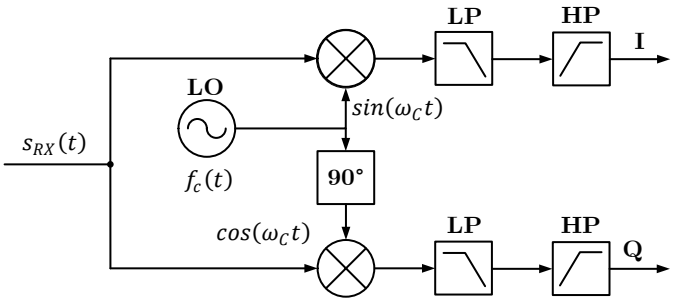


Figure 3.22: I/Q demodulator to demodulate a load-modulated carrier signal $s_{RX}(t)$

As figure 3.22 shows, both, I and Q channel are provided with the same information, the received modulated carrier signal $s_{RX}(t)$. The relation between the carrier signal's absolute phase and the LO's signal phase is pivotal. Subsequently, this relation can be seen as ratio of high and low level and thus the signal-to-noise ratio of the demodulated signal [26].

Practical tests revealed, for transponders converging to a reader the channel delivering the superior demodulated signal can change, due to the received signal's absolute phase depending on the distance between PCD and PICC antenna coils and the mutual coupling between reader and transponder system.

The basic idea behind the I/Q demodulator and its benefit of not being reliant on a synchronization unit will also be utilized later on in chapter 5.4.

[6]The load is commonly either a resistor or a capacitor.
[7]Also commonly referred to as *mixer* or *multiplier*

Chapter 4

Active Load Modulation

The following chapter is intended to shed some light on the principle of Active Load Modulation (ALM), the motivation to use ALM, its opportunities and merits compared to traditional Passive Load Modulation (PLM) and its influence on existing standards.

4.1 Motivation

According to ISO/IEC 14443 contactless transponders are powered from a reader-generated high frequency magnetic field whose field strength is defined to range from 1.5 to 7.5 A/m in zero distance [2]. By introducing such a transponder into the proximity of the reader and its electromagnetic field, according to *Faraday's law of induction* an Electromotive Force (EMF) is induced which can then be utilized to supply the transponder with the required energy. In addition, data transfer between the reader and the transponder is accomplished in the same manner, simply using ASK (reader to transponder) and load modulation (transponder to reader). To achieve load modulation, a modulation impedance connected in parallel to the transponder antenna is switched on and off based on the clock rate of and according to the signal to be transmitted. This method is called OOK, which denotes the most basic form of ASK. The load impedance is keyed by a modulated subcarrier ($f_{sub} = 848\,\text{kHz}$) signal. The subcarrier itself is generated by using ASK modulation with the *Manchester* coded data signal at a bit rate of 106 kilobitspersecond(kbit/s).

However, such a system has some limiting factors regarding its communication range that express themselves in:

1. being able to supply a contactless smart card with enough power to operate in the defined range of the reader, as well as
2. correctly receiving data transmitted by the reader, and similarly

3. being able to transmit data from the smart card back to the reader, adequate magnetic coupling between reader and smart card antenna provided (coupling factor (k) and Mututal Inductance (M)).

ISO/IEC 14443 compliant contactless systems utilizing typical ID1 smart cards have a maximum reading range from approximately 5 to 10 cm [21]. The maximum achievable communication range decreases drastically by using smaller antennas, such as in the format of very common Subscriber Identity Module (SIM) cards or micro Storage Device (SD) cards. Such small-scale contactless cards are commonly used, not only in mobile phones but also in all sorts of today's modern electronic gadgets. The additional shielding due to surrounding batteries and metal layers in a mobile device leads promptly to further issues, so that transponder reception and communication with an external reader gets severely inhibited. [21]

Experimental measurements[1] to determine the impact of a tag using active load modulation were made using an ISO/IEC 14443 Type A compliant reader, which can read contactless smart cards (ID1) over a range of typically up to 7 cm, well between the aforementioned maximum achievable communication range. These measurements, although using the very same antenna size together with a circuit enabling active load modulation, resulted in a reading range of up to 50 cm. The tests revealed a communication and reading range reduced by a factor of approximately two when decreasing the corresponding antenna size by a factor of 10 (figure 4.1).[2] The advantages of ALM compared to PLM seem to be clear: a larger operating distance as well as higher transmission speeds.

ALM can overcome the limitations of low side band amplitudes of minimum antenna sizes and achieve the side band amplitudes similar to these appearing with common PLM. The reader defines the time reference in contactless communication. The card has to respond synchronously to the reader alternating H-field. This is given for PLM, but is a challenge for ALM. To guarantee interoperability, an adequate method for phase drift measurement is necessary.

Hence this technology proved to be especially suitable for accomplishing a satisfactory operating range, especially with very small antenna-designs as for example in data storage devices. So even by using antennas in the size of micro SD cards, installed in mobile devices, suffering the very issues as mentioned earlier, a nevertheless acceptable communication range of at least few centimeters can be obtained, making it applicable in the field of modern electronic communications.

[1] All data and further information can be found in [21]

[2] Refers to effective antenna area [21]

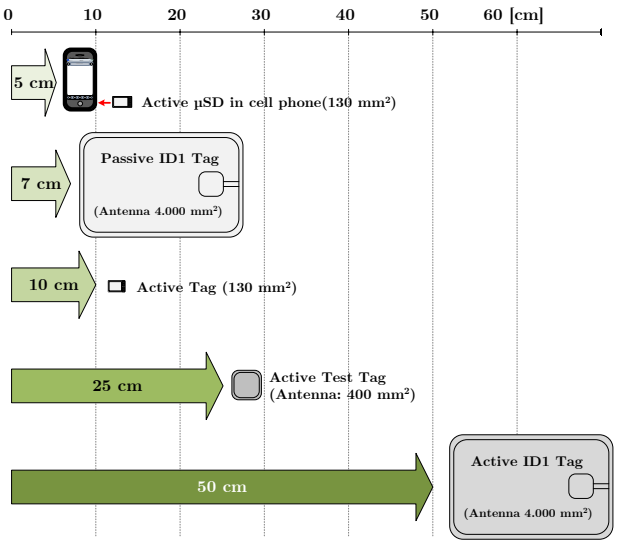


Figure 4.1: Different ranges of active and passive systems with differently sized antennas (adapted from [21]).

4.2 Principles of Active Load Modulation

The Principles of active load modulation arise from the necessity to overcome the limiting factors of transponder-reader systems using conventional PLM. To cope with the intrinsic problem of providing a power supply to a contactless smart card is not an issue in case of mobile devices: all mobile devices come with their own power supply, hence power is always available (active transponder/card).

In contrary, the solution for data transmission from reader to transponder is a bit more complex. An actively powered card with PLM communication provides just insignificant improvement over a passive card unless the magnetic coupling (M or k) can be altered for improvement (for example by decreasing the distance between the reader and the transponder). The chosen method is an approach to transmit an actively generated signal back to the reader, with exactly the same spectral characteristics as a PLM signal: the exact method used in small battery-supplied tags.

According to ISO/IEC 14443 the frequency spectrum of the reader antenna's signal arising as a result from the transponder's load modulation is depicted in figure 4.2. Along with the carrier signal (at 13.56 MHz), two additional spectral lines arise outlining the lower (at 12.712 MHz) and upper (at 14.408 MHz) sidebands resulting from modulating the carrier signal with the subcarrier signal. The upper and lower sidebands are separated from the carrier by the subcarrier frequency $f_{sub} = 848\,\text{kHz}$, having additional modulation sidebands resulting from the modulation of the subcarrier signal. These

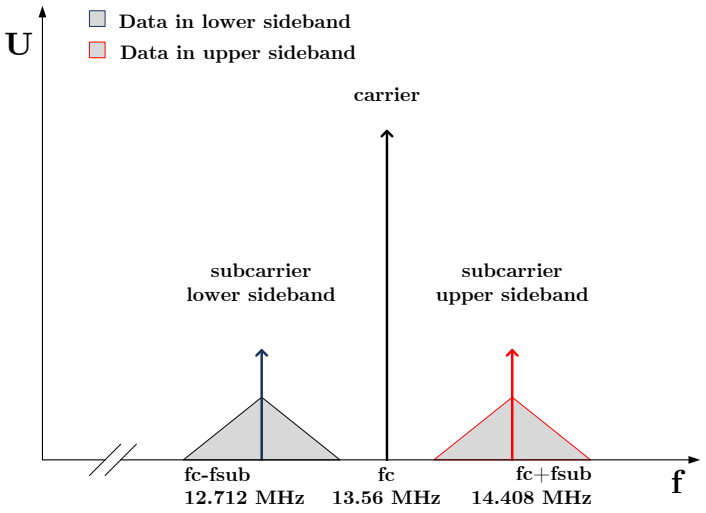


Figure 4.2: Schematic frequency spectrum at the reader antenna resulting from a common modulation with a subcarrier, according to ISO/IEC 14443-2 (adapted from [21]).

modulation sidebands solely comprise the entire information. This indicates that data transmission from an active transponder to a reader can be achieved by only generating these two subcarrier spectral lines with their corresponding sidebands. Therefore, ALM needs to exhibit the same spectral characteristics as PLM. A signal with these exact characteristics is referred to as Dual Sideband Modulation (DSB)[3].

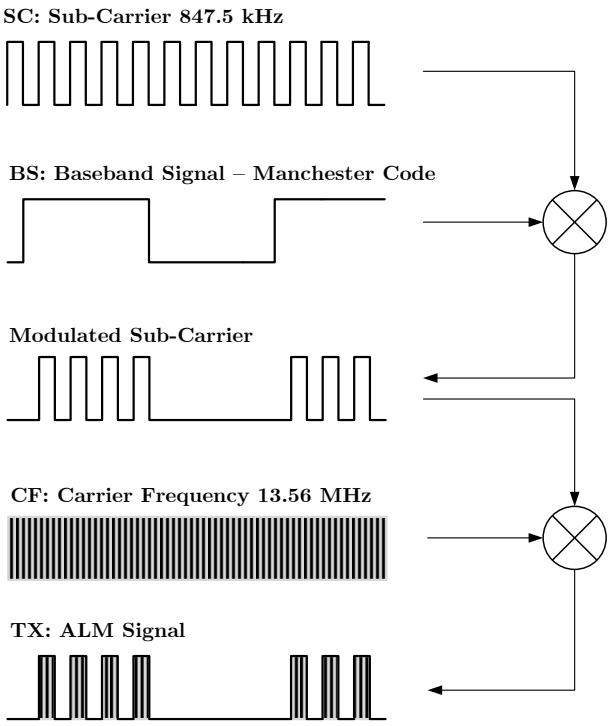
The needed requirements for an enhanced modulation therefore are:

- compatibility - ALM needs to be fully compatible with traditional PLM
- conformity - reader needs to get the same signal spectrum as in common PLM
- efficiency - additional power needs to be used in a most efficient manner

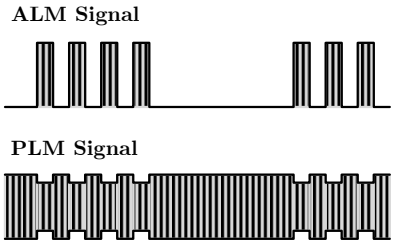
Figure 4.3(a) shows again the basic logical operations in an active RFID transponder, using a simple binary ASK modulator. The modulator is fed with a 13.56 MHz carrier signal (CF), the subcarrier (SC) as well as the baseband data signal (BS). The output signal of the modulator equals the required DSB signal. Before radiated by the antenna, its amplitude gets increased using an amplifier. The data signal is a binary baseband signal, consisting of two states, HI and LO.

The implementation of a simple logical AND operation leads to the multiplication of binary signals ($CF \wedge SC \wedge BS$), the equivalent to the binary ASK modulation. The output signal consists of carrier frequency bursts clocked by the modulated subcarrier signal. [21]

[3] A basic telecommunication circuit to generate a DSB modulation is a *ring modulator*.



(a) ASK modulator to generate an ASK type active load modulation (AND operation)



(b) Active load modulation and common passive load modulation in comparison

Figure 4.3

4.3 Testing against Standards

4.3.1 Context

Near Field Communication (NFC) is one of the most discussed and eagerly awaited topics in our today's industry. More and more projects, devices and applications literally pop up each and every day. Industries know how to read the signs of our times and are well advised to invest and participate in this branch of technology.

Predicted to account for almost a third of mobile payments transactions by 2014[4], mobile NFC promises to revolutionize not only inter-device communication, but also the manner how consumers will engage, interact and transact with brands and everyday activities. Contactless services offer quantities of opportunities in areas like payment, transit & ticketing, marketing & promotion, health-care, education, access control or general data exchange. Many actors will live and rely on projects based on NFC technology, such as:

- chip manufacturers
- tag manufacturers
- mobile phone designers
- system integrators
- banks
- ...

One substantial challenge arises: Interoperability.

Addressing the challenges of the NFC world is critical to enable its success from a device, network and service perspective. Once again, the role of the 'Secure Element' within the device is paramount in managing authentication and certification; not only to ensure the integrity of financial transactions and data exchange throughout the NFC chain, but to deliver the required levels of interoperability as well. Interoperability is defined at several layers:

- Application layer
- Digital layer
- Analog layer

[4]Research and Markets, 2010

4.3.2 Introduction to Contactless Standards

The purpose of standardization is to set technical standards to help maximizing and optimizing compatibility, safety, reproducibility, quality and interoperability. On the most basic level interoperability shall be ensured by defining analog test specifications. As a consequence different institutions with different approaches and aims originated to set separate, yet equivalent standards:

ISO/IEC 14443

ISO/IEC 14443 is the base standard and defines the contactless smart card technology at an operating frequency of 13.56 MHz. The most essential features are:

- 4 different parts, each covering a specific layer including the physical characteristics, specifications up to the protocol layer.
- Two different communication types, namely *Type A* and *Type B*, different in layers 2 and 3 but with similar capabilities thus sharing the protocol model as defined in layer 4, the protocol layer.
- A somewhat strict separation between reader devices, as being the active part, and cards. In general, the reader is initiator and provider of the RF field .
- ... thought to be a generic standard, being used as a base for a multitude of different products.

The base standard only provides basic specifications and requirements. Test scenarios were established later with the introduction of ISO/IEC 10373-6 [2], defining tests for both, cards and readers on all available layers. Within ISO there is a continuous endeavor to add further functionality such as higher bit rates or active modulation functionality, displayed by diverse amendments.

The international committee defines testing methods and handling for contactless smartcards in a generalist approach and not particularly focused on specific businesses. Its test specifications are public and groups are present in all major countries such as France, Japan, Germany etc. Its members are mostly card makers, chip makers but also laboratories or test tool vendors.

The ISO Test PCD assembly as defined in ISO 10373-6 [2] consists of the following parts:

- **PCD antenna**: The PCD antenna encloses a circular area having a diameter of 150 mm and is matched to 50Ω via matching circuit on the same Printed Circuit Board (PCB). The circular antenna creates a homogeneous field distribution in an axial distance of 37.5 mm, to simplify measurement.

- **Two sense coils A and B**: Via balancing circuit, both sense coils are connected in a way, to achieve induced voltages opposing in phase of one another. They are located on the back and front of the main antenna coil, equally distant to the main coil. This allows the effective cancellation of the induced voltages in both sense coils (figure 4.4).

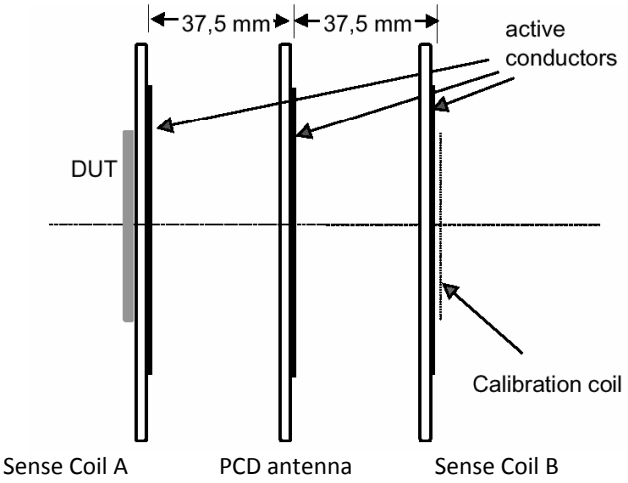


Figure 4.4: Cross-section of the Test PCD assembly [2]

- **Calibration coil**: resembles an ID1 card, containing only a single turn coil and is meant to be connected via high impedance probes. The layout allows for the measurement of the magnetic field strength in the frequency range of 13.56 MHz. Providing high ohmic loads by the applied measurement device, while measuring the field strength is essential to prevent flowing currents in the calibration coil and thus measurement errors. These errors can arise from a rising current induced into the Calibration coil, leading to a rising magnetic field which would, in return, significantly influence the PCD's magnetic field (*Lenz' law*).
- **PCB holding the balancing circuit**: This additional printed circuit, comprising two 240 Ω resistors and a 10 Ω potentiometer P1, is used as a balance point between both sense coils while in an unloaded state, similar to a measurement bridge. Hence it is commonly referred to as *Helmholtz Bridge (HHB)*. Due to tolerance-related asymmetries a low residual voltage between both sense coils can be compensated by using the P1 (figure 4.5).

Reader testing is based on the according Reference Proximity Integrated Circuit Card (RefPICC). The six different RefPICC's consist of various adjustable components which allow the adjustment of the resonance frequency, the load and the signal amplitude of the modulated signal. Each test case requires the tuning of the RefPICC.

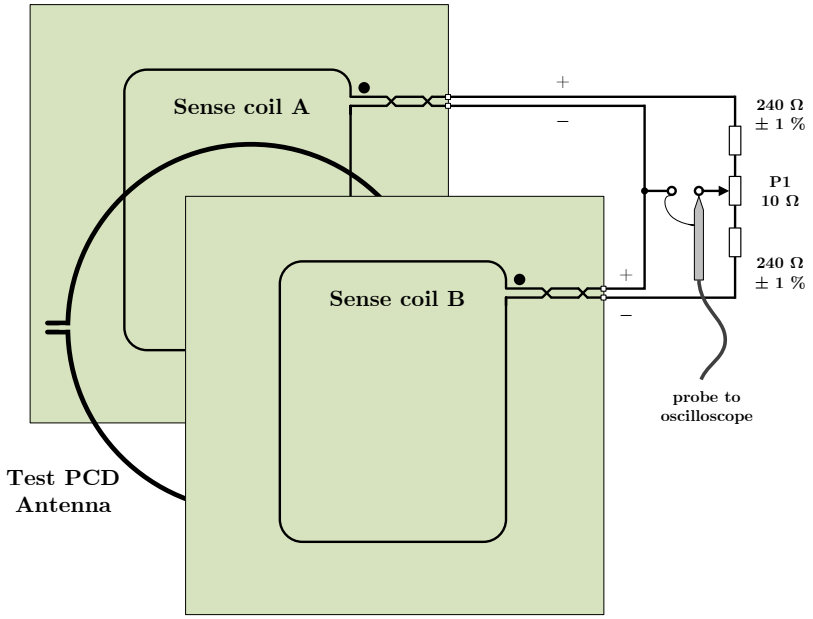


Figure 4.5: Sense Coils A and B and balancing circuit [2]

The standard defines a set of six measurement classes for two different setup types:

- classes 1, 2 and 3 for a setup bigger in dimension
- classes 4, 5 and 6 for a setup smaller in dimension

(a) PCD of ISO/IEC (b) RefPICC of ISO/IEC

Figure 4.6: PCD and RefPICC according to ISO/IEC [23]

A short overview of ISO/IEC testing philosophy [23]:

PICC/card testing	**PCD/reader testing**
tests for Type A and Type B	operating volume
reception of different reader signals	waveshape
loading effect	bit coding
Load Modulation Amplitude (LMA)	PCD power transfer
testing of all baudrates	
alternating magnetic field	

Table 4.1: Testing Philosophy of ISO/IEC regarding PICC and PCD

Further remarkable facts of ISO/IEC 14443 in comparison to other established standards are:

- load modulation measurement computed based on Fast Fourier Transform (FFT)
- just one defined test position; variation of the magnetic field strength available by varying the PCD's source voltage.
- PCD signal can be measured either while loaded via RefPICC or while via calibration coil.

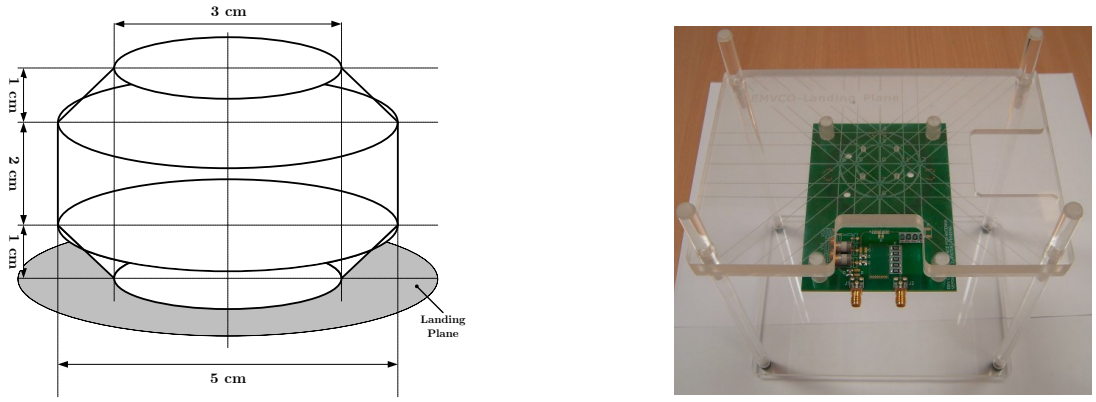
Europay International, Mastercard and Visa Contactless (EMVCo)

EMV's name stems from the companies, initiating the development of its specifications in 1994: *Europay*, *MasterCard* and *Visa*. EMV, compared to ISO/IEC and NFC Forum, takes a completely different approach. Its focus lies exclusively on the payment area. EMV created a comprehensive set of base and test specifications to ensure interoperability between all companies within the global payment system, containing cards, software and terminals.

A multitude of technologies, including contactless smart cards (managed and maintained by EMVCo) are covered this way. The specifications are similar and relate to ISO/IEC 14443. Interoperability to a certain degree is therefore possible. EMVCo also established their own certification scheme. To officially support credit card payments, manufacturers of payment products need to get their products certified mandatorily.

The EMVCo Level 1 Test Equipment consists of three main parts:

- **the EMVCo reference PCD**:
  The PCD is mounted on a mechanical structure to support the free positioning of the DUT. EMVCo defines more than 20 different test positions in a 3-dimensional space, specified by a r-, φ- and z-coordinate (figure 4.7). All defined positions need to be pass for a given test case to be declared successful. The dimension of its antenna coil is based on actual readers, available on markets.



(a) Operating Volume

(b) EMVCo PCD

Figure 4.7: Operating Volume and PCD according to [8]

- **the EMVCo reference PICC**:
  The reference PICC is mostly used to perform measurements and analysis of the reader signal, but in return can also send information back, using load modulation (different jumpers). The antenna is similar to typical *ID1* cards (figure 4.8). The resonance frequency of the PICC is 16.1 MHz and a compromise between commu-

nication capabilities, detuning and power consumption.

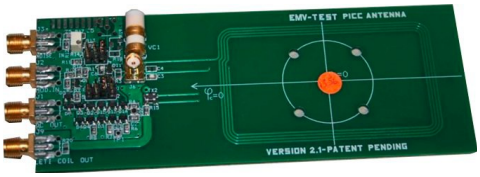


Figure 4.8: EMVCo PICC [8]

- **the EMVCo Common Mode Rejection (CMR) Board**:
  This additional circuitry is directly attached to the PCD - PICC system and used to extract the envelope of the measured signal (figure 4.9). The CMR board uses the peak sampling method.

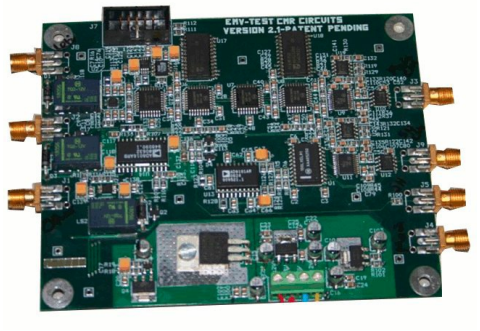


Figure 4.9: EMVCo CMR [8]

A short overview of EMVCo testing philosophy [23]:

PICC/Card testing	**PCD/reader testing**
tests for Type A and Type B	field strength
responsiveness to different reader signals	waveshape (ringing, monotonicity, ...)
loading effect	bit coding
LMA	sensitivity
baudrate of smartcards	
106 kbit/s tests only	

Table 4.2: Testing philosophy of EMVCo regarding PICC and PCD

Further remarkable facts about EMVCo in comparison to other established standards are:

- measurement devices are required to be highly accurate to meet requirements
- test volume is defined by different physical positions tests at all positions which need to be pass
- load modulation measurement based on peak-to-peak amplitude
- designed for ID1 devices only
- Mobile Network Operator (MNO)'s demand EMVCo testing, payment as one core business of NFC

NFC Forum

NFC Forum was founded in 2004 to ensure interoperability for products of different device classes utilizing NFC technology. Therefore base and test specifications have been introduced along with an own certification program.
Similar to EMVCo, NFC Forum specifications are based on ISO/IEC standards such as 18092, 14443-2, -3, -4, as well as others such as the JIS[5] X6319-4. The implementation specifications describe the parts of those standards that are relevant for NFC Forum devices. Therefore, compliant devices behave in the most consistent way and the evolution of existing infrastructure towards an unrestricted NFC support is facilitated. [29]

Some of NFC Forum's characteristics are:

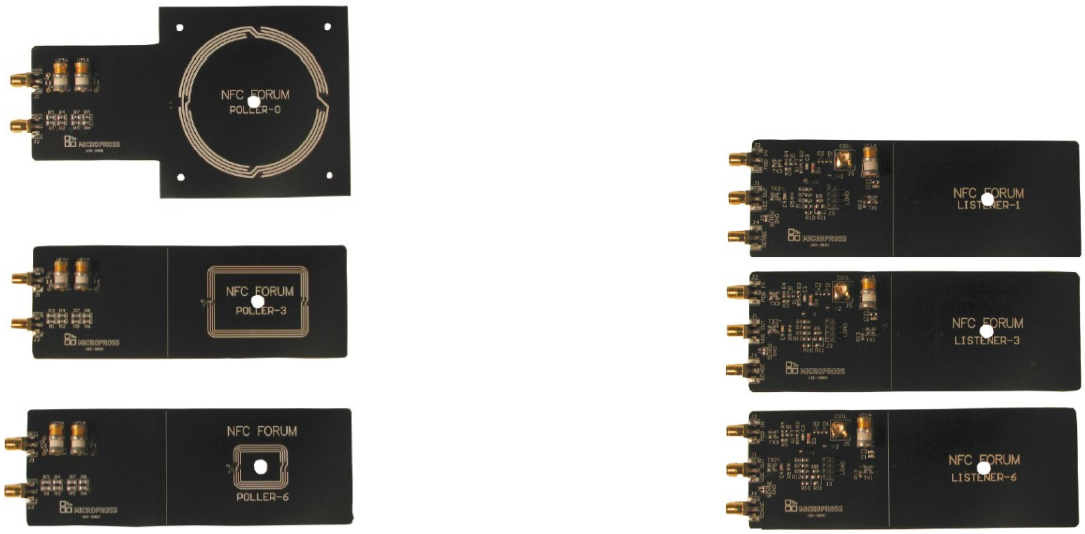
- Base specifications consist of different documents, covering specific topics regarding analog, digital protocol or activation for example.
- Modified versions of both ISO/IEC 14443 defined smart card types (A and B). bit rates are limited to $fc/128$, as being the most prominent.
- A third type, *NFC-F*, based on the *FeliCa* standard is introduced, being the only smart-card specified to be used with even higher bit rates.
- No obvious seperation among reader and card as: *NFC Forum Devices* need to have a reader-functionality along with a card-emulation option. Furthermore a Peer-2-Peer operation mode is mandatory.
- *NFC Tags* representing passive smart cards were introduced to complement *NFC Forum Devices*.

[5] Japanese Industrial Standard (JIS)

NFC Forum reference antennas can be divided into *pollers* and *listeners* and are very similar to EMVCo antennas [23]:

Pollers are used to test devices operating as tags. For interoperability purposes there are 3 antenna sizes. A device can be declared compliant if tested with all of these antennas. The measurement is done directly on the antenna, resonance frequency can be adjusted using a vector network analyzer.

Listeners on the other hand are used to test devices operating as readers. Analogous to pollers, for interoperability purposes 3 antenna sizes are used. A device can be declared compliant if tested with all of these antennas. The measurement is done directly on the antenna, resonance frequency can be adjusted using a vector network analyzer.



(a) NFC Pollers

(b) NFC Listeners

Figure 4.10: Pollers and Listeners of NFC Forum [23]

A short overview of NFC Forum testing philosophy:

Listener testing	**PCD/reader testing**
tests for Type A and Type B and FeliCa	field strength
responsiveness to different reader signals	waveshape (ringing, monotonicity, ...)
loading effect	bit coding
LMA	sensitivity
106, 212 and 424 kbit/s tests	

Table 4.3: Testing philosophy of NFC Forum regarding Listener and Poller

Further remarkable facts about NFC Forum in comparison to other established standards are:

- measurement devices are required to be highly accurate to meet requirements
- test volume is defined by testing at different physical positions; not all positions need to be pass
- operating volume is adapted for small form factor devices (battery powered)
- load modulation measurement based on peak-to-peak amplitude
- form factor of DUT is considered
- test cases for Type A, B and FeliCa

4.3.3 Different Standards, Different Scopes

A brief overview of selected parameters shall show inherent differences between the presented standards:

	Test Position	Antenna Classes	Load Modulation Measurement
ISO	one test position	6 different classes of antennas	uses phase and amplitude of the load modulation
EMVCo	volume with 20+ test positions	only one defined class of antenna (ID1)	peak-to-peak measurement
NFC Forum	volume with 20+ test positions	3 different classes of antennas	peak-to-peak measurement

Table 4.4: Different analog test specs of presented standardization bodies

The choice of the preferred test tool ultimately depends on the case of application of the DUT. Different lines of businesses and fields of applications prefer distinct tools:

- EMVCo: banking applications
- ISO 14443: ticketing, transportation, vouchers and application
- NFC Forum: use cases specific to NFC

Once again it shall be noted, that no test specification is superior to the other. Each test specifications has its distinctive drawbacks and benefits. Results and the transfer between different test specs is difficult. [23]

As Infineon Technologies Austria AG is heavily involved in ISO standardization processes and its costumers are to be found mostly in the fields of payment and transit & ticketing, all following considerations are with the focus on the ISO/IEC standardizations and specs as proposed on ISO/IEC 7816, 10373 and 14443.

4.3.4 Relationship between EMV and ISO/IEC Specifications

The fundamental difference between ISO's *Test PCD assembly* and EMVCo's *PayPass Reference Equipment* lies within the measurement and evaluation of parameters such as the impact of the secondary current, $i_2 = i_{PICC}$. Where EMVCo allows for an indirect measurement of a PICC current-equivalent shunt-voltage due to conductive coupling

with the PCD, ISO's *Test PCD assembly* uses a more direct approach, an inductively coupled measurement bridge, also called *Helmholtz Bridge* (figure 4.11).

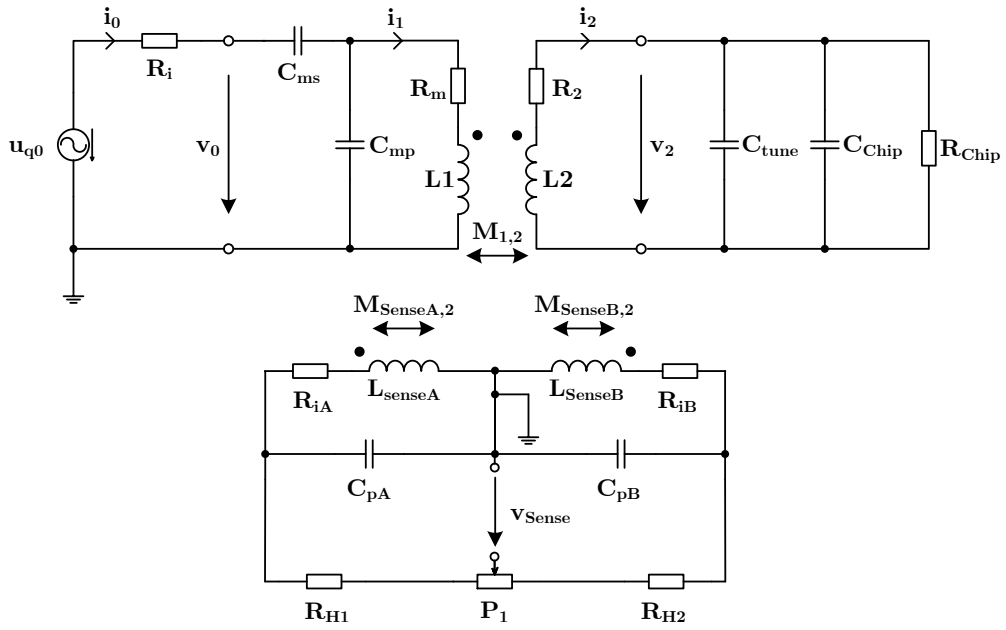


Figure 4.11: Simplified equivalent circuit of the ISO Test PCD assembly, without considering the calibration coil

This so-called *Helmholtz Bridge* is build in a way, so that an unloaded state (no PICC present), erects the same flux density B through both *Sense Coils*, A and B. This is achieved due to a symmetric arrangement in relation to the PCD antenna, erecting the same voltage levels in both branches of the circuitry. Subsequently, this cancels out the PCD induced voltages evenly, leading to a voltage v_{Sense} of zero. By loading and bringing a PICC into vicinity the PICC causes a counteracting electromagnetic field H_{PICC}, decreasing the current i_1 (i.e. *loading*) in the PCD. This results in an uneven magnetic flux in both sense coils and therefore a potential difference of $v_{Sense} \neq 0$. By using the *Helmoltz Bridge*, this method allows the direct measurement of an i_{PICC} equivalent value, as the PCD's influence is eliminated systematically. Contrary to EMVCo's approach, where only the impact of the PICC on the PCD is observable.

In contrast to ISO's Test PCD assembly, EMVCo's standardization setup measures the PICC's impact on the reader's (PCD) current $i_1 = i_{PCD}$. Additionally, the current i_1 in the reader antenna is calibrated to maintain a constant value whereas ISO's approach is to sweep this current. A variety of different loading states leading to different currents (due to different values of mutual inductances M) can be achieved by changing the

distance (z-coordinate) and angles between the PICC and PCD in predefined slots.

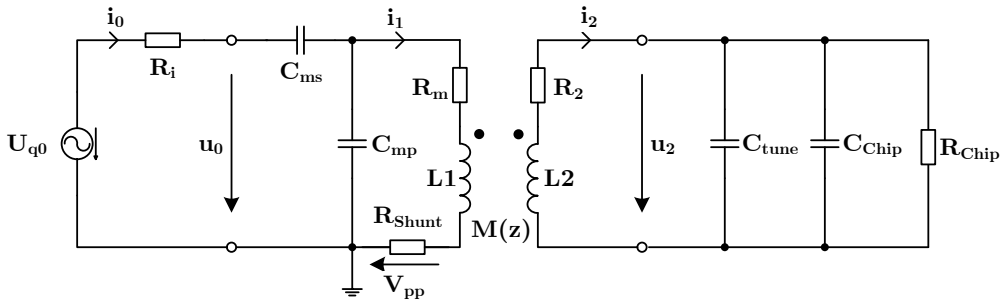


Figure 4.12: Simplified equivalent circuit of the EMVCo Level 1 Test Equipment

Figure 4.12 shows the simplified equivalent circuit of the EMVCo Level 1 Test Equipment. The shunt resistor R_{Shunt} in the primary circuit, resembling the PCD, with its rough value of $1\,\Omega$ operates as trans-impedance. The voltage v_{pp}, measured by the CMR board during load modulation and loading of the PICC, corresponds to the primary current $i_1 = i_{PCD}$. The secondary circuit represents the PICC with C_{Chip} and R_{Chip} defining an unspecified operating point.

4.3.5 ISO/IEC 14443 and ALM

This last section shall close the circle of ALM and standardization, specifically ISO/IEC (see also [21]):

Transponders using ALM generate signals indistinguishable from classical PLM by any reader. Nevertheless, there is a strong need to standardize this technology. For ISO/IEC 14443-2 [3] it is mandatory to use a passive load-modulator. Therefore a transponder using ALM is inherently unable to be compliant with the established version of ISO/IEC 14443-2. It only permits passive load modulation. For that reason some clauses need to be changed:

„Clause 8.2.2 – The PICC shall be capable of communication to the PCD via an inductive coupling area where the carrier frequency is loaded to generate a subcarrier with frequency fs. The subcarrier shall be generated by switching a load in the PICC".

The standard needs to be overhauled accordingly to improve not only the specification of the physical device, defined in ISO/IEC 14443-2, but also the relevant compliance tests defined in ISO/IEC 10373-6 [2] need to be adopted. New wording within the standard texts, to explicitly render ALM possible, along with other needs to clarify some additional issues [15] need to be defined.

"In order to be able to test these (active) PICCs independently from the numerous devices in which they can be inserted and also to test these devices independently from the PICCs which can be inserted in them, it was proposed to define a "Reference Active PICC". The same reasoning also applies for any other PICC which usually or always operates within a device. The main objectives of the New Work Item Proposal were then clarified:

1. *Not to preclude the use of a battery (i.e. allow "active PICC modulation"), because present ISO/IEC 14443-2 explicitly defines "load modulation" for PICC;*
2. *Define the RF limits for " Active PICCs" (independently from any device), so that these limits include margins to take typical device attenuation into account;*
3. *Define the RF limits for devices, measured with a "Reference Active PICC."*

In September 2010, the Deutsches Institut für Normung (DIN) made a contribution brought to Working Group 8 (WG8) [16] and resulting in the launch of an NP ballot in December 2010 by SC17/WG8 [17]. It got accepted by the standardization committees in February 2011:

„PICCs with external power supply – Use power supply other than the PCD-field so that PICCs with very small antenna and/or metallic environment can be compliant with ISO/IEC 14443-2: Currently more and more small PICC form factors are penetrating the market. Very often these PICCs are attached on metal surfaces (mobile phones) or they are even operated inside a mobile phone (memory cards). These metal environments often cause additional drops in performance (reading distance). WG8 has reacted with different antenna classes, which results in different ranges for the field strength for each

class, thus resulting in reduced operating range for classes with increased minimum field strength. Actively powering the PICC will allow the PICC to handle field strength down to 1,5 A/m even in metal environment, while transmitting an enhanced modulation signal will allow the PCD to pick up the PICC signal even with very bad mutual coupling between PICC and PCDs antenna, e. g. with metal environment. So PICCs with external power supply will be an innovative approach to operate very small PICC antennas with PCDs already in the field."

Chapter 5

Components of the Test Bench

Based on the devices and existing circuitry available, a block diagram inheriting both, existing and outlined future components to form a complete test bench can be depicted.

It is suffice to consolidate the different parts to a few major modules:

- the existing being **PCD Emulation** as well as the **ISO Test PCD assembly** plus the ***Extended RefPICC*** [27] and some form of **Signal Acquisition and Measurement**, but also
- now new required components such as a **PICC Emulation** unit along with a needed **Carrier Recovery**, **AM and PM Control** and some form of an interconnecting **Control Interface** to bind the latter components.

Some modules consist of devices present at the development cite Graz of *Infineon Technologies AG* and can also be applied immediately, such as both the PCD (e.g. Tabor WW1281A Arbitrary Waveform Generator (AWG) [38]) emulating element or the signal acquisition.
Others may need a proper overhaul (e.g. the RF current source circuitry or even a complete system design from scratch such as the PICC emulation unit complete with suitable synchronization to allow a phase-coherent behavior between output signals of both emulation blocks.

Everything combined this forms a usable test bench as depicted in figure 5.1 beneath:

The different blocks listed:

- *PCD Emulation* is needed to generate arbitrary modulated signals to the Test PCD assembly to emulate a transmitting reader.
- *PICC Emulation* needs to be able to generate data signals relevant to ISO standards, arbitrary in phase and amplitude. The module must be able to react to a clock signal from outside.

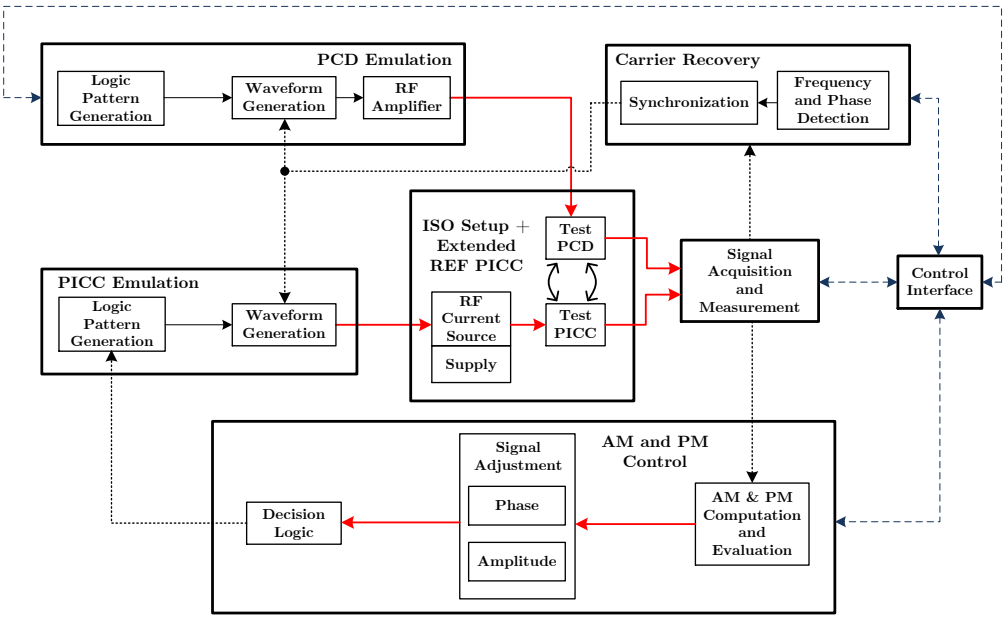


Figure 5.1: Block Diagram of a suggested test bench setup

- *Test PCD assembly + Extended RefPICC* represents the standardized test setup of ISO/IEC [2] designed for PLM communication. An RF current source is applied to the test PICC to allow ALM.
- *Carrier Recovery* represents the whole effort to synchronize the PICC clock with the PCD clock which becomes necessary as during ALM communication phase locking of the PICC onto the PCD phase is not possible leading to drifts and ultimately failing communication.
- *Signal Acquisition and Measurement* goes together with *Control Interface* and is summarizing all devices, such as oscilloscopes, probes, computers etc. to obtain reliable measurement data for evaluation.
- *AM and PM Control* represents software which computes system parameters from measurement parameters, eventually leading to a decision logic where its output signal might influence the further PICC emulation behavior.

5.1 RF Current Source for Active Load Modulation

The following section will mainly focus on the findings of Egger's thesis [27] and the designed RF current source circuitry. In combination with the existing standardized device, the RefPICC as outlined in chapter 4.3 shall result in an *Extended RefPICC*.

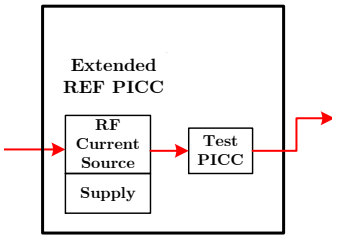


Figure 5.2: RF Current Source and RefPICC within the test bench block diagram

5.1.1 Motivation

Analyses have shown, that standardized EMV Test PICCs are not able to emulate today's relevant DUT/antenna combinations, furthermore the determination of operating points tends to be tedious and time consuming.

The standards are set to evaluate AM information exclusively, although load modulation has non-negligible influence on the phase of the PICC current, $i_2 = i_{PICC}$.

Ultimately this leads to the load modulation represented as combination of both, AM and PM ([28]). Manufacturers of reader devices have long been paying attention to this circumstance and have been producing devices utilizing *quadrature* or I/Q demodulation. These facts culminate in the realization of using an outdated standardization technique with even so outdated devices.

Egger's work was to design a new *Extended* RefPICC, capable of reaching all required operating points by means of AM and PM. This leads to a galvanically coupled approach of basically a current source in parallel to the PICC antenna. The current source drives an additional current, proportional to an input voltage representing the modulation signal, through the PICC antenna.

With the implementation of the Extended RefPICC some crucial requirements are set as well:

- phase/clock recovery of the reader magnetic field H, to maintain a stable phase relation between currents i_{PCD} and i_{PICC}.

- Possibility to specify any reasonable phase relation between currents i_{PCD} and i_{PICC} for transmission of a digitally amplitude-modulated signal.
- Possibility to specify any reasonable amplitude for the PICC current, i_{PICC} for transmission of a digitally amplitude-modulated signal.

5.1.2 Proposed Circuitry

This section will provide a better understanding of the existent circuitry, pros and cons of its design and its application in test scenarios.

As pointed out by Egger, the load represented by the RefPICC may influence the active modulation operation by consuming part of its produced current. Either way, it is crucial to keep a constant load in addition to the present modulation realized,

- either passively as in the present RefPICC, using different resonance frequencies[1],
- or actively, using input connectors of the passive RefPICC[2].

The circuitry as depicted in figure 5.3 shows the RF current source. An in-depth explanation about the several parts and stages of the analog front-end can be found in [27].

To give a short overview, the circuitry can be dissected into two main parts,

- a current deflector, represented by the transistors $T1...T4$
- and a matched current source/sink, represented by the Integrated Circuit (IC)s and the additional Metal Oxide Semiconductor Field Effect Transistor (MOSFET)s $Q1..Q3$.

[1] The calibration steps are described in [2].

[2] The RefPICC offers the possibility to directly apply a Direct Current (DC) voltage via SubMiniature Version A (SMA) connector.

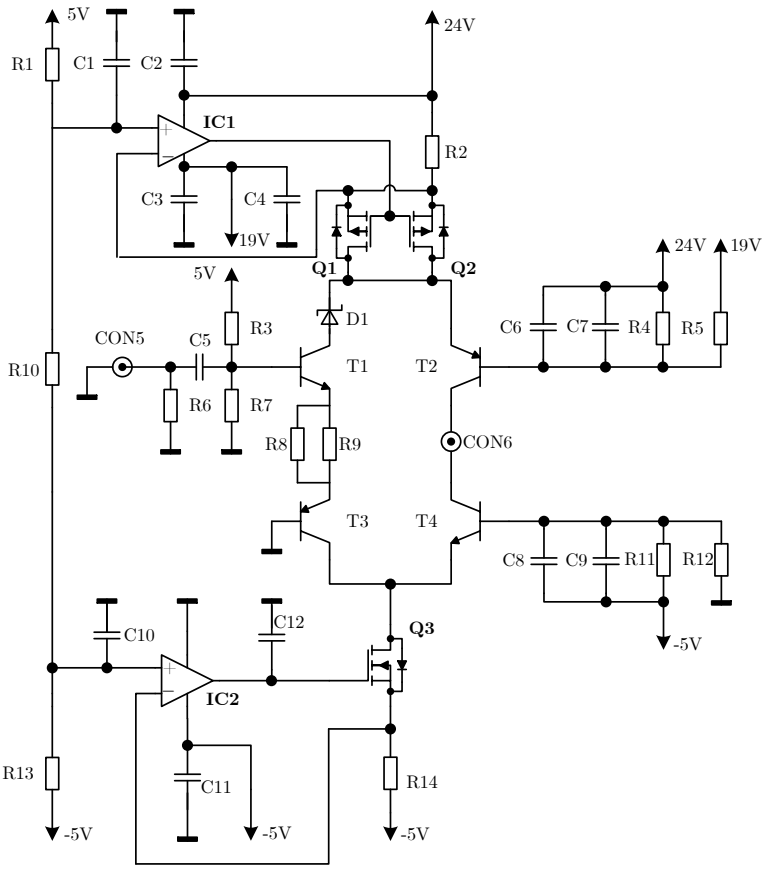


Figure 5.3: Depiction of proposed active reference PICC circuitry (adapted from [27])

The modulation signal is supplied at connector CON5, the amplified and modulated output current is injected into the PICC antenna[3], depending on the layout design optionally via SMA connector or pin strip. The original ISO RefPICC is as well connected to the antenna, in parallel to the RF current source. This offers the initially outlined requirement to keep a constant load and moreover fulfills the requirement of still being able to perform common PLM tests.

What happens is that a DC current, $I_{DC} = 60\,\text{mA}$, generated by the two current sources/sinks, is driven through the current deflector. I_{DC}, if no modulation is applied at CON5, splits into two equal parts $I_{DC}/2$ across both, *input* path T1/T3 and *output* path T2/T4. As soon as an alternating modulated voltage v_{mod} is applied at CON5 an alternating current $i_{mod} = {}^{v_{mod}}/_{(R9 \| R8)}$ drains into $T1$.

[3]L1 is the simplified representation of the PICC antenna.

Component	Value	Component	Value
R1, R13	1 kΩ	C1, C7. C9, C10	1 nF
R2, R14	4.9 Ω	C2, C3, C5, C11	100 nF
R3, R7	100 Ω	C3	100 nF
R4, R11	330 Ω	C4, C12	1 nF
R5, R12	180 Ω	C6, C8	1 μF
R6	51 Ω	Q1, Q2	BSS84
R8, R9	82 Ω	Q3	BSS123
R10	90 kΩ	T1	PZT2222
D1	BZX84C6V2	T2	PZT3906
IC1, IC2	AD8605	T3	Qmmbt2907
CON5	RF Connector	T4	PZT3904

Table 5.1: Components of active reference PICC circuitry

Subsequently, this leads to a shift in the transverse current, as an increase of the input current i_{mod} is leading to a decrease of the output current equal in quantity.
The result can be best described as an inverting transconductance amplifier with a transconductance of $g_m = {}^{-1}/_{(R8 \| R9)}$. [27]

After testing the proposed circuitry in practice, several shortcomings became apparent:

- The current source/sink is basically a system with two control subsystems (AD8605) influencing each other negatively, if not matched accurately enough. In a practical perspective this means an inherent potential for instability.
- Both AD8605 drive fairly high capacitive loads, which put the system to risk of unwanted oscillation, due to parasitic capacities and decreasing phase margin.
- The whole circuitry is extremely prone to environmental changes and influences. The layout design of the PCB needs to have as little parasitic capacities as possible. The current PCB consists of discrete components, a solution with fewer integrated components might be more stable and may grant higher reproducibility.
- The dissipation power, not only, but especially in T1 is near its maximum allowed limits due to the high bias current leading to high voltage drops along the input and output paths. The thermal dissipation can reach up to 90° Celsius. As a direct consequence, the quiescent point of all affected transistors is shifted accordingly resulting in behavior difficult to predict and to control.

5.1.3 Circuitry Improvements

After discovering the problems mentioned above, a review and redesign seemed to be necessary to successfully establish a first proof-of-concept of the proposed test bench.

Adapting and simulating the whole test assembly including the PICC via *LTSpice* [40] lead to the decision to use two 200 mA 2-terminal programmable current sources, *Linear Technology's LT3092*. Its maximum output current, the wide input voltage range as well as the low temperature coefficient and its robustness in terms of stability made a seamless integration into the preexisting circuitry easy.

A main advantage are the integrated protection circuitries and the stability even without using bypass capacitors and capacitors across it. In principle, the turn-on and line transient response is fast enough in principle, however, proved to be a bit slower as the original circuitry. Nevertheless, this drawback however is acceptable as the higher stability and better insensitivity seem to be an acceptable trade-off.

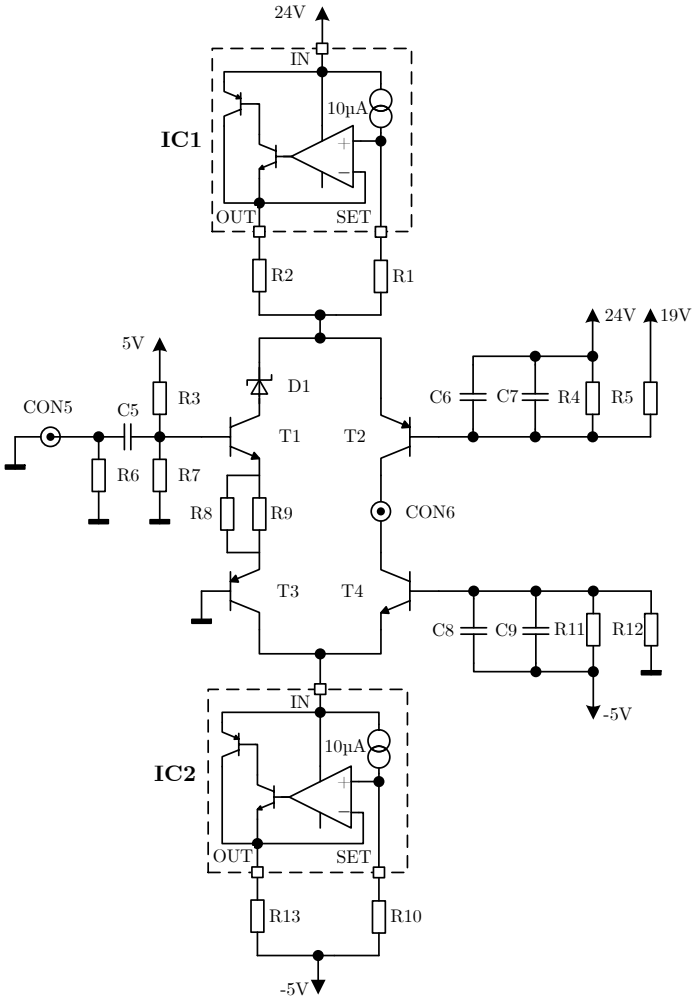


Figure 5.4: Depiction of improved active reference PICC circuitry (adapted from [27])

Figure 5.4 shows the straight-forward implementation of the current sources. Experimentally, small-valued resistors in series with the device were added to isolate the lines from more ringing and oscillations due to the complex load. By placing a shunt resistor between input and output of the current source the power dissipated in the IC could be decreased additionally by a factor of 4.

The $10\,\mu$A reference current is used with a resistor $R_{SET} = R1$ at the SET pin of the IC to generate a voltage in a range from 100 mV up to 1 V. The voltage is then applied across a resistor $R_{OUT} = R2$, connecting the OUT pin of the IC and resistor $R_{SET} = R1$.

The sink and source current $i_{out} = i_{snk} = i_{src}$ is then determined by following equation:

$$I_{OUT} = \frac{V_{SET}}{R_{OUT}} = \frac{10\,\mu\text{A} \cdot R_{SET}}{R_{OUT}} \tag{5.1}$$

Using 30 kΩ for R_{SET} was a reasonable value to create a voltage sufficient to minimize the error caused by the offset between both output pins. The value for R_{OUT} is determined accordingly to create a 60 mA bias current. It is crucial to use a pair of resistors with matching low temperature coefficients. [44]

Component	**Value**
R1, R10	30 kΩ
R2, R13	4.9 Ω
IC1, IC2	LT3092

Table 5.2: Components of improved active reference PICC circuitry

However, it needs to be noted that the adapted version is a trade-off. The original circuitry was designed to overcome all possible limitations of the passive Reference PICC and to approach all quadrants of the amplitude/phase plane. The device proved to be very delicate to handle and at times even yields unreliable measurement results due to the remarks made above. The second, overhauled version is therefore a more compact draft, less prone to environmental and parasitic influences but with much tighter limitations, the natural trade-off between integrated and discrete design.

The following figures showcase the realized PCB version:

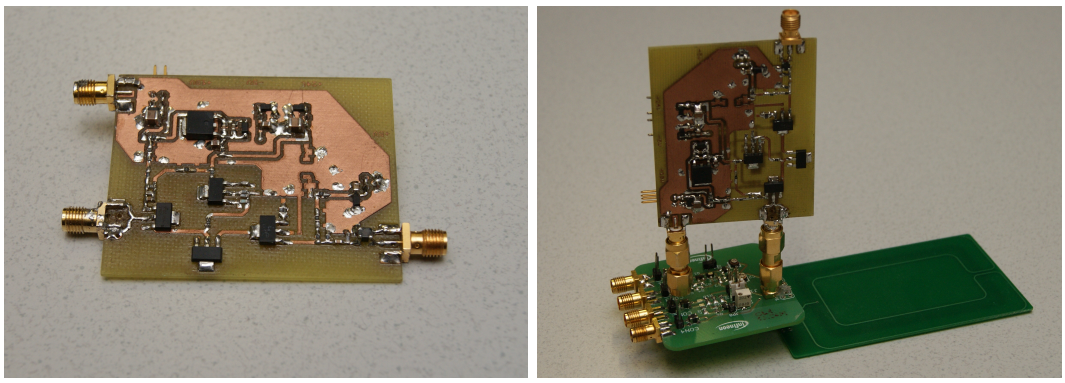


Figure 5.5: The PCB alone (left) and attached onto the existing RefPICC plus antenna (right) leading to the *Extended RefPICC*.

5.1.4 Concluding Thoughts

Working with the circuitry proved to be tricky. Its high sensitivity to environmental influences and the high temperatures dissipated in its crucial parts raise doubts regarding its ultimate usability.
Although WG8/TF2 accepted the initial proposal [11], made by Infineon Technologies, the further course of action remains unclear. A revision of the entire circuitry seems to be inevitable to fully match strict ISO conformities and might, due to its extent, represent a separate thesis in its entirety.

5.2 Carrier/Clock Recovery and Synchronization

One main requirement for a fully-functional test bench setup is the proper synchronization between both, PICC and PCD clocks. In a first step, this is established by using the synchronization in- and outputs of both emulation units. This approach is sufficient for a proof-of-concept but has no relevance regarding a practical implementation.

The ultimate goal of the test bench is to use any kind of reader as DUT, so a required reference or synchronization signal is highly unlikely to be provided separately. A technique to recover the PCD clock signal is needed. Stability, accuracy and as little interference as possible with the existing PICC-PCD system are substantial.

The following section deals with the necessary steps of signal processing to gather the magnetic field signal generated by the PCD, to recover a clock signal and at last, to use that clock for synchronization of the RefPICC's ALM/PLM signal (figure 5.6).

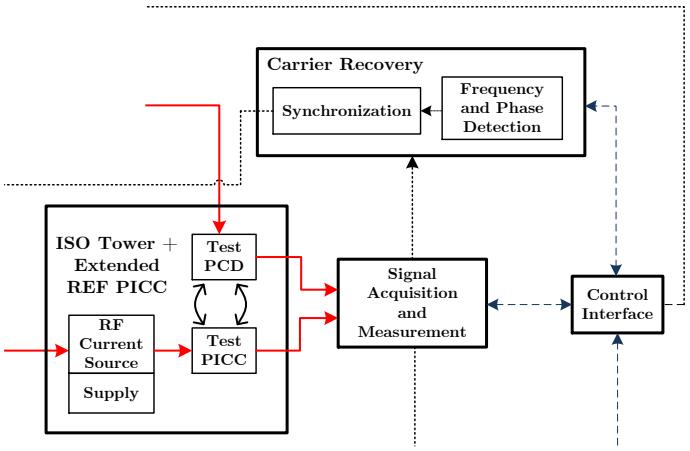


Figure 5.6: Clock recovery and relevant blocks[4] of the proposed test bench

5.2.1 Signal Acquisition

Before looking at the basic principle of carrier/clock recovery the first question in the process of a clock recovery arises with the proper signal acquisition. There shall be a possibility to spy existing signals without influencing the system itself. This sounds fairly trivial in theory, however, leads to many problems in practical uses, as each new antenna brought into the system means additional load (due to magnetic coupling) and interference of measured signals due to induced currents.

Based on this idea, the signal acquisition can be achieved by using the already built-in *Pick-up Coil* of the RefPICC [2]. The *Pick-up Coil* is designed in a way, so that there is no apparent magnetic coupling between the *Main Coil* and the *Pick-up Coil* of the RefPICC antenna. Figure 5.7 shows the bottom and the top layer of the Class 1 Reference PICC antenna.

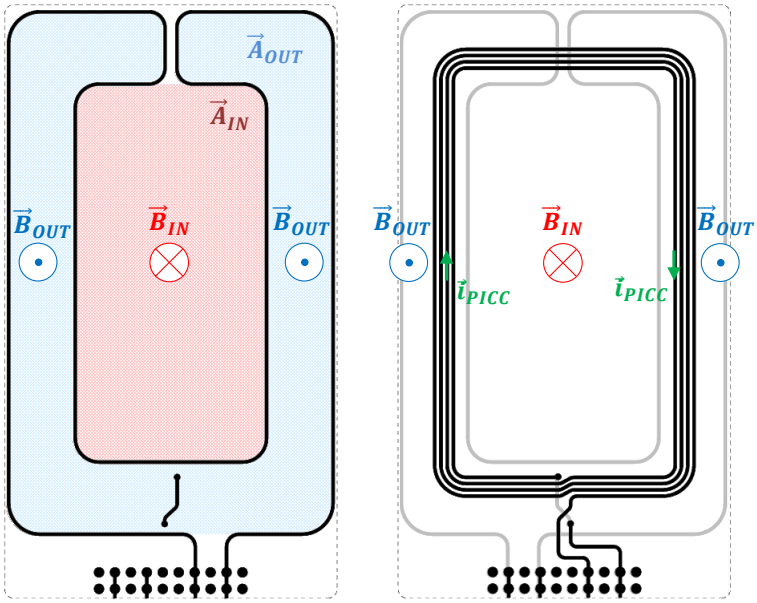


Figure 5.7: Pick-up Coil (left) and Main Coil, with underlying Pick-up coil (right) of the RefPICC antenna - Class 1 (adapted from [2])

The figure above also demonstrates the design concept of the *Pick-up Coil*: The induced current, $\vec{i}_{PICC}$ in the *Main Coil* (bottom layer) is the reason for a magnetic field $\vec{B}_{IN}$ in the area of $\vec{A}_{IN}$ and an additional magnetic field $\vec{B}_{OUT}$ in the area of $\vec{A}_{OUT}$ in the *Pick-up Coil* (top layer). This magnetic field, due to *Lenz's law*, creates a current in the pick-up coil, which remains negligibly low because of the coils high terminating impedance.

The part of the PICC's magnetic field influencing the area $\vec{A}_{IN}$ is contrary to the magnetic field's part penetrating the area $\vec{A}_{OUT}$. As the depiction above suggests, both areas are of the same size, so that the voltages induced in both areas are equal with opposing signs.

$$\vec{A}_{IN} = -\vec{A}_{OUT} \tag{5.2}$$

$$u_{IN}\left(\vec{B}_{IN}, \vec{A}_{IN}\right) = -u_{OUT}\left(\vec{B}_{OUT}, \vec{A}_{OUT}\right) \tag{5.3}$$

Due to the pick-up coil's layout, the circuits surrounding both areas are basically connected in series. The voltages, u_{IN} and u_{OUT} are aggregated with a sum equaling zero. They cancel out the effects of the main coil's magnetic field on the *Pick-up Coil*. In other words, the pick-up coil does not feature a magnetic coupling, M, with the main coil.

5.2.2 Fundamentals of Synchronization

After resolving the question regarding picking up the signal the question arises why it is necessary to synchronize PCD and PICC. An ordinary passive RFID tag receives, as mentioned in chapter 3, its power and clock from the electromagnetic field of the RFID reader (or PCD). The time reference is defined by the reader, the tag responds synchronously to the alternating electromagnetic field by changing its load. The de-facto synchronicity is therefore inherent in the principle of system interaction of a passive RFID tag (PICC) and an RF reader (PCD).

In ALM, the phase shift between the PCD's magnetic field and the carrier a PICC uses for generating an active load modulation signal is a key parameter (referred to as relative phase drift $\Delta\varphi$). Especially during active transmission and communication of a weak PCD electromagnetic field, it is not directly observable in presence of a strong active transmitting PICC. A high driven current in the PICC is affecting the PCD-field to a degree where it is left non-observable from the PICC's point of view. This leads to a desynchronization of internal clocks of PCD and PICC and the phase of the PICC antenna current tends to drift away.

Even more, as older readers use only the AM information provided to decode the signal, a proper carrier/clock recovery was not necessary. However, latest and state-of-the-art readers use IQ-demodulation where a phase information is indispensable

So in order to work properly a modulator and a demodulator need to know both, the exact symbol phase and the exact symbol rate, and they also need to know the exact carrier frequency f_C and carrier phase $\varphi(t)$. In practice, the receiver as well as the transmitter rarely have the same timing and carrier clocks or information of their counterpart, unless there are proper synchronization techniques provided, mostly referred to as *phase-locking*. A control system which performs phase-locking is widely known as PLL.

A common PLL consists of the following major blocks:

1. **Phase Detector: Phase-Error Generation** - The initial operation derives a phase difference between the phase $\varphi(t)$ of the reference signal and the estimated feedback phase $\hat{\varphi}(t)$ of the receiver. The actual signals are $s(t) = \cos(\omega_{lo}t + \varphi(t))$[5] and $\hat{s}(t) = \sin(\omega_{lo}t + \hat{\varphi}(t))$, but only their phase difference is of interest in the synchronization procedure. In control systems the difference is known as *control error*, in case of a PLL also called ***phase-error*** $\Delta\varphi(t) = \varphi(t) - \hat{\varphi}(t)$. To derive a phase-error and to implement a *phase detector*, there are various known methods. [31]

2. **Loop Filter: Phase-Error Processing** - The next block in the loop obtains information, such as trends from the actual phase-error. This processing step usually suppresses random noise and other undesirable components of the phase error signal for example by using different filters.

3. **Voltage-Controlled Oscillator (VCO): Local Phase Reconstruction** - The last operational block is the so-called VCO[6], which regenerates a local phase signal from the processed phase-error to match the incoming phase $\varphi(t)$. The control system attempts to force $\Delta\varphi(t)$ equal 0 by adjusting of the local phase $\hat{\varphi}(t)$ so that $\hat{s}(t)$ equals $s(t)$. Again, along with VCO's there are a multitude of different methods to regenerate a local clock.[7]

The main premise of all phase-locking mechanisms is an inevitable finite delay in all practical implementations. By regenerating the local phase $\hat{\varphi}(t)$ a PLL will immediately try to predict the incoming reference phase $\varphi(t)$ and then proceed to calculate the new phase error $\Delta\varphi(t)$. The better and faster the tracking of phase deviations, the more susceptible the whole mechanism will be to random noise and distortions.
There is no optimal solution, rather a trade-off between the mentioned opposing effects which need proper consideration (e.g. the appearance of the transmitted signals) when designing a synchronization system.
For the most practical purposes it is necessary to generate an estimate of either the incoming signal's clock or the phase error. Furthermore a distinction can be made, whether phase detectors are used to recover a symbol clock (clock extraction for timing/clock recovery) or recover the phase of the carrier (carrier recovery), respectively. [31]

The EXG vector signal generator offers a variable reference input for signals up to 50 MHz with a resolution of in $f = 0.1$ Hz using a PLL working according to the the basic principle explained above. Further intrinsic informations about the underlying reference and the synthesizer circuitry can be found in [33].

[5] ω_{lo} being the local oscillator angular frequency
[6] If in digital form also referred to as NCO, N controlled oscillator.
[7] The various methods to derive a phase-error as well as to regenerate a local clock shall not be part of this thesis.

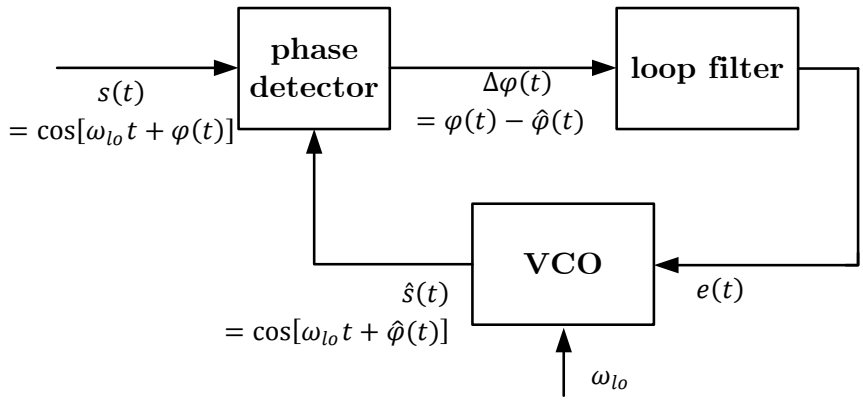


Figure 5.8: General structure of a phase-lock loop, comprising phase detector, loop filter and VCO

5.2.3 Clock Recovery Circuit

There are many possibilities such as designing an analog or digital PLL unit, its more advanced derivative, the *Costas Loop*[8] or even an integrated circuit such as Austrian Microsystems' *AS3922*[9] RFID reader. However, Agilent's *N5172B EXG* vector signal generator seems to be the best fit for a compact and flexible all-in-one device.

With the additional *Reference In* option, phase-locking on the desired 13.56 MHz carrier signal seems possible. The synchronization accuracy as well as the locking range are totally acceptable considering the carrier frequency being stable and possible phase drifts staying within limits defined in ISO 14443/10373. ± 1 ppm matches ± 13.56 Hz which corresponds to a phase drift of $< 5\,^{\circ}$ over one millisecond. Pretesting proofed a maximum locking range of about 100 Hz, far enough for the intended purpose.

The input specifications can be seen in the following table:

Input frequency	1 to 50 MHz (in multiples of 0.1 Hz)
Stability	follows the stability of external reference input signal
Lock Range	± 1 ppm
Amplitude	> -3.0 to 20 dBm, nominal
Impedance	50 Ω, nominal
Waveform	sine or square

Table 5.3: *Reference In* specifications [34]

The specifications of table 5.3 make a signal pre-processing step mandatory. The *Clock Recovery Unit* needs a high impedance input to keep currents in the coil low. A 50 Ω output impedance is needed, the amplitude input range is limited between 223 mVp and 3.16 Vp. To get most stable and verifiable results the generated clock signal shall have a stable, defined amplitude, insensitive to variation in the PCD electromagnetic field H. Again, testing revealed very low sensitivity to broader amplitude variations as well as to lower input amplitudes.

The Clock Recovery Circuit basically needs to meet the following challenges:

1. provide a high input impedance for the main circuitry to prevent influencing the existing PCD-PICC-system too much.
2. provide a conventional 50 Ω output impedance
3. cover a wide range of signal amplitudes, especially relevant regarding ISO/IEC standards mentioned in [3]

[8] a PLL based circuit, used for carrier phase recovery from suppressed-carrier modulation signals, e.g double-sideband suppressed carrier signals.

[9] boosted NFC IC employing active load modulation by *AMS*, developed in cooperation with Infineon Technologies

4. provide an output-signal with stable amplitude
5. provide a coherent and stable phase relation between the signal $V_{PickUp} = V_{in}$ induced in the *Pick-Up* antenna, corresponding the clock recovery unit's input signal, and generated clock signal V_{out}, so basically between circuit in- and output.

Basic Circuitry

The simplest, yet most efficient way to generate a clock signal is to use an ordinary comparator. In order to meet the prior postulated requirements it was decided to use a single/dual supply comparator with rail-to-rail output, working on single supply.

Linear Technology's *LT1719* [41] fits the basic demands and offers moreover an ultrafast propagation delay of 4.5 ns at a 20 mV overdrive (figure 5.9).

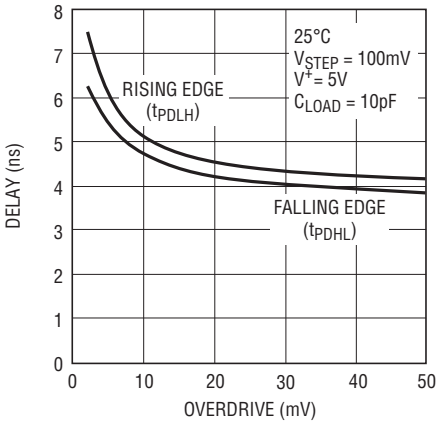


Figure 5.9: LT1719's propagation delay vs overdrive (borrowed from data sheet [41])

The ISO/IEC 14443 specified range of PICC and PCD operating field strengths, both being 1.5 to 7.5 A/m, results in the induced voltage being in a range of 1.364 and 6.818 Vpp at an operating frequency of 13.56 MHz for a class 1 antenna. Measurements revealed, the induced voltage in the Pickup antenna $V_{PickUp} = V_{in}$ due to the PCD field is even smaller. Instead of a usual factor of 1.1 (for more elaborate information see [1]) the factor increases to 1.77 [10], which makes the signal appear smaller in amplitude.

With an input supply voltage from minimum 2.5 to maximum 10.5 V and a resulting input voltage range of minimum $V_{EE} - 0.1\,\mathrm{V}$ and maximum $V_{CC} - 1.2\,\mathrm{V}$ as well as the demand to utilize as few external power supplies as possible, it was determined to use V_{EE} as GND and $V_{CC} = 10\,\mathrm{V}$. Due to the selected supply voltage levels it is necessary to elevate the input voltage to a mid-level of 5 V.

[10] Measurements were made during this thesis, by increasing the H-field step-by-step from 0.5 up to 10 A/m and measuring V_{PickUp}

By using a serial capacitor C_1 for DC-decoupling and a voltage divider the input signal from the antenna is modulated to a stable offset potential of +5 V. At the operating frequency, the divider along with the capacitor C_1 creates an input impedance similar to a scope-probe.

To provide the 5 V reference for the positive comparator input two options were available:

1. a voltage divider usable for generating a reference voltage level dependent on the supply voltage V_{CC}, of course leading to increased vulnerability against distortion and ripple from the supply voltage, or
2. using a Low Dropout Regulator (LDO) to produce a robust reference but being uncoupled from variations in V_{CC} and therefore from the input signal V_{in}.

The decision fell on the latter as it proved to be the much more reliable option for the ultimate purpose. Furthermore no substantial variations in supply voltage and therefore negligible influence of the phase coherence are to be expected. The chosen LDO is Texas Instruments' *LP2985* which provides low noise and low dropout voltages as well as a low standby current [43]. The comparator also comes with its own output supply voltage, which is provided by a second *LP2985*. In addition, the same voltage regulator supplies the downstream buffer *BUF602* [42], a push-pull stage to provide the required 50 Ω environment, along with resistor *R*6.

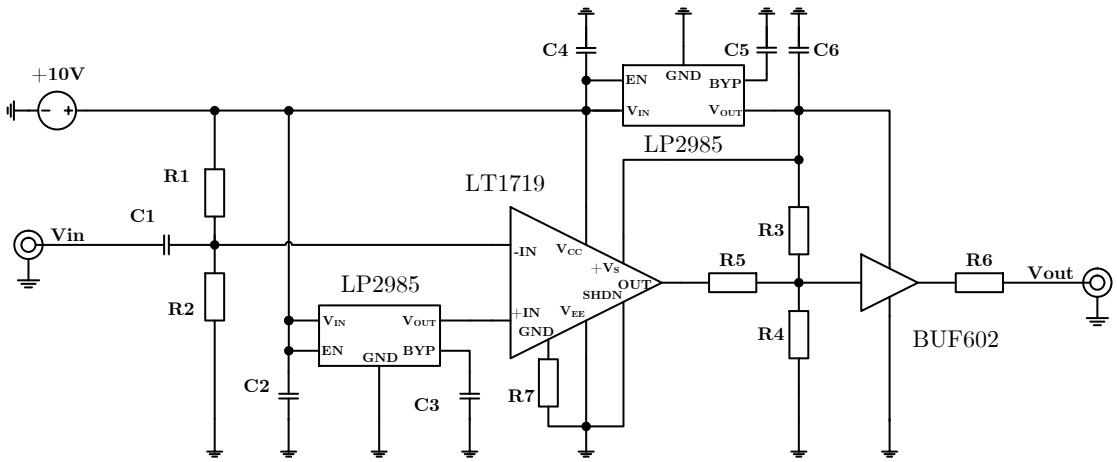


Figure 5.10: Schematics of the Clock Recovery Circuit also referred to as *Conditioning Board*

The vector signal generator is able to add phase offset to the reference input signal V_{out}, thus rendering it unnecessary to create a predefined phase-relation between input and output.

A simple simulation with Linear Technology's *Spice* shows promising results:

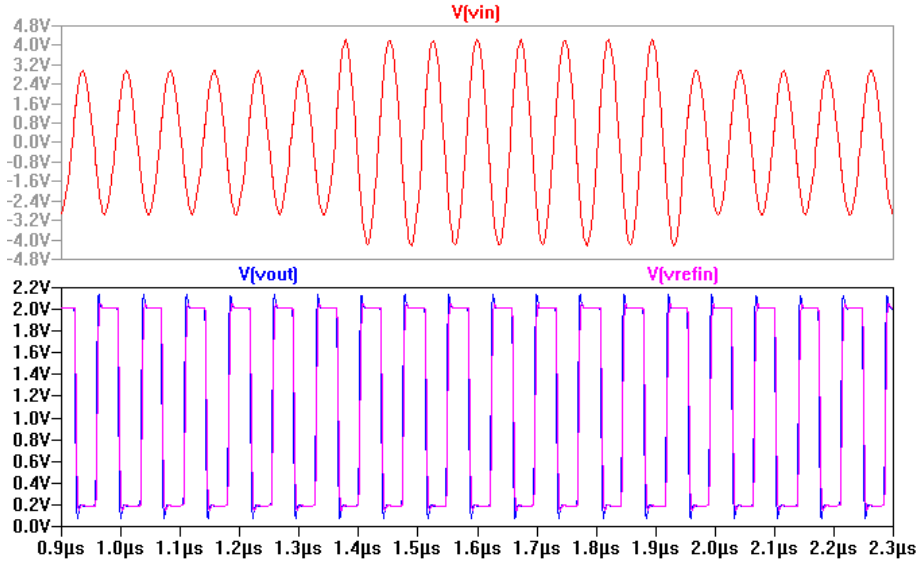


Figure 5.11: Picked-up signal with $m = 30\%$ at H_{max} according to ISO/IEC 14443 along with output signal and signal at the Ref-In port of the vector signal generator

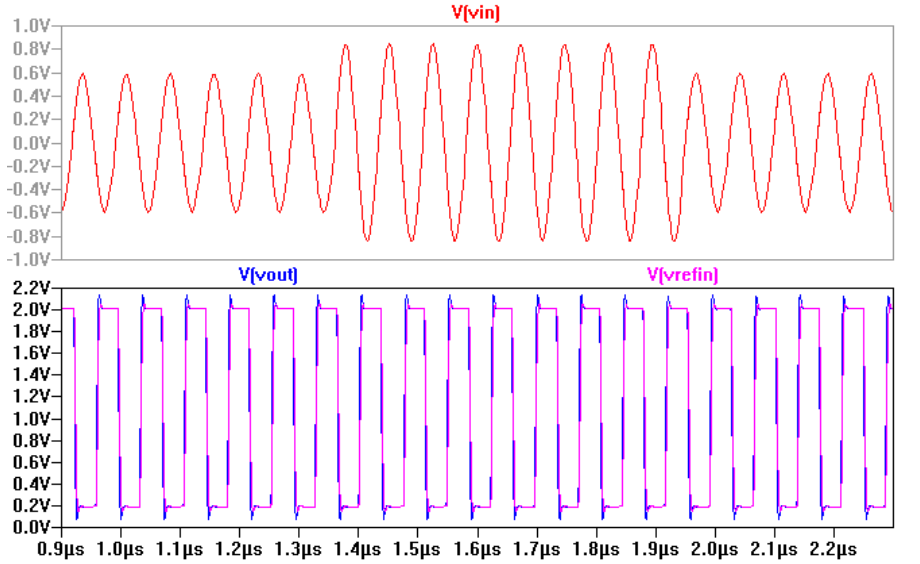


Figure 5.12: Picked-up signal with $m = 30\%$ at H_{min} according to ISO/IEC 14443 along with output signal and signal at the Ref-In port of the vector signal generator

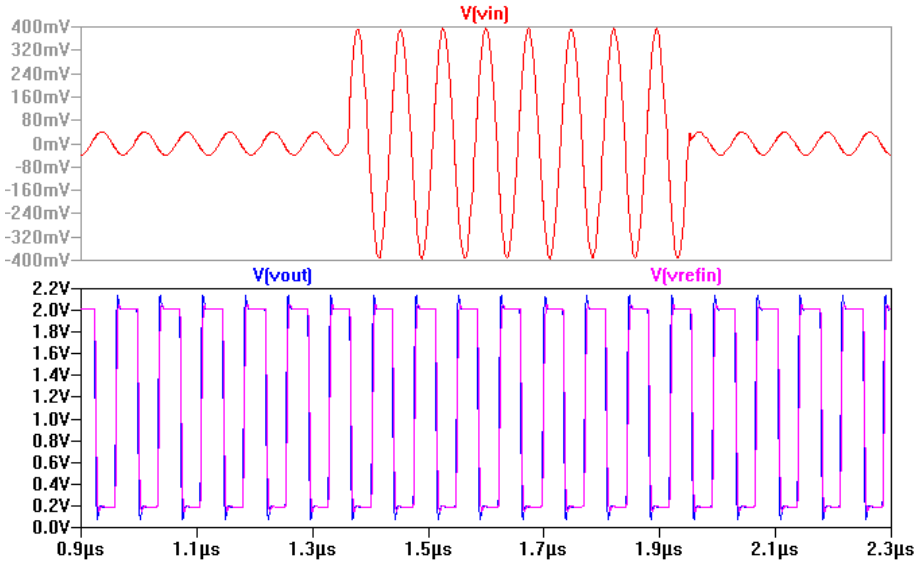


Figure 5.13: Picked-up signal with $m = 90\%$ at $H = 0.7\,\mathrm{A/m}$ or equivalent $0.385\,\mathrm{Vpp}$. according to ISO/IEC 14443 along with output signal and signal at the Ref-In port of the vector signal generator

Further considerations and conclusions

The circuitry was constructed regarding aspects coming from *WG8/TF2* group aspects to keep proposals fairly simple and as comprehensible as possible. There is of course room for further considerations such as pre- or post-filtering of the signal. The idea however was to keep the genuine signal as unaffected as possible.

The work with the signal vector generator proved to show limitations regarding its use as an adequate PLL alternative. Although the device is able to lock onto the external signal and even maintains coherency during minor variations in amplitude or frequency, major shortcomings were revealed in the process:

While the *Reference Input* port is denoted to work as a PLL the device, in fact, only locks onto an external frequency (as shortly outlined before in this chapter). So, a more accurate term would be *frequency locking*. The signal is detected at its input port and a stable phase coherency is established. As a consequence, a random phase between input signal and the further generated signal at the device's RF output port can be observed. Every time the reference gets lost or is non-existent, the device switches to its internal 10 MHz clock leading to a phase-drift.

This is a major drawback for the use in a test-bench, leading to a severe restriction of the field of applications and test-signals. The lack of a PCD electromagnetic field and

signal $V_{CalCoil}$ as for example in case of a *field reset*. While this can be circumvented by creating according test-signals in a test-environment, this creates problems in practical uses, for example the testing of an actual reader.

An envisaged possibility might be a real PLL in parallel to the recovery circuit, creating a stable phase-locked signal regarding the PCD electromagnetic field as and when required superimposed on the recovered clock or even different methods such as described in [32].

5.3 PICC Emulation

The following section focuses on the proper PICC emulation for the test bench. Basic requirements are the ability to create and implement existing and proposed test patterns compliant to ISO/IEC 14443, as well as any practically relevant modulated signal curve as defined in [3].
Furthermore the emulated signal is required to gain and maintain a stable phase coherency with the PCD emulated signal over a defined period of time[11].

The following subsections examine the postulated and defined requirements, trying to offer a practicable solution which unifies all aspects mentioned above.

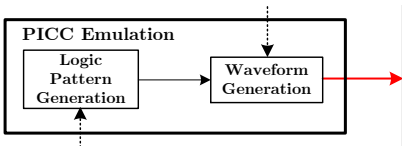


Figure 5.14: PICC Emulation

5.3.1 Proposed PCD Reception Tests

The impact of phase drift on the bit representation and coding has been a topic of research priorly, resulting in following requirements regarding bit grid violations and bit coding violations.

1. *Bit coding* violation is mostly valid for Type A communication beyond 106 kbit/s and all bit rates in Type B communication. A maximum tolerable phase drift and criterion for bit coding violations might be 30° over one frame[12].
2. In contrast, ISO/IEC 14443 currently only defines *bit grid* for Type A and 106 kbit/s. Type B on the other hand defines *bit boundaries*. The criterion for bit grid violation is presumably 0.1 Elementary Time Unit (etu) over one frame.

Consequently, not only the necessity of potential adaptations of current ISO/IEC requirements, but also the necessity to evaluate a potential phase drift during data transmission between PICC to PCD. Algorithms which can measure the phase drift of a load modulated signal can be utilized to evaluate potential bit grid and bit coding violations ([12]).

[11] *Stable* and *defined period of time* are characteristics, to be defined over the course of the upcoming subsections

[12] *Sequence of data bits and optional error detection bits, with frame delimiters at start and end* [4]

The considerations mentioned above lead to a WG8/TF2 amendment [5] in ISO/IEC 14443-2, quoting:

> *During the whole PICC response, the PICC field shall fulfill the following requirements when measured as described in ISO/IEC 10373-6 for each first half of the subcarrier period:*
>
> - *the amplitude of the PICC field shall be at least 0,6 times Voltage Load Modulation Amplitude (VLMA), PICC depending on the PICC class*
> - *the phase of the PICC field shall be both:*
>   - *between $-175°$ and $+5°$ relative to the phase of the PCD operating field,*
>   - *between $-30°$ and $+30°$ relative to the phase of the PICC field at the beginning of the PICC response."*
>
> *The PCD shall be able to receive a PICC response with the following characteristics during the whole PICC response, when measured as described in ISO/IEC 10373-6 for each first half of the subcarrier period:*
>
> - *amplitude of the PICC field of at least 0,5 times VLMA, PICC depending on the supported class*
> - *phase of the PICC field both:*
>   - *between $-180°$ and $0°$ relative to the phase of the PCD operating field,*
>   - *between $-35°$ and $+35°$ relative to the phase of the PICC field at the beginning of the PICC response.*

For PCD reception tests regarding ALM and PLM - among a variety of other defined tests - phase analysis, tests to evaluate the minimum and maximum V_{LMA} and bit rate dependent tests over the whole PICC response up to half a subcarrier period of each etu were proposed in WG8/TF2 amendment [5].
These tests shall also contain differing initial phase tests to evaluate if Receive (RX) command of PCD can cope with the information in I- and Q-channels as well as positive and negative phase drifts for all bit rates and both communication types, Type A and Type B.

Bit-Dependent Tests

The bit dependent tests as mentioned in section 5.3.1 comprise different test patterns of varying communication methods (*Type A*/*Type B*), polarity of the ALM signal (bipolar/unipolar) as well as the different bit rates (106 - 848 kbit/s):

- Type A, 106 kbit/s:

  - Bipolar: ±35° over four subcarriers per etu
  - Bipolar: ±35° over the entire PICC response
  - Unipolar: ±35° over each subcarrier-half per etu
- Type B, 106 - 848 kbit/s and Type A, > 106 kbit/s:
  - Bipolar: ±35° over the entire PICC response
  - Unipolar: ±35° over each subcarrier-half per etu

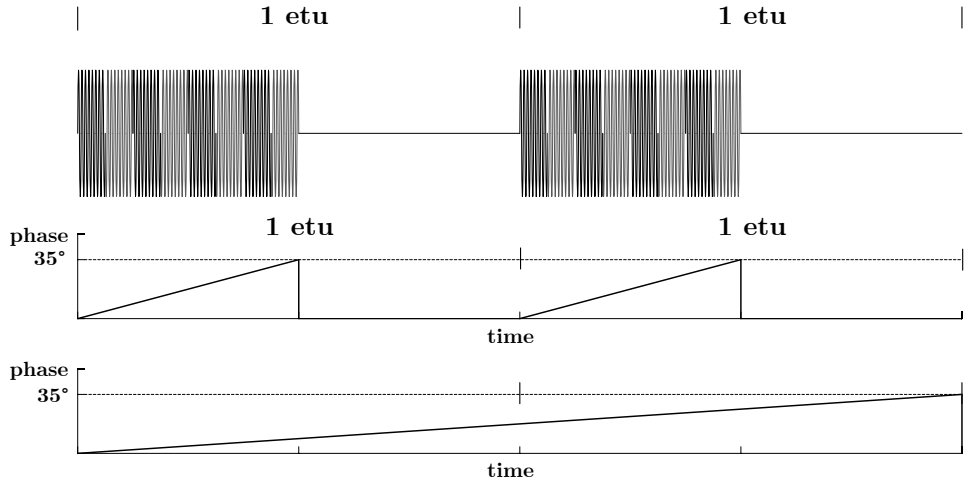


Figure 5.15: PCD reception test case 1: Type A, 106 kbit/s, bipolar modulation

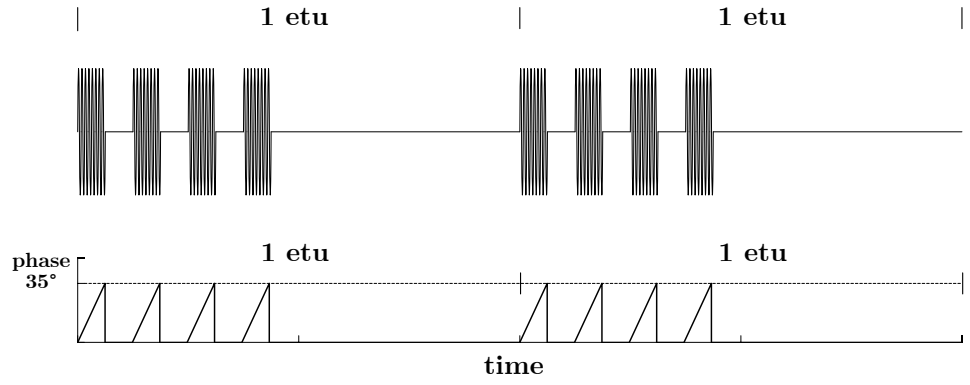


Figure 5.16: PCD reception test case 2: Type A, 106 kbit/s, unipolar modulation

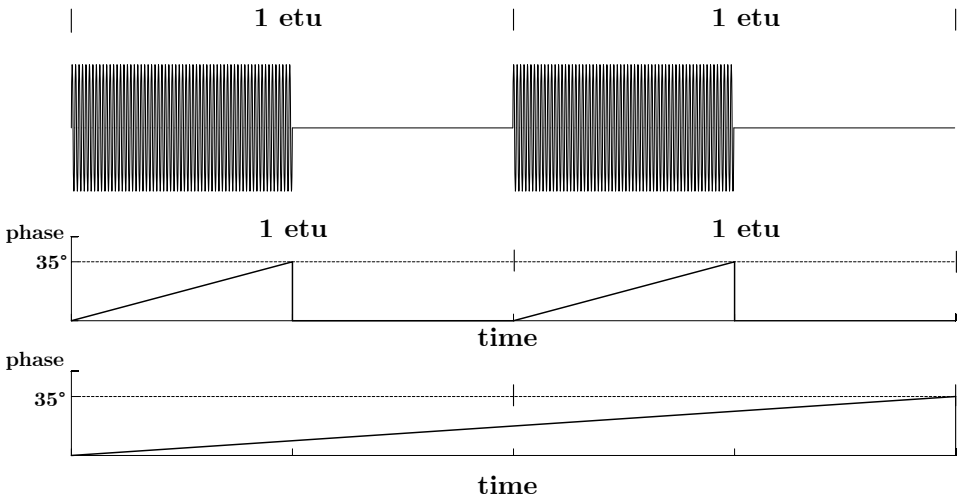


Figure 5.17: PCD reception test case 3: Type A, > 106 kbit/s and Type B, all bit rates

5.3.2 Realization via Vector Signal Generator

In order to verify not only PLM but also ALM signal behavior on a test PCD assembly, the PICC emulation shall not only be able to synchronize with the PCD emulation device but shall also be able to generate the previously mentioned proposed signals and signal behavior.

The Vector Signal Generator *Agilent N5172B EXG* with its huge offer of optional features is not only able to recreate exactly these proposed test cases [12] but comes also with even another very valuable option: a flexible reference input accepting periodic signals in a frequency range of 1 to 50 MHz, as already pointed out in section 5.2.

Figure 5.18: EXG N5172B Front Panel [36]

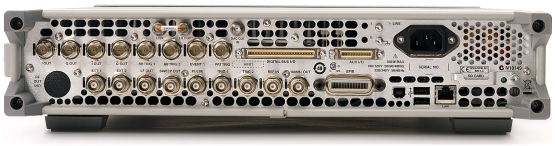


Figure 5.19: EXG N5172B Back Panel [36]

The WG8/TF2 group strives always for the most simplistic way, easy to implement,

easy to verify with high reproducibility, accuracy and durability. These very reasons, along with the thoroughly investigated options and behavior of the EXG Vector Signal Generator [34] makes the device a very interesting option to be used as a complete all-in-one solution for the PICC emulation process. The EXG unifies pattern logic and waveform generation as well as offers a flexible reference input with up to 50 MHz to allow phase synchronization with the PCD magnetic field.

The Vector Signal Generator *Agilent N5172B EXG* with integrated Baseband Generator (BBG) (Option 653) [34] uses exactly this method to generate and provide a modulated signal at its RF output. The data used for generating the I and Q signals can be provided internally by using Matlab^{TM}to create proper baseband data and Standard Commands for Programmable Instruments (SCPI) to transfer the data set via Ethernet or General Purpose Interface Bus (GPIB)/Institute of Electrical and Electronics Engineers (IEEE)-488 to the device [37].

Matlab^{TM}Implementation

The amplitude and phase of the sine wave generated by the synthesizer section of the vector signal generator can be controlled by discrete voltage levels at the I/Q inputs. For the sake of simplicity these discrete levels are assumed to be infinitesimally small for the next considerations:

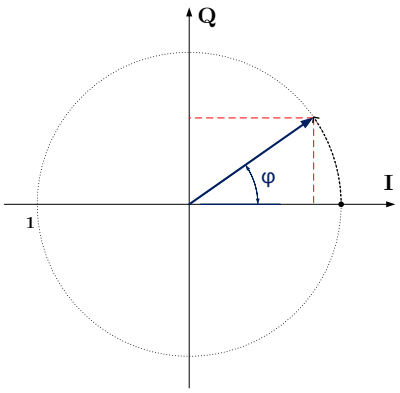


Figure 5.20: Phasor diagram representing I and Q of the I/Q modulator

The vector (or phasor) diagram is a useful tool to help visualizing how the sine wave is modified. The phasor diagram is interpreted as follows: the amplitude of the signal is represented by the length of the vector, the phase of the signal is represented by the angle relative to the in-phase, or I axis. All modifications happen within the range of the unit circle.

A short example shall help to understand the procedure, starting from a desired signal

in its time domain, transforming this signal to its according IQ data representation and finally downloading the IQ data via SCPI to the device.

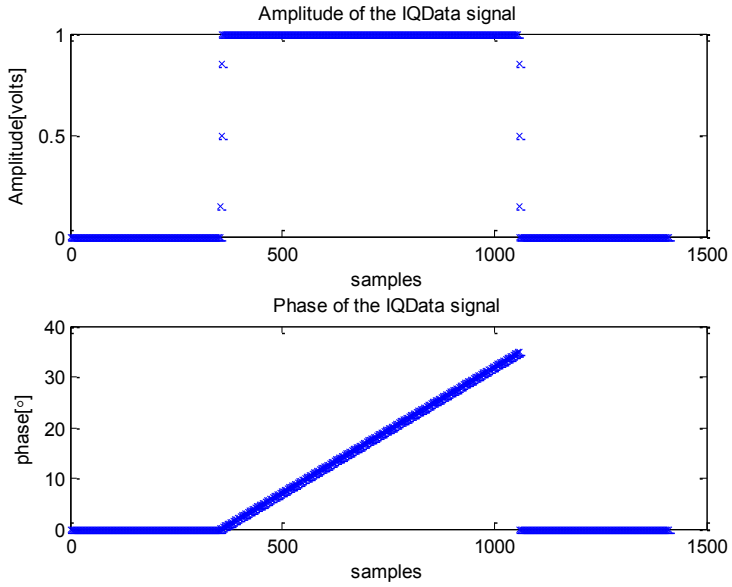


Figure 5.21: Matlab representation of the data signal

A short summary for the code (figure 5.22) creating the simple data signal:
The code enables generating of a vector signal, in other words, a pulse signal with an amplitude of 1 and a phase drift from 0° to 35° over one etu at a bit rate a 106 kbit/s. By adding zeros before and after the pulse the total period is extended to 2 etu. Such concatenating can be done deliberately.
In order to avoid too high overshoots at the EXG output the edges of the pulse are softened by using a few samples to interpolate the transitions from high to low and vice versa. A simple raised-cosine filter is used for this procedure.

In the end one complex IQ data vector is generated (figure 5.21), the EXG Vector Signal Generator can process. The function needs the IQ data vector as well as the ARB[13] sample clock f_S as transfer parameters. The sample clock is based on the time resolution or the bandwidth of the signal. It is the basis for the length of all data signals to be created further on.

All other steps provided to establish connection via LAN/GPIB or download the IQ-data signal onto the device is possible via Matlabs *Waveform Download Assistant*, which can be found, along with examples, on [39].

[13] Arbitrary waveform unit within the EXG to create various modulation signals

```
function [IQData fs] = create_waveform();

 %% Definitions
fc = 13.56;          %carrier frequency
BR = fc/128;         %Bitrate
etu = 1 / BR;        %1 etu of actual Bitrate BR
sig_length = etu;    %Signal length

fs = 75e6;           %ARB Sample Clock
N = floor(sig_length * fs); %defines number of samples used for data signal
fs = N / sig_length;  %recalc of fs due to integer samples

%% calculation of the data signal
phi = 35/180*pi;           %defines wanted phase drift
samples = linspace(0,1,N); %defines a sample vector
I = cos(samples*phi);      %calc I
Q = sin(samples*phi);      %calc Q

IQData = I + j*Q;       %defines the complex IQ vector

%%Define Rise and Fall time
n=4;                              % defines the number of points in the rise-time & fall-time
tr=-1:2/n:1-2/n;                  % number of points translated to time
rise=(1+sin(tr*pi/2))/2;          % defines the pulse rise-time shape
on=ones(1,length(IQData)-2*n);    % defines the pulse on-time characteristics
fall=(1+sin(-tr*pi/2))/2;         % defines the pulse fall-time shape


%Concatenate vectors
am = [rise on fall];          % adds the softened rise/fall time to the pulse
zero_vector = zeros(1, floor(length(samples)/2)); %defins zero-vectors for the data signal
IQData = [zero_vector IQData.*am zero_vector]; %adds zeros 1/2etu before/after the pulse

end
```

Figure 5.22: *.m-file to create a signal with constant amplitude and phase drift over 35°

Verification Measurements

This subsection shows the verification procedure using a test signal generated with the *Agilent EXG N5172B* vector signal generator. The procedure consists of three test scenarios which are:

1. The test signal is directly applied to the oscilloscope without the use of the ISO test PCD assembly.
2. The test signal is applied to the active RefPICC (as mentioned in section 5.1) on the ISO test PCD assembly without PCD magnetic field
3. The test signal is applied to the active RefPICC on the ISO test PCD assembly with activated PCD magnetic field.

In principle, the utilized test signal is the same pulse as mentioned above:

- Amplitude: $1\,\mathrm{V_{pp}}$
- Phase: $\varphi_{start} = 0°$, $\varphi_{end} = 35°$
- Duration: $t_{on} = t_{off} = 9.44\,\mu\mathrm{s}$

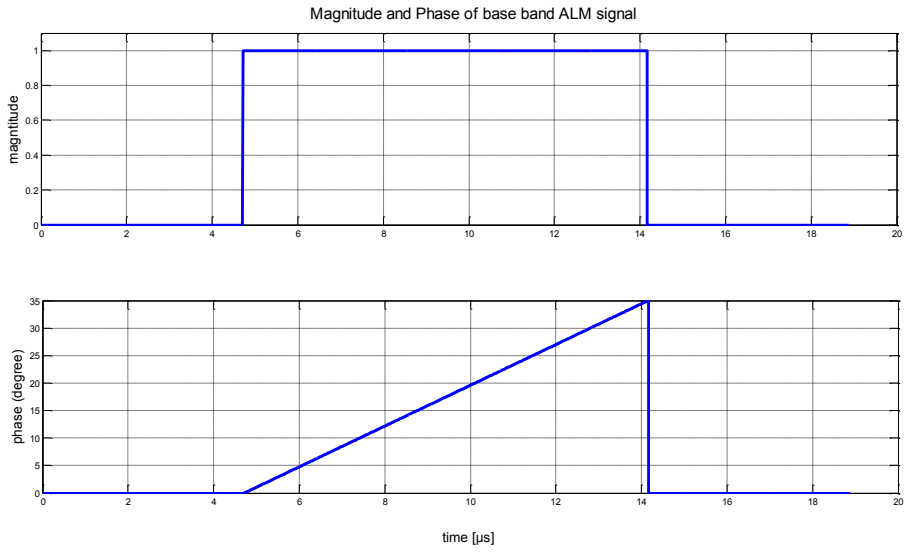


Figure 5.23: Baseband test signal, magnitude (above) and phase (below)

1) Test without ISO test PCD assembly

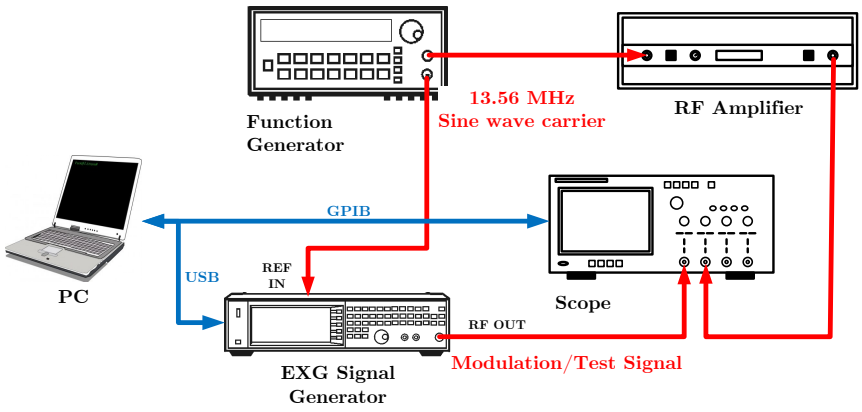


Figure 5.24: Test Setup without ISO test PCD assembly.

The setup provides both, PICC and PCD emulation devices synchronized using the reference input of the *EXG Signal Vector Generator* and the synchronization output of the chosen PCD-emulating AWG.
The signal provided by the PCD emulation unit, is a 13.56 MHz sine wave carrier fed into an amplifier. The synchronized EXG utilizing its internal baseband generation unit with a downstream I/Q modulator emulates the PICC, providing the prior defined test signal, referenced to as *modulation signal*.
Both device outputs, terminated with 50 Ω are directly fed into channels of a scope with a reasonable high sampling rate[14].

[14] *Nyquist-Shannon Theorem of sampling*: for baseband signals $f_{sample} \geq 2 \cdot f_{max}$ with f_{max} being the highest appearing frequency of the useful signal

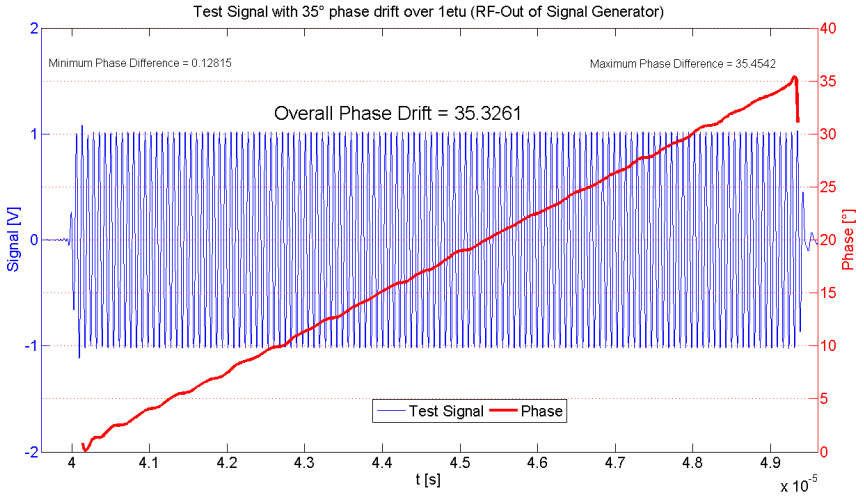


Figure 5.25: Test Setup without ISO test PCD assembly.

Figure 5.25 shows both signals with a resulting phase drift of 35° over 1 etu. The reference (carrier) signal is generated to be in phase with the first zero-crossings of the modulation signal (test signal) to reach an initial phase offset of zero.

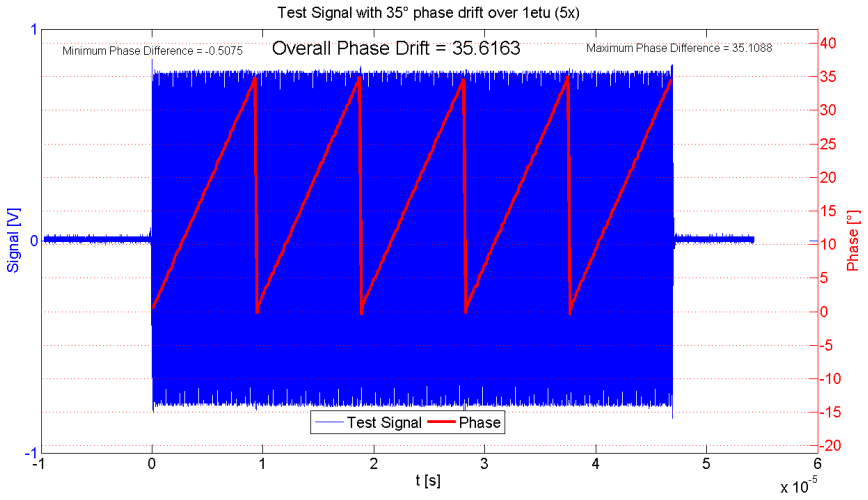


Figure 5.26: Test Setup without ISO test PCD assembly.

The phase is calculated in a similar manner as mentioned in previous chapters prior. During the test signal's transient oscillation from a flat line to its steady state, the argument of the Hilbert transform underlies a certain oscillation. Compared to the steady reference HF sine signal this results in a jitter when calculating the difference of both arguments whenever signal-transitions occur. This leads to uncertainties in these sections and raises the general question if and how to assess transients in this

context.

Figure 5.26 shows a signal sequence of five consecutive bursts with $t_{off} = 0$ and a phase drift from 0 to 35 ° each over 1 etu.

The signal vector generator is able to create the demanded signal within an acceptable transition width which equals a few μs, with extra *Narrow Pulse Option* even less then 10 ns). Consequently, so higher bit rates are easily achievable.

2) Test without PCD magnetic field

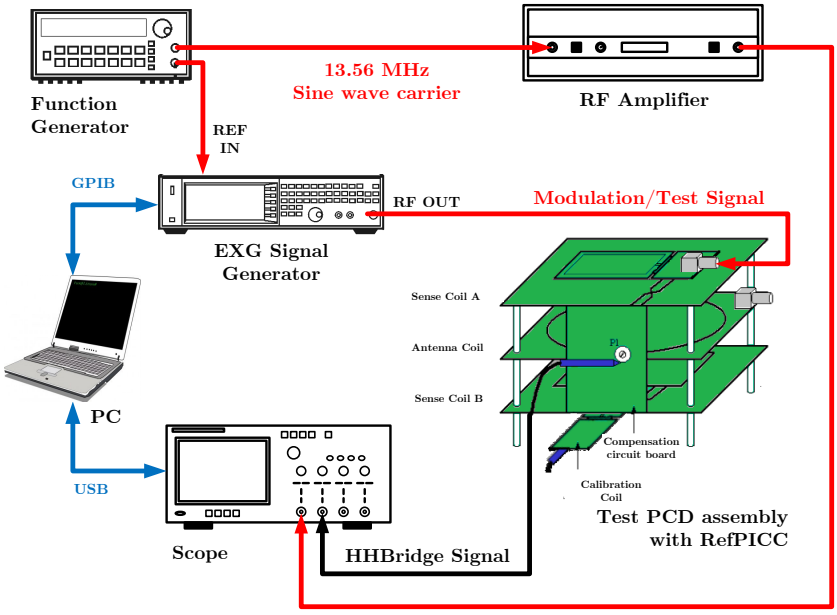


Figure 5.27: Test Setup without PCD magnetic field.

The modulation signal is applied to the current source of the Extended RefPICC acting as DUT on the ISO/IEC Test PCD assembly. However the sine wave carrier is not applied to the PCD antenna, thus the PCD is not generating a magnetic field. Again the reference sinusoidal carrier signal is generated to be in phase with the first zero-crossings of the modulation signal.

Figure 5.28 shows that also this test's result meets the expectations. The modulation signal is no longer the measured parameter, instead the voltage V_{Sense} at the Sense Coil is now obtained as it is representing the PICC current an thus the modulation signal again.

Rise/fall times of the modulated signal appear noticeably larger due to the signal path

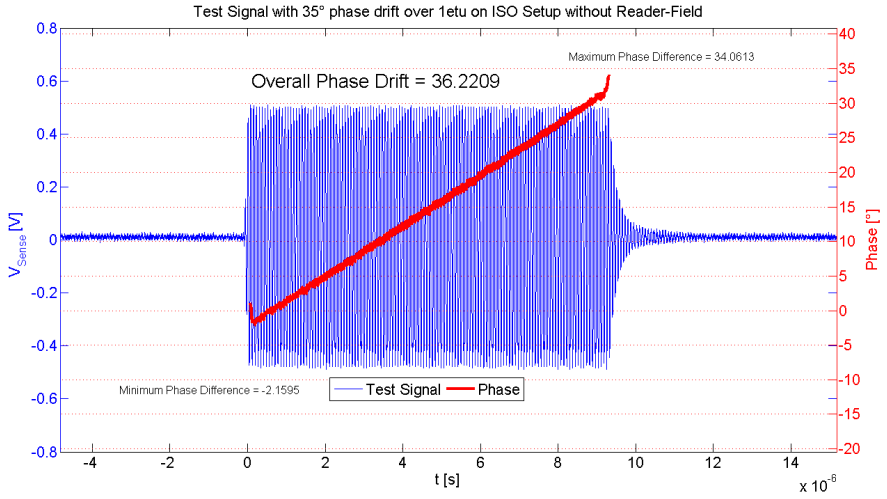


Figure 5.28: Test Setup without PCD magnetic field.

across the PICC. The transient behavior is influenced which leads to now even larger distortions of the calculated phase drift in these areas. The targeted phase shift of 35° however can be met.

3) Test with PCD magnetic field

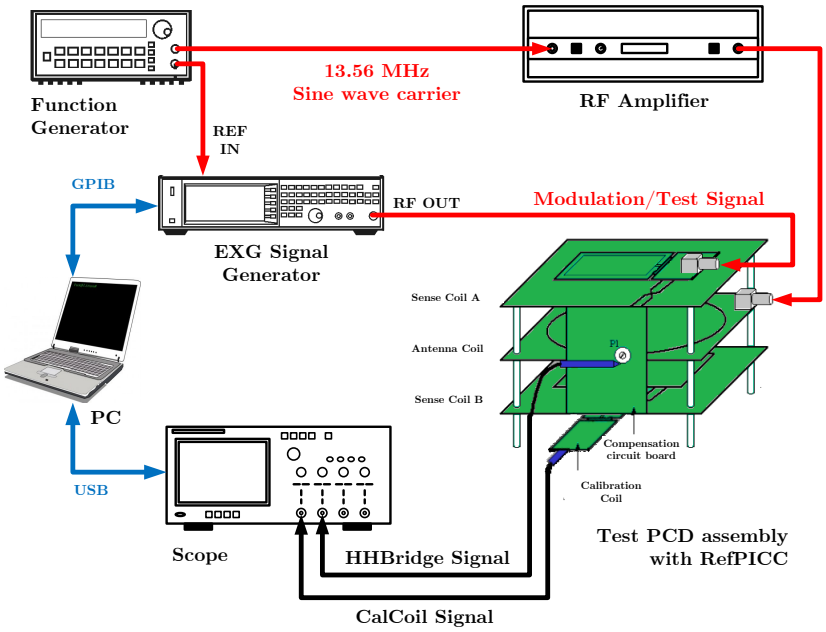


Figure 5.29: Test Setup with PCD magnetic field.

The test signal is fed into the current source of the Extended RefPICC, in this case also with the sine carrier of 13.56 MHz applied to the Test PCD assembly thus generating a magnetic field. Both relevant measurands are now captured from the Test PCD assembly, V_{Sense} from the Sense Coil and $V_{CalCoil}$ from the Calibration Coil.

Figure 5.30 shows distinct impacts on the signal V_{Sense}. The signal is noticeably affected by the present PCD magnetic field. Also, the voltage V_{Sense} can no longer be considered as direct representation of the PICC current. The superposition of an active PCD magnetic field and as a consequence thereof changes in the induced voltages and current in the PICC lead to an altered magnetic field signal measurable at the *Sense Coil* and corrupting the representation of the PICC current I_{PICC} and thus a relative phase drift measurement.

An aimed phase drift is still present, due to the interference. the phase can be seen distorted and is not linear over a whole etu.

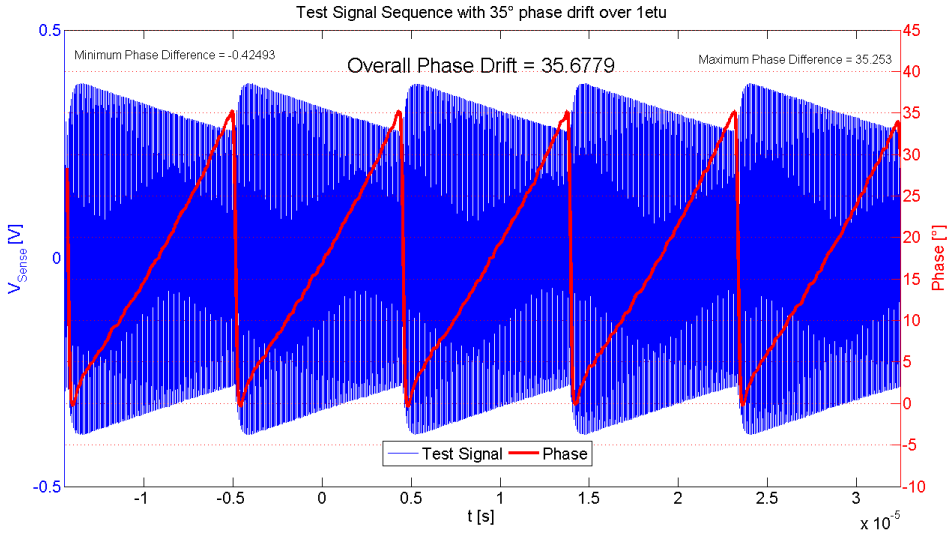


Figure 5.30: Test Setup without PCD magnetic field.

Concluding remarks

- It is possible to create proper test signals regarding PCD reception tests with the EXG Vector Signal Generator. A proof-of-concept was made which show-cased the possible usage of the present Extended RefPICC in combination with the existing ISO/IEC Test PCD assembly.
- The *Extended RefPICC* is able to maintain predefined phase specifications and can be considered a device being usable for future phase drift measurements and reception tests.
- The *Sense Coil* signal is based on the interaction between both, PICC and PCD, dependent on different parameters such as transponder antenna sizes, quality factor Q, resonance frequency f_{res} or PCD magnetic field, in reality existing of *noise vector*[15], V_{Noise} and the real representation of the PICC voltage, V_{PICC}. Further signal-processing steps are required to gain a real representation of the PICC current. (c.f. section 5.4.2)
- The phase calculation is a matter of calculation techniques and approaches. Transients as well as the calculation of a phase in every single sampled data-point might be inefficient and not expedient.

[15]The *noise vector* can be seen as a product of deficiencies in metrics of the ISO Test PCD assembly and is extensively explained in [28]

5.4 Evaluation Software

The purpose of the evaluation software and component of the test-bench is to determine a phase φ as well as an amplitude deviation of the PICC with the DUT in reference to the PCD emitted signal over an arbitrary time frame.
The following section focuses on the recovery and calculation, mainly of a phase deviation φ of such an ISO/IEC 10373-6 Test PCD assembly. It shows the implementation, proposed alterations and modifications as well as possible alternatives and future prospects.

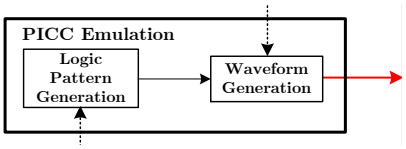


Figure 5.31: PICC Emulation

The evaluation of the magnitude and phase of a load modulated signal can be achieved in several ways: depending on the test setup which is described in the according standard (section 4.3) appropriate methods can be developed. One method for the use of an EMVCo Setup was introduced by *Christoph Egger* in [27].

5.4.1 Hilbert Transform - Hilbert Transformer

Starting with the real signal from equation 3.11

$$s(t) = A(t) \cdot \cos\left(\omega t + \varphi\left(t\right)\right) \tag{5.4}$$

and its analytic pendant, the conjugated complex expression $\underline{s}_a(t)$, equation 3.12 can be obtained. However, at first and foremost the transfer of the real signal $s(t)$ into its complex form $\underline{s}_a(t)$ needs to be sought out.

$$s_a(t) = \Re\left\{A\left(t\right) \cdot e^{j(\omega_0 t + \varphi(t))}\right\} \tag{5.5}$$

Characterizing the phase $\varphi(t)$ at any given time would then be possible by observing the instantaneous angle between the real and imaginary part of the complex expression.

The aim of Hilbert transform demodulation in the frequency domain therefore is to express a real signal in its complex form, whereas the original signal $s(t)$ remains as the real part of the complex form. This complex expression is also commonly referred to as *analytic signal* $s_a(t)$.

Utilizing *Euler's Formula* and the analytic signal $s_a(t)$ leads to the following conclusion

$$s_a(t) = [\underbrace{A(t) \cdot \cos(\varphi(t))}_{\Re\{s_a(t)\}=s(t)} + j \cdot \underbrace{A(t) \cdot \sin(\varphi(t))}_{\Im\{s(t)\}}] \cdot e^{j\omega_0 t}$$

The signal $s(t)$ can be represented in its analytic form $s_a(t)$ by summation of the original real signal $s(t)$ and an imaginary sine of the instant phase $\varphi(t)$ of the original signal.

In order to allow such a representation, there needs to be a mathematical operator which allows transforming a cosine into a sine[16]: the Hilbert transform.

Signal $u(t)$	Hilbert transform $\mathcal{H}\{u\}(t)$
$\sin(t)$	$-\cos(t)$
$\cos(t)$	$\sin(t)$

Table 5.4: Table of selected Hilbert transforms

The equations above show the relevant correspondence, with $\mathcal{H}\{\cdot\}$ as the Hilbert transform operator.

The following step shows the construction of the analytic signal for the example 3.9 by using one of the most common mathematical functions in the frequency domain: the *Fourier transform.*

$$S(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} s(t) e^{-j\omega t} dt. \tag{5.6}$$

By representing a cosine in its complex form using Euler's Identity

$$s(t) = \cos(\Omega t) = \frac{e^{j\Omega t} + e^{-j\Omega t}}{2} \tag{5.7}$$

and using equation 5.6 to express the time function $s(t)$ as a function of frequency $S(\omega)$ the following equation

[16] Requirement is a valid range of values in the domain of definition

$$S(\omega) = \frac{\delta(\omega - \Omega) + \delta(\omega + \Omega)}{2} \tag{5.8}$$

is obtained, with δ as the Dirac delta function.

If we multiply equation 5.8 by 2 and zero all negative frequencies

$$S_a(\omega) = \delta(\omega - \Omega) \tag{5.9}$$

the obtained result denotes a simple *Dirac delta function* with a shift of Ω in its frequency domain (equation 5.9).

$$e^{j\Omega t}x(t) = \mathcal{F}\{X(\omega - \Omega)\} \tag{5.10}$$

The inverse Fourier transform of equation 5.9 along with the transform pair in table 5.10 leads to the following new function

$$s_a(t) = e^{j\Omega t}, \tag{5.11}$$

the analytical signal of prior defined $s(t)$. As already pointed out in section 3.5, an analytic signal is defined as being complex in the time domain and therefore not having negative-spectral components in its frequency domain. The summation of a real signal $s(t)$ as defined in equation 5.7 with its own complex multiplied Hilbert transform is thereby per definition an analytic signal.

Summarizing

Given a real function $s(t)$ with its Fourier transform $S(\omega)$, the analytic signal $s_a(t)$ is defined by

$$s_a(t) = 2\int_0^\infty S(\omega)e^{j\omega t}dt\omega \tag{5.12}$$

The Hilbert transform of a real signal $s(t)$ is defined as the imaginary part of the analytic signal $s_a(t)$, denoted as $\hat{s}(t)$

$$s_a(t) = s(t) + j\hat{s}(t) \tag{5.13}$$

Thus, the Hilbert transform utilized in the frequency domain represents a phase demodulation technique, expressing a real signal in its complex form, often referred to as an *analytic signal*. The special characteristics of the Hilbert transform can be utilized for signal processing purposes. A *Hilbert transformer* allows a phase shift of 90° to a sine signal leading to transformation of signals as shown in table 5.4 which will be also the case in the following sections of this chapter [22].

5.4.2 Implementation

1st iteration - proposal

This subsection is going to discuss an effective way to retrieve the phase drift Φ during PICC response with the use of the existing ISO/IEC 10373-3 Test PCD assembly.

The requirements for such a Phase Test are:

- Determination of the PICC current's phase in relation to the PCD over a response frame.
- Determination of the phase drift, $\Delta\varphi$ in relation to the response's start phase.
- The tool shall provide at least one value of the phase information per subcarrier period to guarantee interoperability over various PCDs.

As determined by the group WG8/TF2 during the whole PICC response the PICC's current shall fulfill the following requirements:

1. The phase of the PICC current needs to stay within $-175°$ and $-5°$ relative to the phase of the PCD operating field.

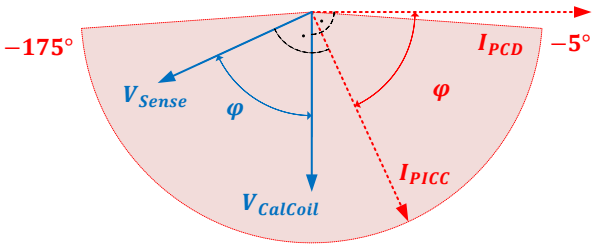


Figure 5.32: Requirement #1: current phase between PICC andPCD

2. The PICC current shall also lie within a range of $-30°$ and $+30°$ relative to the phase of the PICC field at start of its response RX.

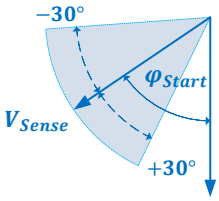


Figure 5.33: Requirement #2: limits for relative phase drift

These restrictions are necessary, in order to maintain an actively modulating PICC behavior similar to PICCs which are passively modulating. These stem from physical limitations of passive PICCs but may be removed in future revisions of the standard. [3].

Figure 5.34 shows the basic principle to retrieve a possible phase deviation by using the Hilbert transform.([18])

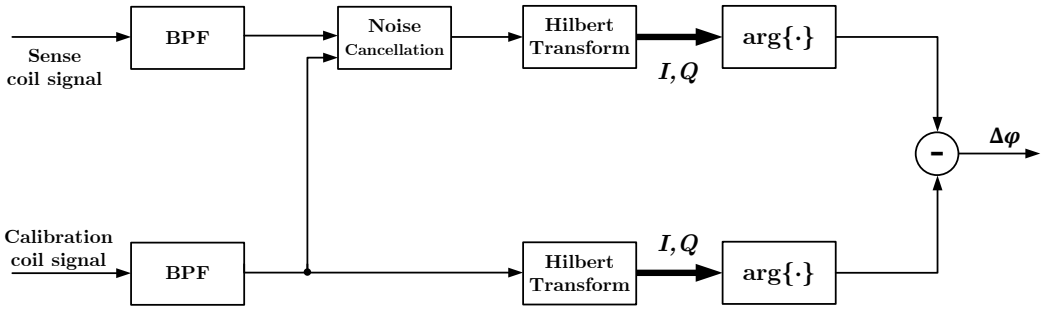


Figure 5.34: Hilbert Transform demodulation principle

To obtain phase drift between the current of the PICC i_{PICC} and the PCD i_{PCD} the corresponding voltages are captured and bandpass filtered. Their output is split into to sub-paths - I and Q - by using the Hilbert transform. The quadrature representation allows an assessment of instant phase and amplitude of the bandpass filtered I/Q - data pairs.
A final subtraction of the gathered phase φ_{PCD} from φ_{PICC} leads to the phase deviation value $\Delta\varphi$.

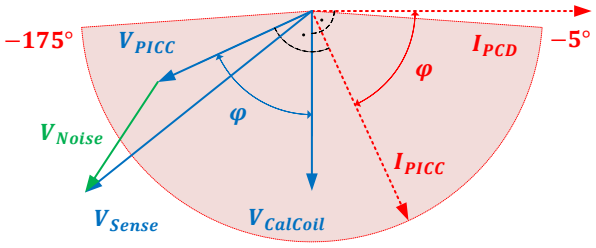


Figure 5.35: Vector representation of the PICC loading a PCD

As mentioned earlier this approach allows the unrestrained use of the the existing ISO/IEC 10373-6 Test PCD assembly. This means both i_{PICC} as well as i_{PCD} are represented as a voltage v_{Sense} measurable at *Helmholtz Bridge* (Sense coil) and the *Calibration coil*, $v_{CalCoil}$, respectively. Figure 5.35 depicts the vector signals of the relevant measurands as well as a *noise* vector.

The following Bandpass (BP) in both paths matches a Butterworth filter of 2$^{\text{nd}}$ order with a center frequency of $\omega_C = 13.56\,\text{MHz}$ and a bandwidth of 10 MHz in order to remove DC components and higher harmonics.

The next important step happens in the PICC path. As outlined in chapter 4.3.4, the signal measured at the Helmholtz Bridge is actually heavily influenced by the actual PCD incorporated magnetic H-field, the remaining carrier as well as the continuous loading of the PCD caused by PICC. This premise leads to a necessary removal of these *noise signals* to gain a signal which represents the PICC. This effect can be considered in form of an additional noise value or *noise vector* regarding a vector representation of the PICC loading the PCD (c.f. section 5.4.2).

The procedure to cancel the noise is to cross-correlate a part of the unmodulated Sense Coil signal with the Calibration Coil signal. To maximize the correlation the Calibration Coil signal is shifted and normalized to find an optimum. The manipulated signal is geometrically subtracted from the Sense Coil signal resulting in a quantity representing i_{PICC}.

After the cancellation procedure, signal periods with an inverted phase (180° phase shift) regarding the PCD and periods in which there is no signal driven to the PICC are extracted, leaving only exploitable parts of the sampled signal to be processed. The parts of the signal without measurable amplitude are removed during the cancellation procedure because applying the Hilbert operator on such sections of the signal would

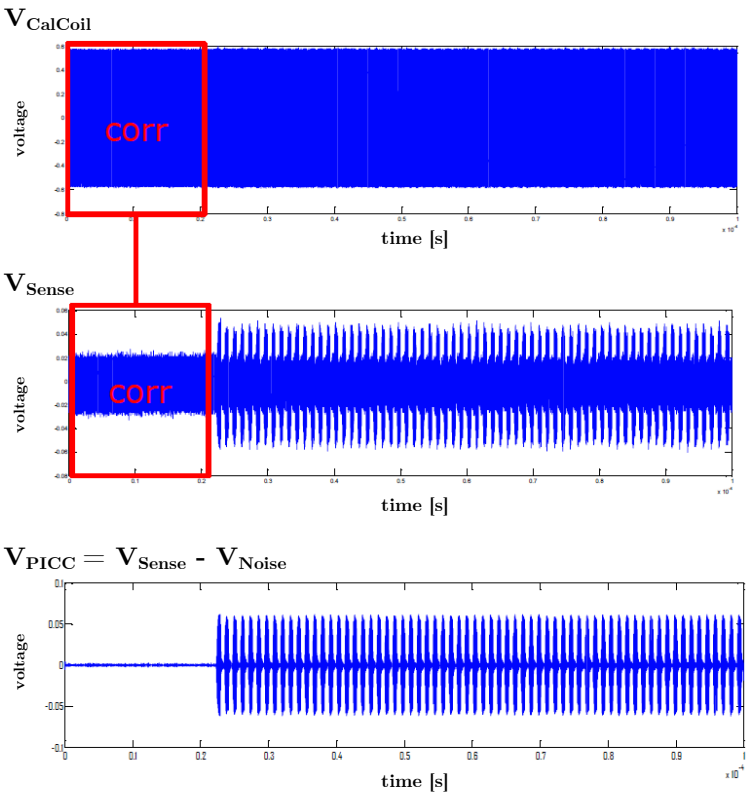


Figure 5.36: Noise Cancellation Procedure adapted from [18]

lead to a huge, monotonically rising phase drift between both data signals created in the IQ paths. The cancellation needs to take place in both signal paths simultaneously to maintain a correct phase relation. The decision making to where and when to cut and retrieve the relevant parts of the data sequence is implemented using the demodulated Sense coil signal (Figure 5.37).

At last Hilbert transform of both signals can be calculated, the result's argument yields phase values for both. The difference is the equivalent instantaneous phase difference, a phase-drift $\Delta\varphi$.

The resulting phase is displayed by averaging the phase drift over one subcarrier period leading to only one data point per subcarrier.

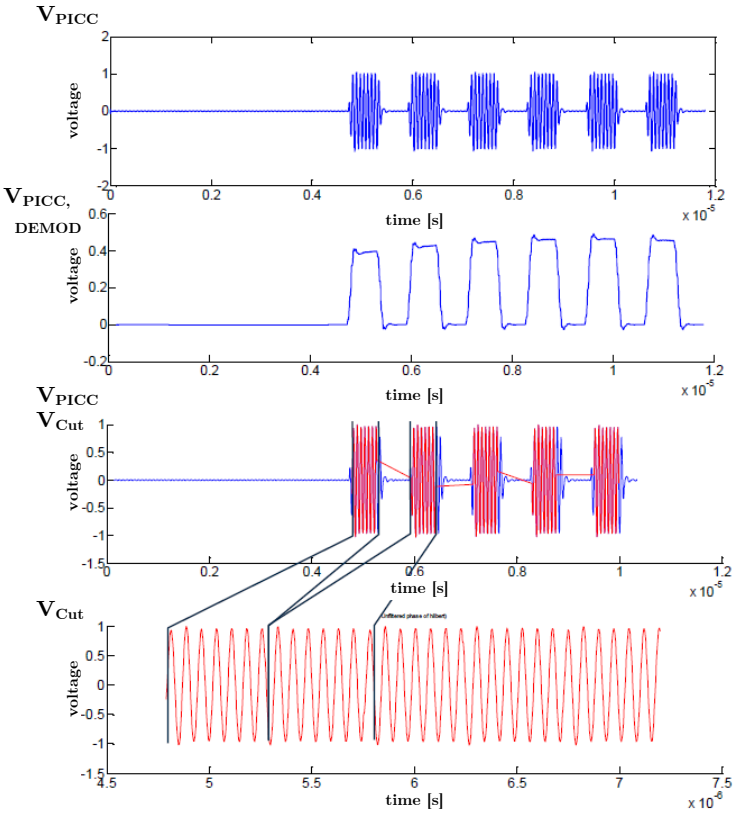


Figure 5.37: Cutting Procedure for V_{Sense}, analogous to $V_{CalCoil}$ adapted from [18]

2nd iteration - adaptation

In terms of communication signal quality, the relevant PICC parameter is the modulation seen by the PCD, which is the vectorial difference between the two PICC modulation states (c.f. amendment [3] of ISO/IEC 14443-2). As the amplitude and phase continuously change during PICC modulation, it might seem only reasonable to calculate the vectorial difference between each PICC signal vectorial value and the vectorial value located exactly $^1/_2 f_{sub}$ later, in other words: building the difference between the complex PICC signal and the same signal shifted by $^1/_2 f_{sub}$. All complex values of any series made by sampling this complex difference at a sample rate of $^1/_{f_{sub}}$ shall be processed to show a PICC phase drift.

The following segments show adaptations made to the prior introduced phase evaluation method.

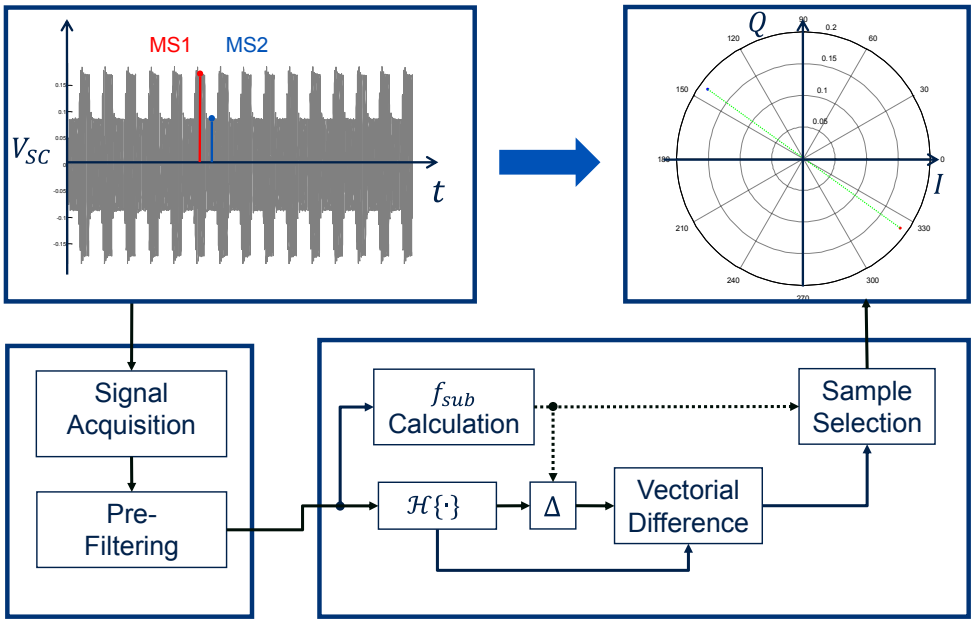


Figure 5.38: New adapted phase evaluation method developed in order to depict the vectorial difference between each PICC signal value

The amendment [3] made to ISO/IEC 14443-2 describes *Modulation States* as follows:

The PICC transmits data by using at least one modulated state. The first modulation state is called MS1. The second modulation state is called MS2 and may be the same state as before PICC transmission. Amplitude and phase of these modulation states are measured by specific test methods described in ISO/IEC10373-6.

The evaluation method has been adapted to additionally depict these modulation states in constellation diagrams.

The enhanced concept can be split into several parts:

- **Signal Acquisition**: The Sense Coil signal $V_{Sense}(t)$ representing the PICC current is acquired by a scope with a sampling frequency $f_s \geq 1GS/s$ as described in chapter 5.4.2.
- **Pre-Filtering**: A bandpass filter ($13.56MHz \pm 5MHz$) filters the signal $V_{Sense}[n]$ with a bandwidth of $10MHz$ in order to cancel DC as well as higher harmonic frequency components out.

- **Hilbert Transform**: The Hilbert Transform is used to transfer the filtered signal $v_{SC,filt}[n]$ into the complex domain.

$$\boldsymbol{H_{SC}[n]} = \mathcal{H}\{v_{SC,filt}[n]\} \tag{5.14}$$

$$\boldsymbol{H_{SC}[n]} = \Re\{\boldsymbol{H_{SC}[n]}\} + j \cdot \Im\{\boldsymbol{H_{SC}[n]}\} \tag{5.15}$$

Equation 5.15 shows a real and an imaginary part, the *(*In-phase) and the *Quadrature phase* part (see section 3.5.2). The In-phase and Quadrature part define the Modulation State (MS) vectors', MS1 and MS2, current location over time in the constellation diagram

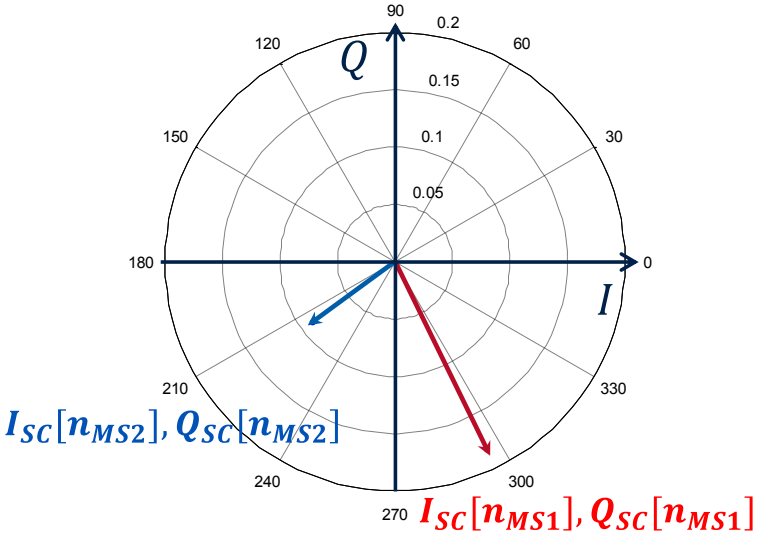


Figure 5.39: The phasor of both, MS1 and MS2

- **Computation and Shifting of f_{sub}**: The subcarrier frequency, f_{sub}, is directly derived from the nominal carrier frequency, $f_{carrier}$ of 13.56 MHz. However the heedful reader will learn, that this will lead to problems explained in an example on the following subsection.
  Mathematically, the shifted signal can be expressed as

$$\boldsymbol{H_{SC,sh}[n]} = \Re\{\boldsymbol{H_{SC,sh}[n]}\} + j \cdot \Im\{\boldsymbol{H_{SC,sh}[n]}\} \tag{5.16}$$

- **Calculation of the Vectorial difference**: $\boldsymbol{H_{diff}[n]}$ is the difference of shifted

and unshifted signal.

$$\boldsymbol{H_{diff}[n]} = \Re\{\boldsymbol{H_{SC}[n]}\} - \Im\{\boldsymbol{H_{SC,sh}[n]}\} \tag{5.17}$$

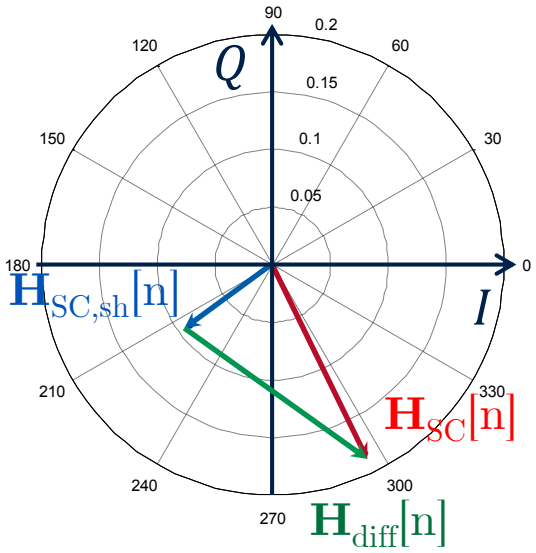


Figure 5.40: Vectorial difference of two $\frac{1}{2f_{sub}}$ shifted Hilbert transformed data sequences

- **Sample Selection**: For a correct evaluation, the selection process of samples is quite important. It is possible to evaluate both, transients as well as longterm drifts. Since there has been no decision if and how important transients are in the modulation process the focus is set on longterm drift evaluation[17].
  To gain a better resolution in the evaluation results one sample is selected each $^1/_2 N_{sub}$ which leads to two series of data, in other words one sample per modulation state.

[17] This subject has been up to discussion during creation of this thesis.

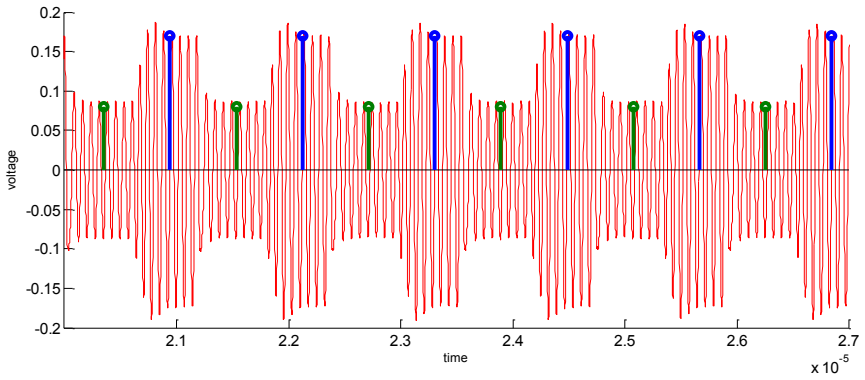


Figure 5.41: 1 sample each $^1/_2 N_{sub}$ obtained from the sample data

Method illustrated by an example

For further considerations an example is used: a typical PLM signal, Type B ATQB with a bit rate of 106 kB RX/Transmit (TX) operated at a PCD magnetic field strength of 1.3 A/m with a Class 1 antenna and f_{res} tuned to 16.1 MHz. In a traditional PLM the Device Under Test (DUT) clock is synchronized with the PCD field, thus a phase drift is not expected.

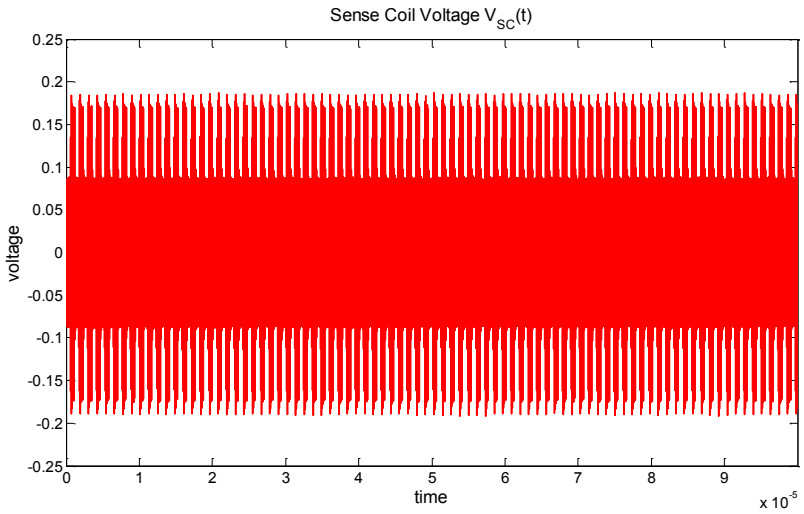


Figure 5.42: Sense Coil Voltage, Type B, 106 kbit/s

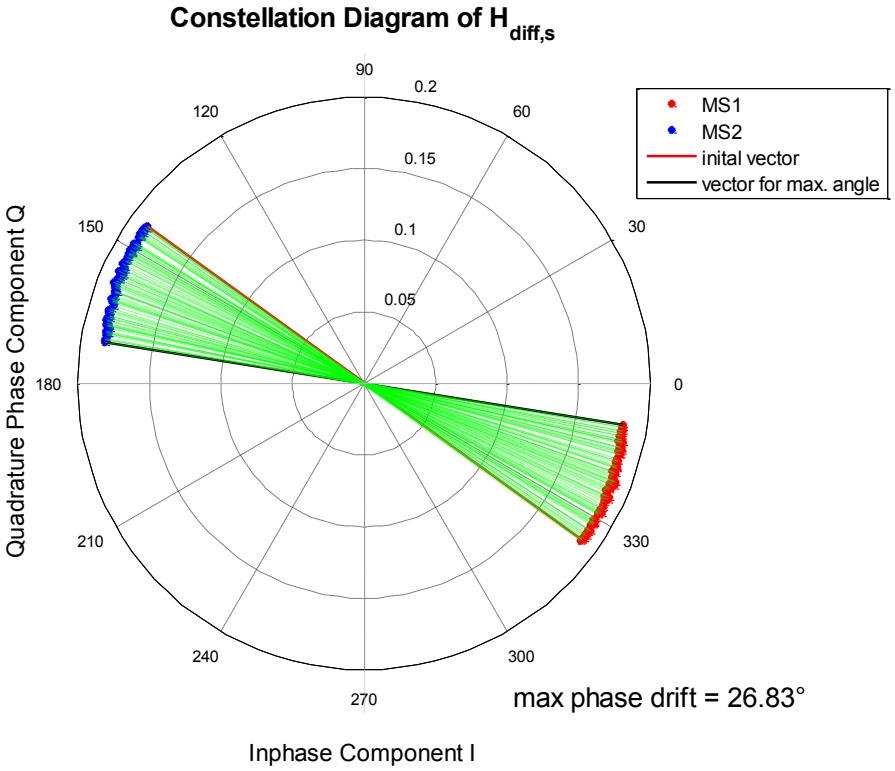


Figure 5.43: Constellation Diagram of $H_{diff,S}$

Common PCDs do not show any significant phase drift with less than $\pm 1°$ measured in most cases, attributed merely to noise than real phasor variations. [19]

However the constellation overview in figure 5.43 depicts a real phase drift of 27° within 0.1 ms. This has very obvious reasons. The internal oscillator of the acquisition instrument (oscilloscope) is not synchronized with PCD field, thus when comparing the PICC signal value and the value almost exactly $^1/_2 f_{sub}$ later, mainly jitter errors occur, but unlikely continuous phase drift.

In addition, a typical 50 ppm difference between the carrier frequency of the PCD and the nominal 13.56 MHz will give a difference of 678 Hz, i.e. a 360° phase shift every $^1/_{678}$ seconds, meaning a 24° shift every 0.1 ms. (cf. figure 5.43).

To overcome this problem, there are several solutions:

Firstly, the determination of the actual subcarrier frequency, f_{sub}, by computing the Discrete Fourier Transform (DFT) of $v_{SC,filt}$ and extraction of the actual $f_{carrier}$. This

also allows the computation of the actual f_{sub} and N_{sub}, respectively. Therefore N_{sub} is the amount of samples per subcarrier, re-sampled to ensure a constant (even) amount of samples per subcarrier period $^1/_{f_{sub}}$.

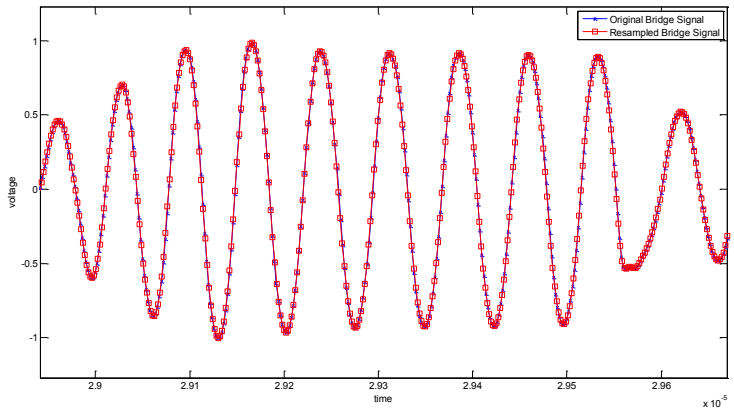


Figure 5.44: Evenly sampled carrier signal over one subcarrier period, $^1/_{f_{sub}}$.

The DFT is actually a periodogram function, an estimate of the spectral density of a signal. [22]

This is implemented as an iterative process in which the size of the DFT window with every step increasingly is narrowed towards the frequency of the highest Power Spectral Density (PSD). The decision to use an iterative approach was owed to otherwise relatively long calculation times and therefore a non-existent real-time capability. I.e. the first step in determining the exact $f_{carrier}$ is computing the PSD over a span of frequencies leading to a coarse first estimation of $f_{carrier}$. The next step centers around the first estimation but with a significantly narrower window. This loop proceeds until there is a $f_{carrier}$ with reasonable accuracy of $\pm 100\,\text{ppm}$ given.

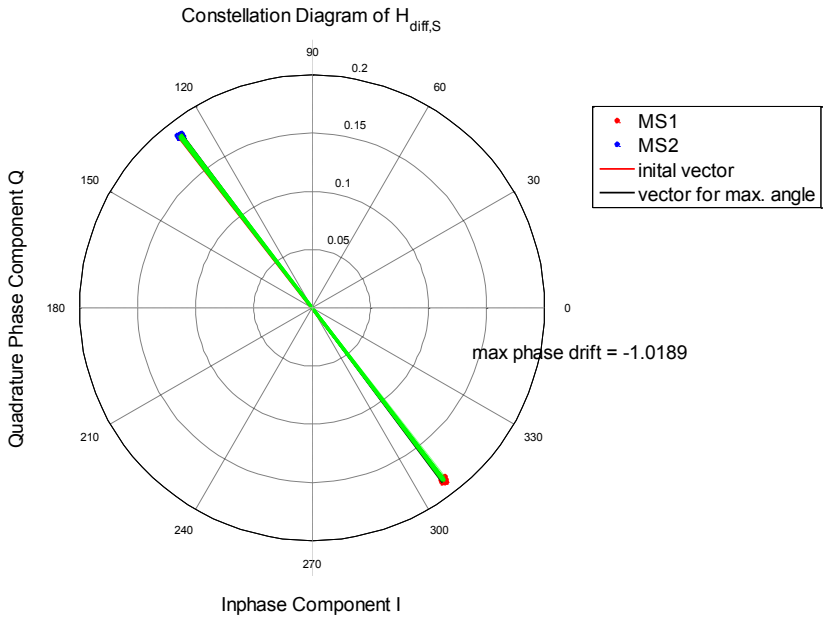


Figure 5.45: Constellation Diagram of $H_{diff,S}$ without significant phase drift

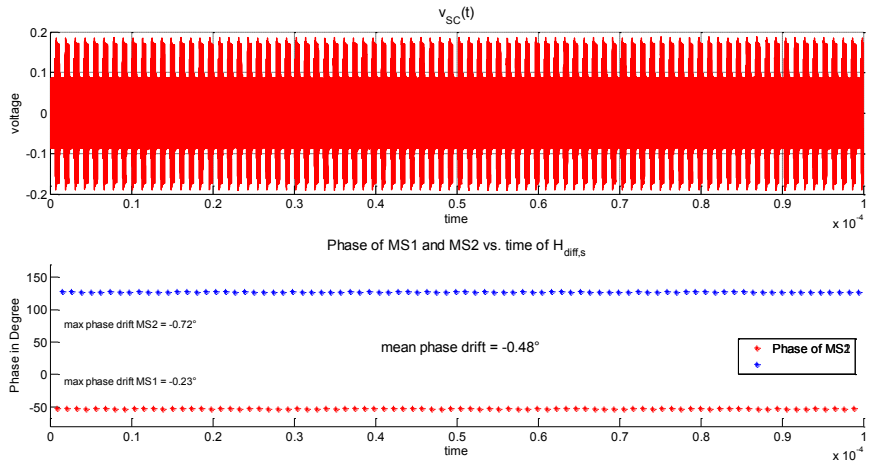


Figure 5.46: $H_{diff,S}$ in time domain without significant phase drift

If eliminating the error caused by choosing a wrong carrier frequency for the computation of the phase drift, the mean phase drift (mean of maximum phase drift of MS1 and MS2)

equals $-0.48°$, mostly to be contributed to noise. This result is depicted in figures 5.45 and 5.46.

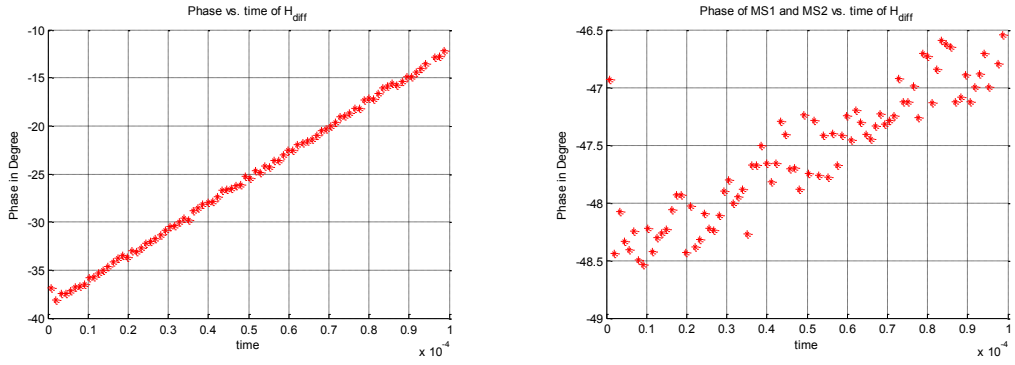


Figure 5.47: $H_{diff,S}$ in time domain with $f_{carrier}$ recovery but without re-sampling (left) and without $f_{carrier}$ recovery but with additional re-sampling (right). Note the narrow phase scaling on the right graph.

To get a better understanding of the proposed steps a comparison between the impact of either to re-sampling the acquired signal and the impact of recovering the carrier frequency, $f_{carrier}$, from the actual PCD magnetic field is depicted in figure 5.47.

Again, the signal example is generated having zero phase drift. As one can see, evenly re-sampling the acquired data has a huge impact on the result. The figure on the right shows only a fraction of the initial erroneous phase drift. The remaining error is explained with the lack of an actual carrier frequency recovery.

Figure 5.48 shows the impact of a slightly altered $f_{carrier}$ in comparison to the reference frequency used for the calculation. A deviation of only 50 ppm causes an already remarkably erroneous calculation of the phase drift.

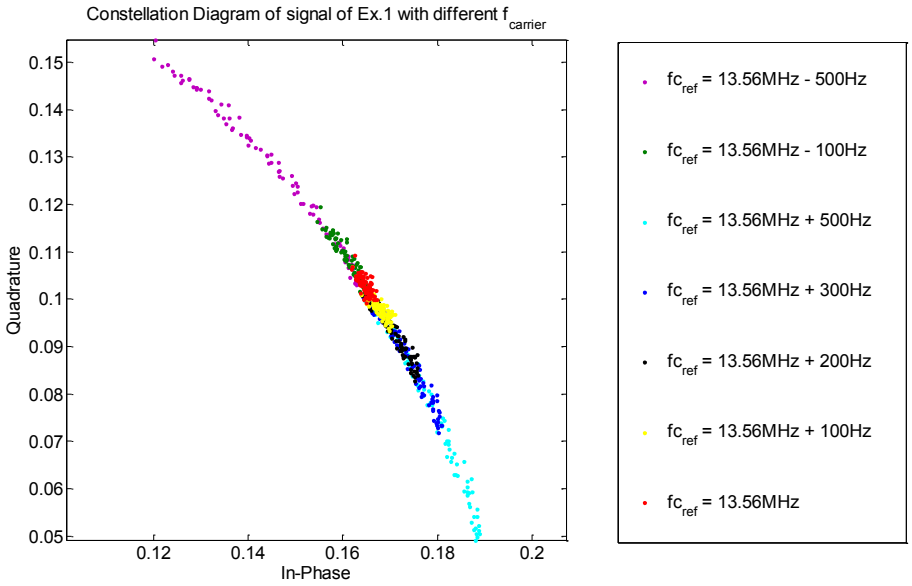


Figure 5.48: Sensitivity of results due to erroneous (max. 50 ppm) $f_{carrier}$

Test Signals

The following section shows several test signals and their efficient evaluation according to the method described above.

A) Ideal XOR[18] test signal with a subcarrier drift of 1.7° at a field strength equal to 3.5 A/m:

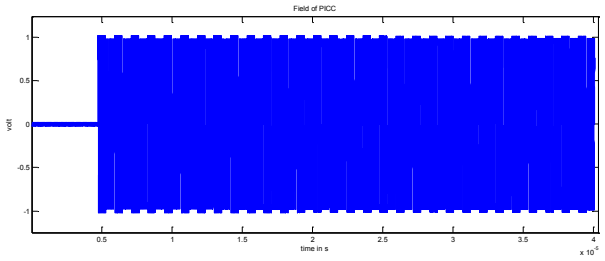


Figure 5.49: Ideal XOR - test signal with a subcarrier drift of 1.7° over its frame

[18]XOR means two modulated states with reciprocal phases

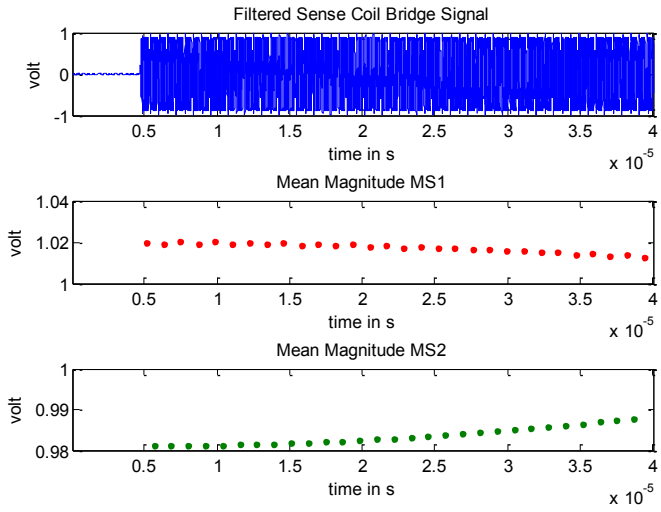


Figure 5.50: Ideal XOR - test signal: magnitude of both MS

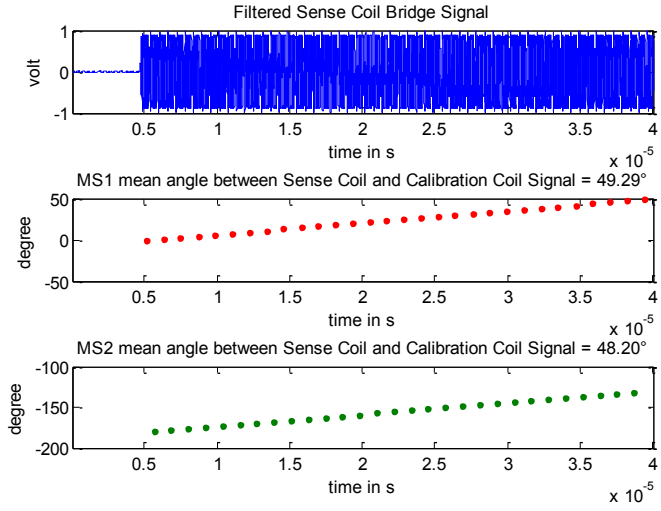


Figure 5.51: Ideal XOR - test signal: phase of both MS

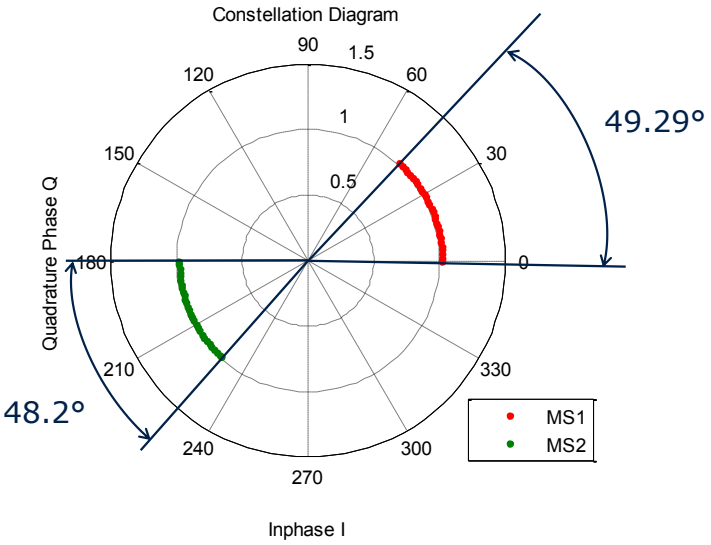


Figure 5.52: Ideal XOR - test-signal: constellation diagram

B) Ideal Type A test signal at a field strength equal to 3.5 A/m:

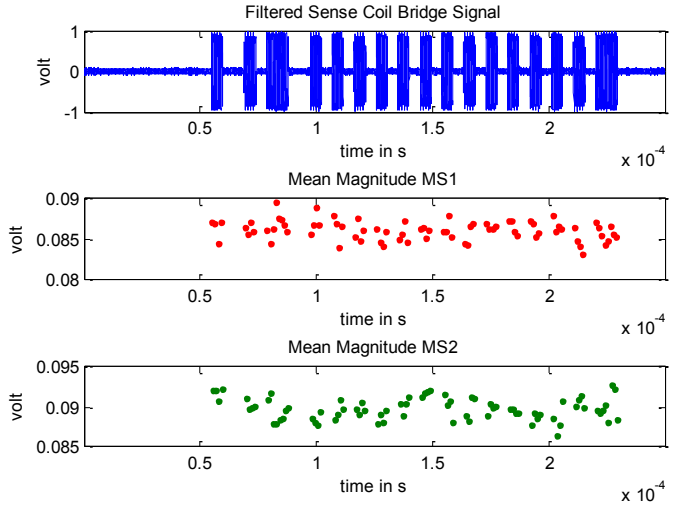


Figure 5.53: Ideal Type A - test-signal: magnitude of both MS

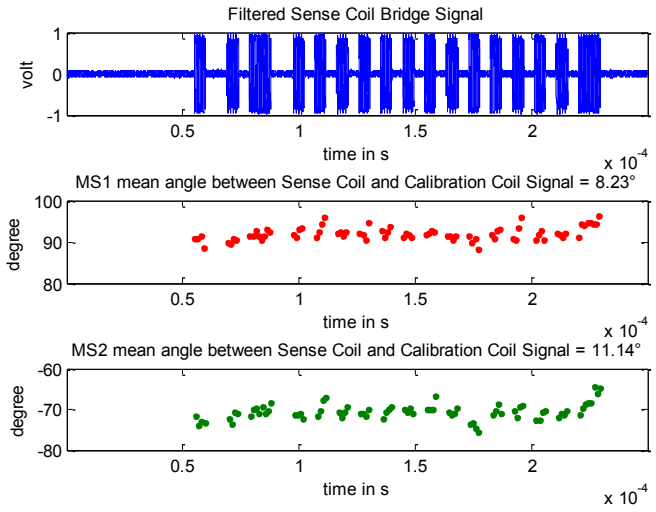


Figure 5.54: Ideal Type A - test-signal: phase of both MS

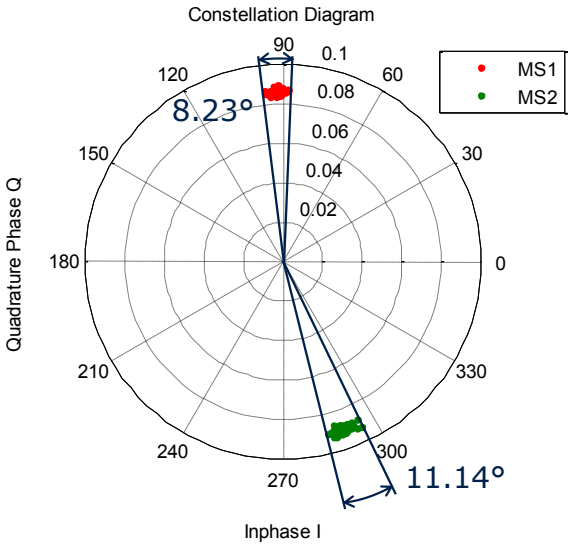


Figure 5.55: Ideal Type A - test-signal: constellation diagram

C) Ideal Type B test signal at a field strength equal to 3.5 A/m:

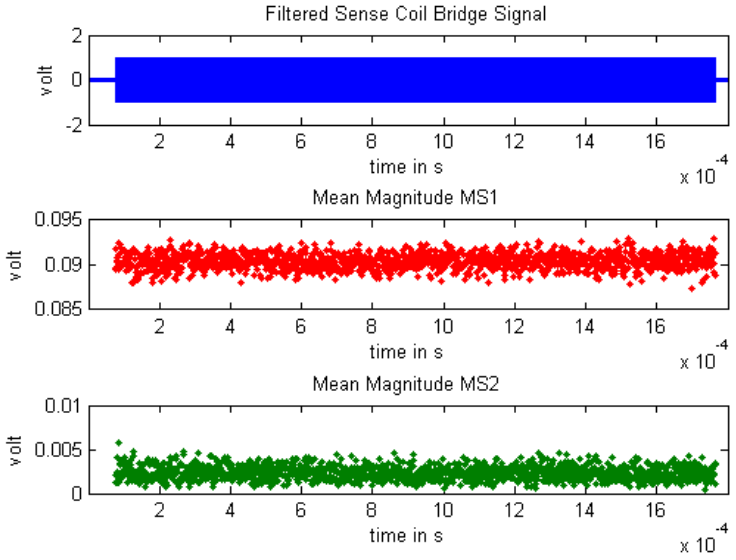


Figure 5.56: Ideal Type B - test signal: magnitude of both MS

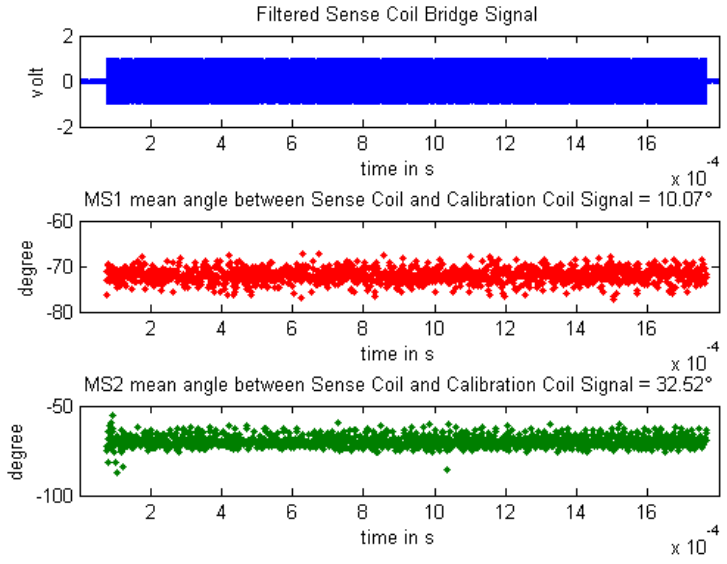


Figure 5.57: Ideal Type B - test signal: phase of both MS

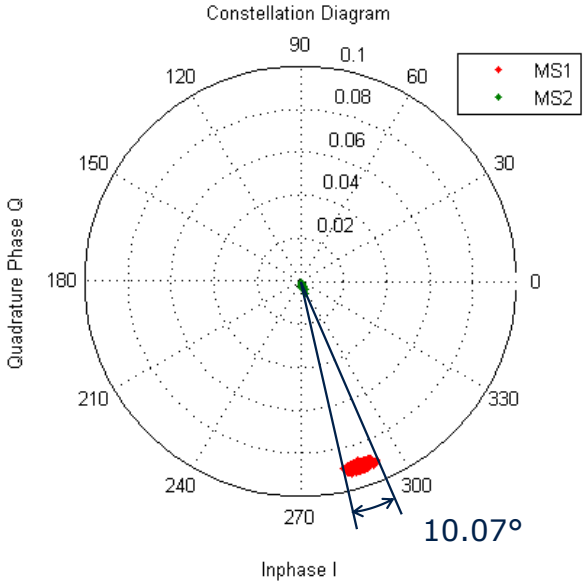


Figure 5.58: Ideal Type B - test signal: constellation diagram

5.4.3 Discussion of Proposed Methods

Conclusions

- Issues concerning inaccuracies of the carrier frequency, $f_{carrier}$, and its value used for calculations: an inaccurate carrier reference has profound effects on the evaluation. Differences of a few ppm can lead to an outcome showing distinctive phase drift. An artificial carrier reference $f_{carrier}$ is necessary. The adaptation proposed an accurate estimation of the carrier frequency. The approach of a consecutive determination of $f_{carrier}$ might be considered to calculate the instant carrier frequency on-the-fly using Short-Time Fourier Transformation (STFT). Additionally, jitter of $f_{carrier}$ over an observed frame is taken into consideration.
- Finite sampling precision of the acquisition device needs to be considered: When sampling the PCD magnetic field the sampling device's sampling rate usually will not be synchronized with the carrier. Data signals need to be re- and up-sampled to result in an evenly distributed amount of samples.
- The associated voltage $V_{CalCoil}$ representing the PCD current can be fairly easily acquired to create reference $f_{carrier}$. This also provides accurate information about the initial phase.
- The method needs an algorithm to differ between modulated and unmodulated states and to find a steady state for being able to choose samples properly. However, the procedure in general needs still optimization.
- The evaluation software is applicable on both PLM and ALM signals. Nevertheless, especially pauses within Type-A PCD commands tend to be a problem. The loss of the clock signal leads to a loss of the phase coherence between the PCD and the PICC.
- As the phase measurement is continuous and the transitions between states are not controlled and create phase variations, it must be decided:
  - how much of the transitions between modulation states are ignored, knowing that transition speed depends on the PICC quality factor, and
  - if averaging is done on the remaining, steady part of each modulation state.

Homodyne Demodulation Method

There are also alternatives to be considered, such as the *homodyne* principle:

The *Helmholtz Bridge* (Sense Coil) signal $V_{Sense}(t)$ can be demodulated by use of the homodyne demodulator as depicted in figure 5.59. The in-phase path is demodulated by the *Calibration Coil* signal V_{CC} whereas the quadrature-phase path is demodulated by a 90° shifted *Calibration Coil* signal. Low pass filter in both paths suppress 2nd harmonics

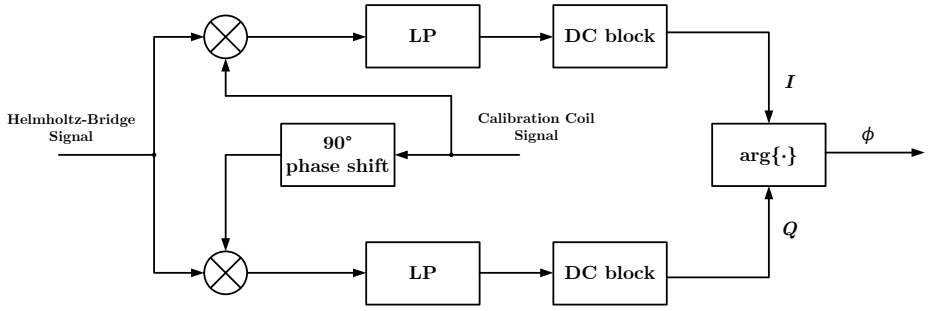


Figure 5.59: Homodyne demodulation principle

of the carrier signal. DC blocking filters are provided to remove the DC component of the signal.The argument between inline-phase and quadrature-phase signals result in a phase signal $\varphi(t)$

Following aspects have to be taken into account if implementing the homodyne demodulation principle:

- To accurately measure the phase deviation of a signal in the presence of a strong signal at the same frequency is tricky.
- A Homodyne demodulation algorithm and removal of DC component can solve this problem in the Baseband.
- Homodyne demodulation of the continuous wave carrier component in HHB with the calibration coil continuous wave carrier produces DC voltage which can be removed.
- It is possible to use the existing ISO/IEC 10373-6 [2] test bench and to define an additional RF compliance test in order to guarantee interoperability of ALM devices with existing infrastructure.

Evaluation Software - Control

The *controlling aspect*, the interaction in both directions between evaluating system and PICC emulation, RefPICC and Test PCD assembly has not been part of this master thesis due to lack of time. The main idea behind an automation aspect would be to simply specify a desired AM and PM target values within a software interface such as Matlab^{TM}used for implementing the control program. The measured signal would be evaluated and analyzed, while adjusting parameters in the PICC emulation block as long as the target values would be reached eventually.

Chapter 6

Verification regarding ISO/IEC 14443

The EMV requirements of both, the signal interface and the RF power interface of the PCD and PICC are specified in the document *EMVCo Level 1 Test Equipment* [9].

The most glaring difference between both standards: Tests according to ISO/IEC 10373-6 [2] are defined in order to evaluate only the DUT, whereas the EMV procedure takes into account the overall contactless system in which a DUT interacts with the EMVCO Level 1... in order to be evaluated.

Although the limits in the standard are defined in a way that compatibility with the limits defined in ISO/IEC 14443-2 should follow, a direct conversion of measured values is hardly possible and is currently investigated by *Infineon Technologies AG*.

6.1 Test Setup

Earlier in chapter 5, a rough concept for a possible test bench has been introduced, as depicted in figure 5.1. Due to limitations and restrictions in both, time and range of functions available, the original concept mentioned in this chapter had to be adapted and changed leading to the final test-bench setup shown:

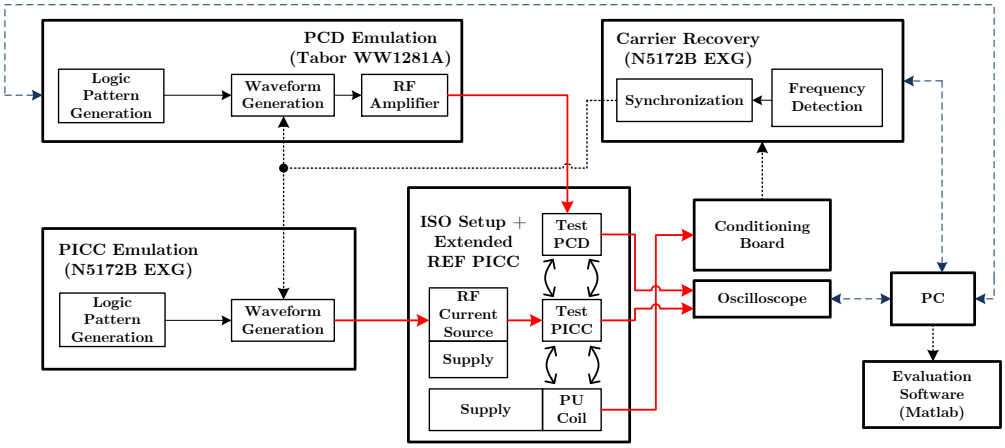


Figure 6.1: Block diagram of the final test bench setup

The most noteworthy differences between the initially envisioned test setup and the final setup can be briefly explained as follows:

The EXG vector signal generator is responsible for both, the entire PICC emulation and to a large extent for the carrier recovery. The signal to be locked on the carrier frequency is provided by the *Pick-Up Coil*, introduced in section 5.2 and depicted in figure 5.7. The auxiliary *Conditioning Board* (figure 5.10) is needed to provide a well defined interface between reference input of the vector signal generator and the the ISO test setup.

The automation aspect together with the AM/PM feedback to the PICC emulation unit was skipped entirely. What remains is an evaluation software able to process PLM as well as ALM signals.

The *ISO Setup* is represented by the *ISO Test PCD Assembly* and the *RefPICC*, as mentioned in chapter 5. Both are depicted in figure 4.3.2. The *RefPICC* utilizes an antenna coil, called *Pick-Up Coil*, comprising a main coil on its bottom layer and the pick-up coil on its top layer.

6.2 Calibration Steps

Chapter *5.4* of *ISO/IEC 10373-6* and its subsections describe the design and operating principles of the *RefPICC* in detail. It basically consists of a rectifier and an adjustable load as well as additional input and output connectors. The input connectors allow applying a load modulation signal, and a voltage to adjust the load. The output connectors allow measuring a DC voltage related to the load and a voltage signal used for

evaluating PCD waveform parameters. [2]

Section *5.4.3* furthermore describes the necessary steps to calibrate (resonance frequency tuning) the RefPICC. It is important to note, that with every deviation in the providing magnetic field strength, H, emitted by the PCD, re-calibration is required.

To calibrate the RefPICC's resonance frequency the following procedure is defined:

1. *Set jumper J1 to position 'a'.*
2. *Connect the calibration coil directly to a signal generator and the Reference PICC connector CON3 to a high impedance voltmeter. Connect all the other connectors to the same equipment as used for the tests.*
3. *Locate the Reference PICC at a distance d = 10 mm above the calibration coil with the axes of the two coils (calibration coil and Reference PICC main coil) being congruent.*
4. *Drive the calibration coil with a sine wave set to the desired resonance frequency.*
5. *Adjust the Reference PICC capacitors C1 and C2 to get maximum DC voltage at CON3.*
6. *Adjust the signal generator drive level to read a DC voltage of 6 V at CON3.*
7. *Repeat steps 5) and 6) until the maximum voltage after step 5) is 6 V.*
8. *Calibrate the Test PCD assembly to produce the Hmin operating condition on the calibration coil.*
9. *Place the Reference PICC into the DUT position on the Test PCD assembly. Switch the jumper J1 to position 'b' and adjust R2 to obtain a DC voltage of 6 V measured at connector CON3. The operating field condition shall be verified by monitoring the voltage on the calibration coil and adjusted if necessary.*
10. *Repeat steps 2) to 7) with the obtained value of R2.*

Previous investigations showed that there are just marginal differences between calibrating with and without the *RF Current Source* attached [27]. However the calibration procedure shall be executed with the device attached (and actively supplied) in all following considerations.

6.3 Measurement and Evaluation

As mentioned earlier, a field - reset or an ISO 14443 Type A communication gap for example would lead to an inevitable loss of the actual phase coherency between PCD and PICC field. Consequently, for the following measurements, a continuous PCD signal without pauses or gaps over the observed time frame is used.

6.3.1 PCD Reception Test Case 2: Type A, 106 kbit/s

The signal sent by the *PICC Emulation* is an XOR signal according to ISO 14443 Type A. It is also noteworthy that the commonly used phase deviation was altered from 35°[1] to 30° in the final measurements.

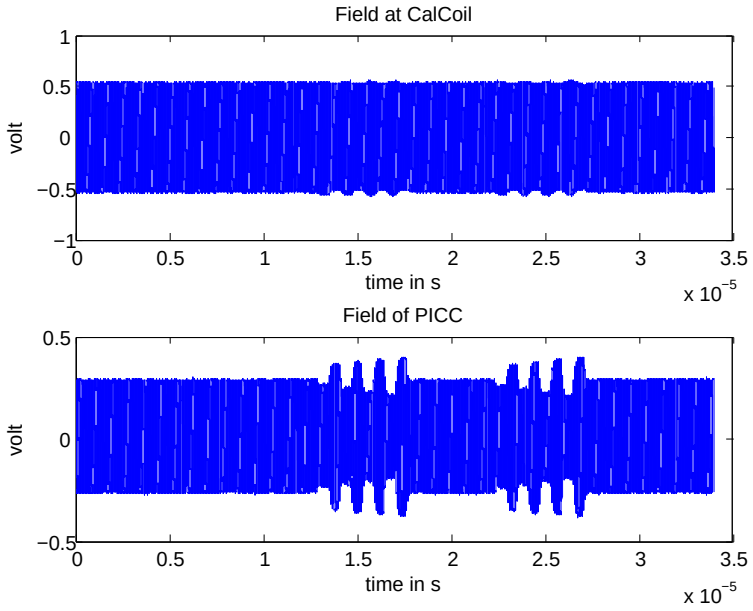


Figure 6.2: PCD reception test case 2: calibration coil signal and PICC signal at 1 A/m and a modulation voltage of 316 mV

As an example, figure 6.2 shows the system signals at a modulation power of 0 dBm. Figures 6.3 and 6.4 show distinctive differences upon varying the modulation input-signal of the *RF Current Source*. MS1 should reach 30° with every half etu while MS2 is ignored. While at lower modulation voltages this seems to correspond well with the theory, increasing the modulation voltages leads to a steady decline of the observable phase drift. The drift of MS2 comes from the relatively low gradient of the falling edges when the device switches from hi to low (0 mV).

[1]The phase deviation for the PCD reception test cases was defined in chapter 5.3.1

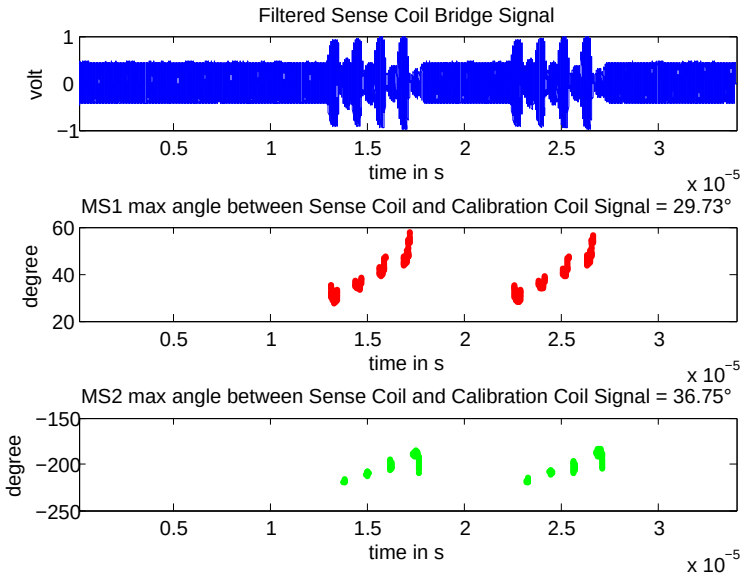


Figure 6.3: PCD reception test case 2: sampled phase of both MS at 1 A/m and a modulation voltage of 316 mV

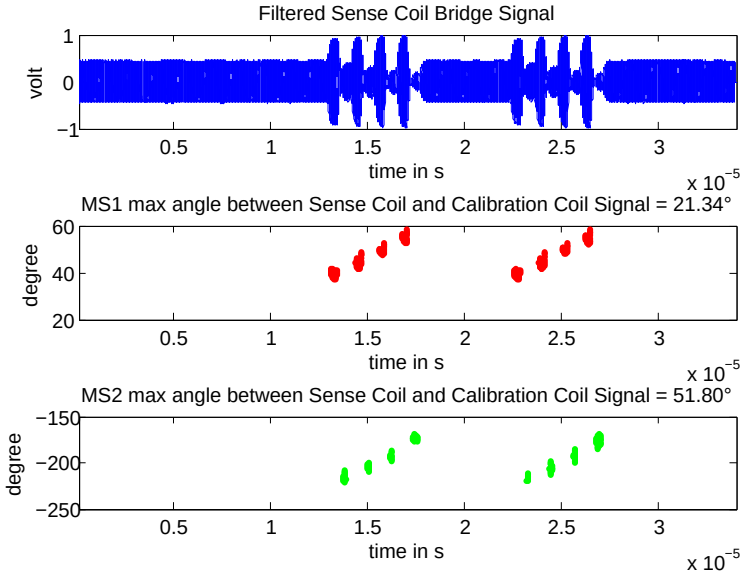


Figure 6.4: PCD reception test case 2: sampled phase of both MS at 1 A/m and a modulation voltage of 500 mV

6.3.2 PCD Reception Test Case 3: Type A, 106 kbit/s

The signal sent by the *PICC Emulation* is again an XOR signal according to ISO 14443 Type A. It is also noteworthy that the commonly used phase deviation was altered from 35°[2] to 30° in the final measurements.

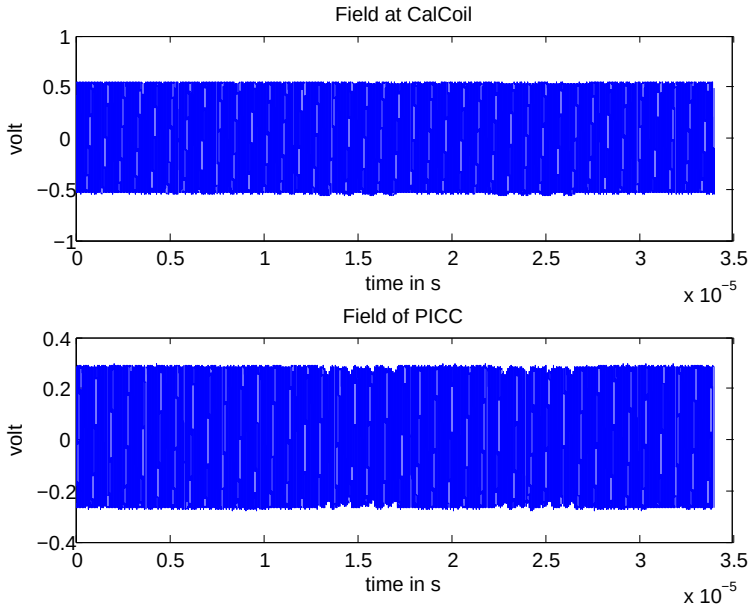


Figure 6.5: PCD reception test case 3: calibration coil signal and PICC signal at 1 A/m and a modulation voltage of 316 mV

As an example, figure 6.5 shows the system signals at a modulation power of 0 dBm. Figures 6.6 and 6.7 show basically the same signals, however, the signal-frame in figure 6.7 is slightly wider than 1 etu. The results show that the evaluation procedure is dependent on coherent frame-sizes, or even more generally treated, coherency between measured signals and parameters used within the evaluation procedures. While the results with correct etu show a good match, the results for the wider and incorrect etu regarding bit rate 106 kbit/s show far less conformity. Again MS1 should reach 30° with every half etu while MS2 is ignored.

[2]The phase deviation for the PCD reception test cases was defined in chapter 5.3.1

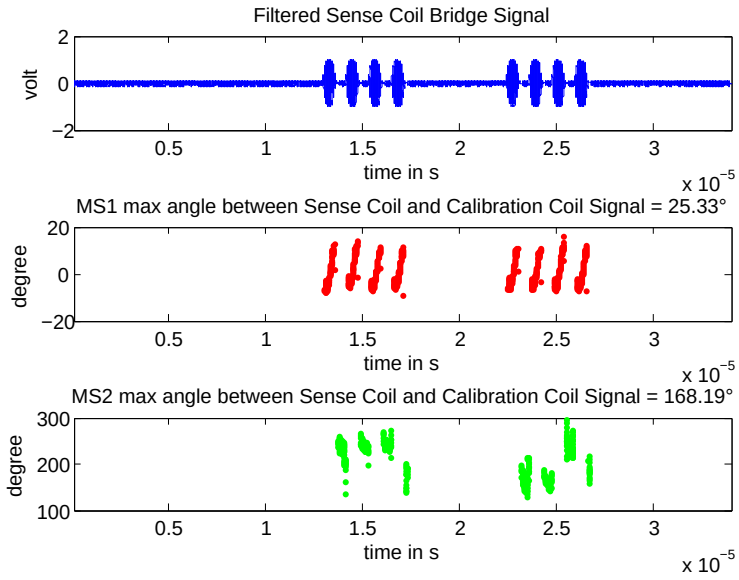


Figure 6.6: PCD reception test case 3: sampled phase of both MS at 1 A/m and a modulation voltage of 316 mV; correct $etu = 9.44\,\mu$s

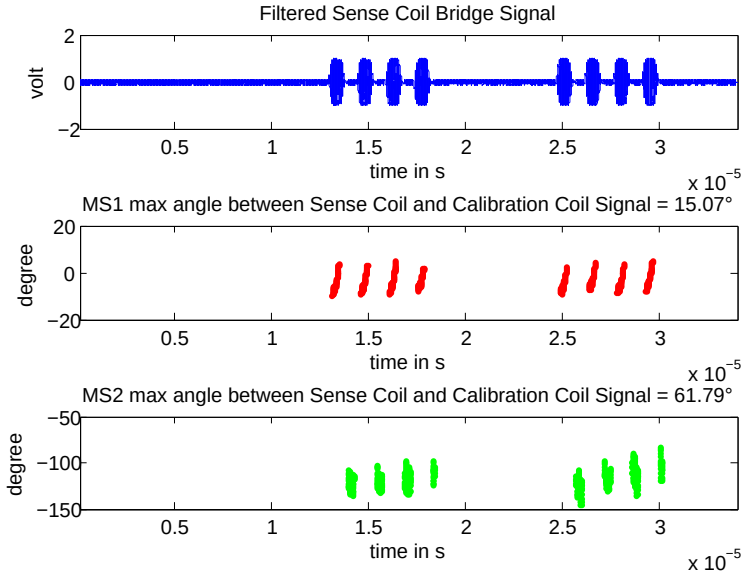


Figure 6.7: PCD reception test case 3: sampled phase of both MS at 1 A/m and a modulation voltage of 316 mV; incorrect $etu > 9.44\,\mu$s

6.3.3 Test Case 5° Sweep: Type A, 106 kbit/s

The final measurement is not part of the PCD reception test cases, however, was used to better show the general functionality of the test bench as a whole. The signal sent by the *PICC Emulation* is again an XOR signal according to ISO 14443 Type A and is increased in 5° steps to reach a phase drift of 360°.

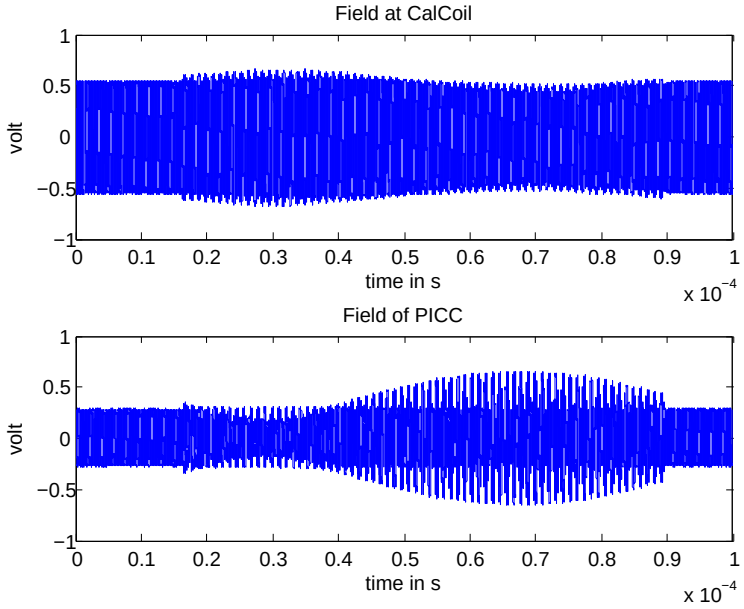


Figure 6.8: Test case 5° sweep: calibration coil signal and PICC signal at 1 A/m and a modulation voltage of 2000 mV

As an example, figure 6.8 shows the system signals at a modulation voltage of 2000 mV. Figures 6.9 to 6.12 show the test bench working with a PCD field of $H = 1\,\mathrm{A/m}$ and different modulation voltages. Figures 6.13 to 6.15 show the test bench working with a PCD field of $H = 1.5\,\mathrm{A/m}$ and different modulation voltages. The relaxed requirements with less phase drift per etu are also one of the reasons that all measurements show good, even very good results at times. The magnitude of the PCD field and the modulation voltage do not seem to have the same impact on the phase drift as seen in the test cases before.

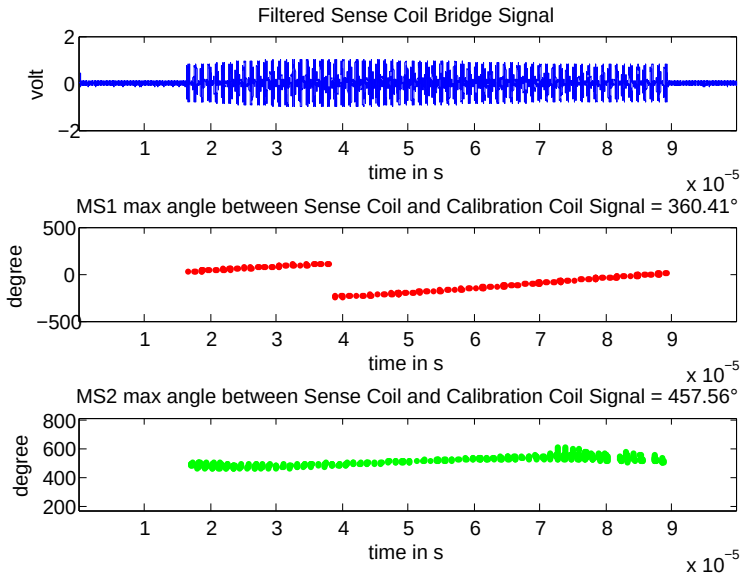


Figure 6.9: Test case 5° sweep: sampled phase of both MS at 1 A/m and a modulation voltage of 2000 mV

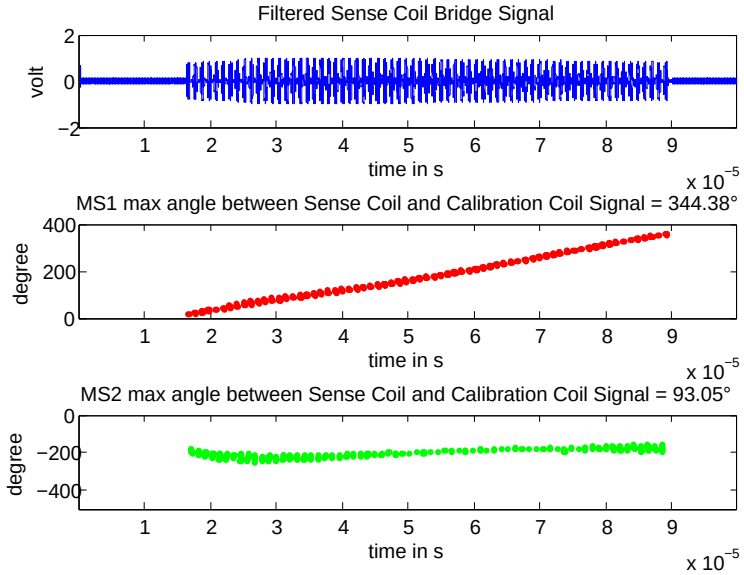


Figure 6.10: Test case 5° sweep: sampled phase of both MS at 1 A/m and a modulation voltage of 1500 mV

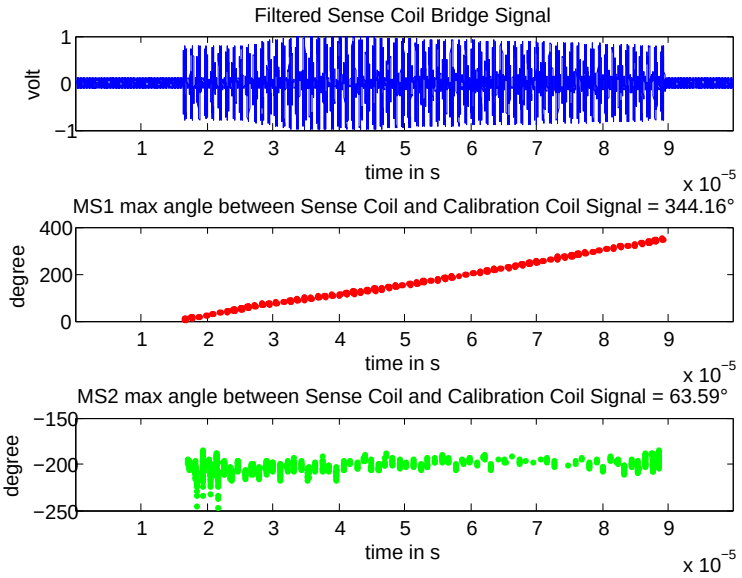


Figure 6.11: Test case 5° sweep: sampled phase of both MS at 1 A/m and a modulation voltage of 1000 mV

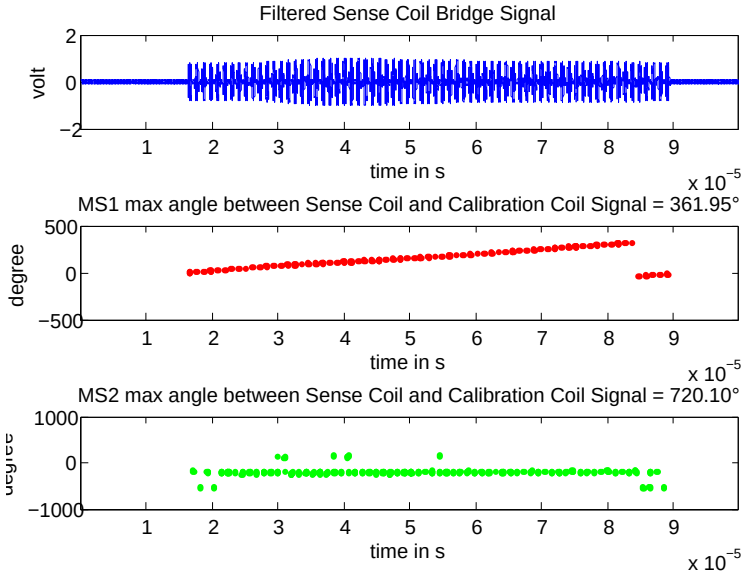


Figure 6.12: Test case 5° sweep: sampled phase of both MS at 1 A/m and a modulation voltage of 100 mV

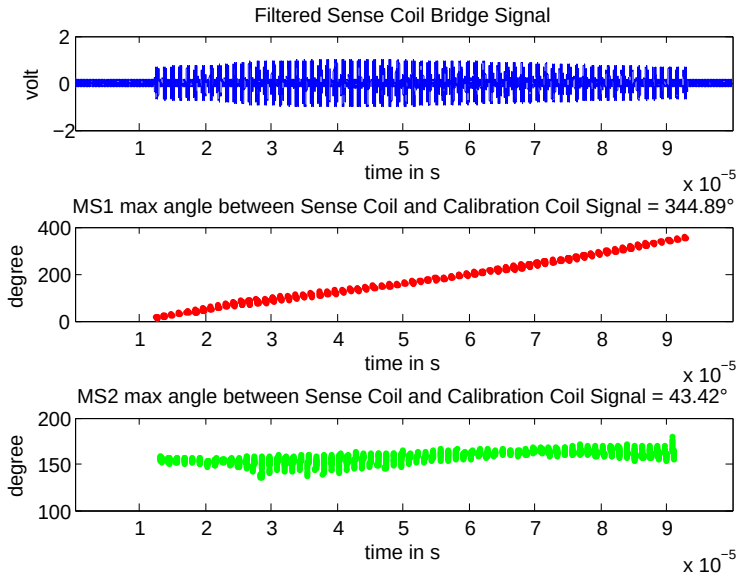


Figure 6.13: Test case 5° sweep: sampled phase of both MS at 1.5 A/m and a modulation voltage of 2000 mV

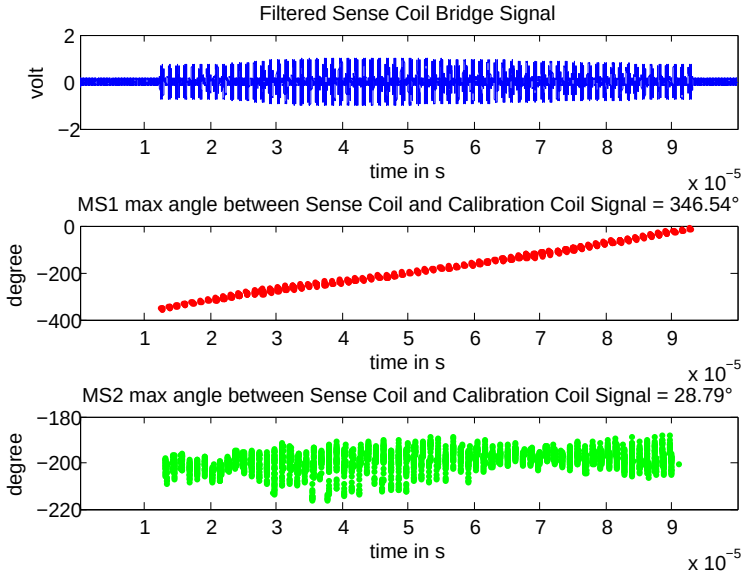


Figure 6.14: Test case 5° sweep: sampled phase of both MS at 1.5 A/m and a modulation voltage of 1500 mV

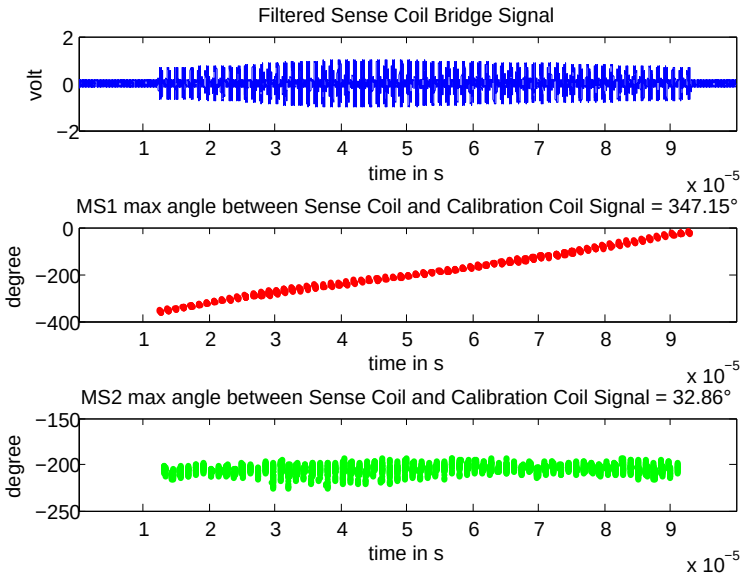


Figure 6.15: Test case 5° sweep: sampled phase of both MS at 1.5 A/m and a modulation voltage of 1000 mV

6.4 Discussion

Unfortunately, the final chapter is characterized by lack of time as well as technical issues. Problems with the *Conditioning Board* along with the *Extended RefPICC* lead to a premature end of the final test measurement series without being able to fully evaluate the imposed test signals as defined in section 5.3.1. Therefore the relevance and interpretability must be questioned to some extent.

To protect the test bench the field strength for the PCD field was set, most of the times, below the ISO 14443 defined range of 1.5 to 7 A/m.

The applied evaluation algorithms as presented in the prior chapters, proved to be more sensitive to the actual test-system as expected. In particular the selection- and cutting-algorithms showed shortcomings leading to unintended edges in the depictions of the phase drift or minor distortions which do appear in the depictions of MS1 at times, but more prominently in the depictions of MS2, mostly leading to huge artificial phase drifts (see especially 6.3.3).

The setup proved to be functional as long as no communication gaps, in case of an ISO 14443 Type A communication, or field resets of the PCD appeared.

Chapter 7

Conclusion and Outlook

The decision to use compact devices instead of a complex circuitry set the agenda of this master thesis very early on. It was determined not only by *Infineon Technologies AG* but also the WG8 council[1] that a possible solution shall be as least complicated as possible. The use of an all-in-one device was the logical decision. The test bench, as a Proof-of-Concept, shows to work under defined preconditions, such as ISO 14443 Type B communication in general, or under a continuously applied PCD magnetic field without signal gaps.

There are some issues which clearly remain:

Firstly, the *Current Source Circuitry* forming the *Extended RefPICC* along with the RefPICC defined in ISO/IEC 14443 which proved to be inherently unstable (section 5.1) and quite delicate to handle. It needs to be decided whether a different concept or a revision with more focus on better durability, robustness and stability may come in favor. Throughout this thesis, the inability to reach the ISO 14443 defined maximum load modulation amplitude, V_{LMA} became evident. The current concept would need to be able to drive even a higher bias-current through the current source device. Given the already impairing influence of these high currents and temperatures, a whole different approach seems to be inevitable. Also the concept to unite ALM and PLM in a single PCB needs to be evaluated and discussed.

Secondly, the proper adaptation to use the test bench universally is essential. In general, field-resets and pauses of the sinusoidal PCD magnetic field (e.g. Type A gaps) mean the loss of synchronicity between the PCD and the PICC signals. The use of the vector analyzer therefore proved to be only suitable for PCD signals which remain without field-resets or communication gaps. Under these circumstances, a practical relevance seems to be unimaginable. With Mifare, using ISO 14443 Type A communication dominating

[1] WG8 is one of the Working Groups within the subcommittee ISO/IEC JTC1/SC17 "Identification Cards" and was established in 1988 to develop standards for contactless chip cards.

the contactless smart cards market the relevance of the current test bench seems to be only of theoretical nature.

Thirdly, the evaluation methods outlined are a first iteration, which proved to be functional and stable enough for artificial signals. The final measurements revealed several shortcomings which all impede a correct and even more so, a reliable interpretation of the obtained results. A reworking of the evaluation algorithms or reconsideration of used methods is therefore highly recommended.

As long as these most glaring issues remain unresolved, further considerations towards automation or optimization are not expedient.

Bibliography

[1] Austrian Institute of Technology: *Test PCD Assembly*. Web: 26. Apr. 2014. http://www.ait.ac.at/fileadmin/mc/mobility/downloads/MIFARE_RFID/Test_PCD_assembly.pdf

[2] ISO/IEC 10373-6:2011: *Identification cards - Test methods - Part 6: Proximity cards 2nd edition*

[3] ISO/IEC 14443-2:2010: *Identification cards - Contactless integrated circuit cards - Proximity cards - Part 2: Radio frequency power and signal interface*

[4] ISO/IEC 14443-3:2013: *Identification cards - Contactless integrated circuit cards - Proximity cards - Part 3: Initialization and anticollision*

[5] ISO/IEC 14443-2: *Identification cards - Contactless integrated circuit cards - Proximity cards - Part 2: Radio frequency power and signal interface: AMENDMENT 6 Parameters supporting active and passive PICC transmissions*

[6] EMVCo: *EMVCo-FAQ*. Web: 10. Apr. 2014 http://www.emvco.com/faq.aspx?id=37

[7] EMVCo: *Card / Terminal General Questions*. Web: 10. Apr. 2014 http://www.emvco.com/faq.aspx?id=41#1

[8] EMVCo: *EMV Contactless Specifications for Payment Systems - Book D: EMV Contactless Communication Protocol Specification Version 2.1*

[9] EMVCo: *EMVCo Type Approval Contactless Terminal Level 1: PCD Analogue Test-Bench and Test Case Requirements Version 2.1a*

[10] NFC Forum Website: *About NFC*. Web: June 2014 http://members.nfc-forum.org/aboutnfc/interop/

[11] WG8 *WG8 Documents*. Web: 22. Apr. 2014. http://wg8.de/secure/wg8n1955_CD_14443-2_PDAM6_Parameters_supporting_active_and_passive_PICC_transmissions.zip

[12] WG8/TF2 *PICCs supporting passive and/or active transmission PCD and PICC test methods Test case definition and signal generation feasibility analysis*. Web: 22. Apr. 2014.
ISO-IECJTC1-SC17-WG8_N2085_TF2_N794_PICC_supporting_passive_.pdf

[13] Minutes of the 41th meeting of WG8/TF2, Singapore, September 2013

[14] SC17/WG8N2054, Peter Raggam, *PICC phase drift analysis tool*, DIN contribution, May 2013

[15] SC17/WG8N1745, Pascal Roux, *Minutes of the 33rd meeting of WG8 Task Force 2*, S. 7, http://wg8.de/WG8DocList.html, September 2010

[16] SC17/WG8N1722, Klaus Finkenzeller, *Enhanced Modulation PICC to PCD*, DIN Contribution, http://wg8.de/WG8DocList.html, September 2010

[17] SC17/WG8N1755, New Work Item Proposal, Revision 1, PICCs with external power supply, http://wg8.de/WG8DocList.html, October 2010

[18] SC17/WG8N2054, PICC Phase Drift Analysis, http://wg8.de/WG8DocList.html, June 2013

[19] SC17/WG8N2040, Measurements on carrier (fc) stability, http://wg8.de/WG8DocList.html, June 2013

[20] Finkenzeller K: *RFID Handbuch - 6. Auflage*. Munich, Carl Hanser Verlag (2012)

[21] Klaus Finkenzeller: *Battery powered tags for ISO/IEC 14443, actively emulating load modulation*. Web: 10. Apr. 2014
http://www.rfid-handbook.de/downloads/Active-load-modulation_Finkenzeller_20110413_final.pdf

[22] Oppenheim, Schafer: Discrete Time-Signal Processing 3rd Edition, Paerson

[23] Stephane Czeck, *ISO? EMV? NFC Forum? NFC Analog testing in a nutshell*. Web: January 2013 http://www.wima.mc/dan/2012/PRESENTATIONS/czeck_stephane.pdf

[24] Jurisch, Reinhard (1994) Coil on Chip — monolithisch integrierte Spulen für Identifikationssysteme, GME technical report Identifikationssysteme und kontaktlose Chipkarten, vde-Verlag, Berlin

[25] Bernard Sklar. *Digital Communciations - Fundamentals and Applications*. Prentice Hall, 2nd edition, 2002.

[26] H. Zangl/Th. Bretterklieber. *Demodulation of 13.56 MHz load-modulated signals*. e&i - Elektrotechnik & Informationstechnik, 11, 2007.

[27] Egger Ch: *Reference PICC for Extended Modulation and LMA Measurement Principles*. Master's Thesis (2013)

[28] Hoelzl J: *Extended Card Modulation - Test Methods*. Master's Thesis (2011)

[29] Lund University, Sweden, Bilginer, Ljunggren *Near Field Communication*. Master's Thesis, February 2011 http://cwi.unik.no/images/Master_thesis_lu_NFC.pdf

[30] Agilent Technologies: *Digital Modulation in Communication Systems - An Introduction*. Web: 15. Mar. 2014
http://cp.literature.agilent.com/litweb/pdf/5965-7160E.pdf http://www.ni.com/white-paper/4805/en/

[31] Course Readings of Stanford University: *John Cioffi: Digital Communication: Signal Processing*. Web: 15. Apr. 2014
http://www.stanford.edu/group/cioffi/doc/book/chap6.pdf

[32] Transactions on electrical and electronic materials: *A 13.56 MHz Radio Frequency Identification Transponder - Analog Front End Using a Dynamically Enabled Digital Phase Locked Loop* . Web: 25. Apr. 2014
http://www.transeem.org/Upload/files/TEEM/article4.pdf

[33] Agilent Technologies *Agilent X-Series - Service Guide*. Web: 22. Apr. 2014.
http://cp.literature.agilent.com/litweb/pdf/N5180-90059.pdf

[34] Agilent Technologies *EXG X-Series Signal Generators N5171B Analog & N5172B Vector Data Sheet*. Web: 22. Apr. 2014.
http://cp.literature.agilent.com/litweb/pdf/5991-0039EN.pdf

[35] Agilent Technologies *Agilent X-Series Signal Generators - User's Guide*. Web: 22. Apr. 2014.
http://cp.literature.agilent.com/litweb/pdf/N5180-90056.pdf

[36] Keysight Technologies *N5172B EXG X-Series RF Vector Signal Generator, 9 kHz to 6 GHz*. Web: 22. Apr. 2014.
http://www.keysight.com/en/pd-2115739-pn-N5172B/

[37] Keysight Technologies *Keysight X-Series Signal Generators - Programming Guide*. Web: 22. Apr. 2014.
http://literature.cdn.keysight.com/litweb/pdf/N5180-90074.pdf

[38] Tabor Electronics Ltd: *Model WW1281A - 1.2GS/s Single-Channel Arbitrary Waveform Generator*. Web: 27. Feb. 2013
http://www.taborelec.com/products_home.asp?prod=arbitrary_waveform_function_generator&model=WW1281A&over=products&prod3=single_channel_arbitrary_waveform_generators

[39] Mathworks: *Generating Waveforms on Agilent MXG, ESG, PSG Signal Sources using MATLAB*. Web: 29. October. 2013
http://http://www.mathworks.com/matlabcentral/fileexchange/24048-generating-waveforms-on-agilent-mxg--esg--psg-signal-sources-using-matlab

[40] Linear Technology Corporation: *LTSPICE IV*. Web: 27. Feb. 2013. http://www.linear.com/designtools/software/#LTspice

[41] Linear Technology: *LT1719 - 4.5ns Single/Dual Supply 3V/5V Comparator with Rail-to-Rail Output*. Web: 10. Apr. 2014 http://cds.linear.com/docs/en/datasheet/1719fa.pdf

[42] Texas Instruments: *BUF602: High Speed, Closed-Loop Buffer*. Web: 10. Apr. 2014 http://www.ti.com.cn/cn/lit/ds/symlink/buf602.pdf

[43] Texas Instruments: *LP2985: 150-mA LOW-NOISE LOW-DROPOUT REGULATOR WITH SHUTDOWN*. Web: 10. Apr. 2014 http://www.ti.com/lit/ds/slvs522n/slvs522n.pdf

[44] Datasheet and Overview of Linear's LT3092, Web: 10. Jan. 2014 http://www.linear.com/product/LT3092#overview